ON THE WEIL SUM EVALUATION OF CENTRAL POLYNOMIAL IN MULTIVARIATE QUADRATIC CRYPTOSYSTEM

TOMOHIRO HARAYAMA

Abstract. A parity checking-styled Weil sum algorithm is presented for a general class of the univariate polynomials which fully characterize a system of n polynomials in n variables over F_2. The previously known proof methods of explicit Weil sum evaluation of Dembowski-Ostrom polynomials are extended to general case. The algorithm computes the absolute values of the Weil sums of the generic central polynomials in MQ problem.

1. Introduction

1.1. **Character and Weil Sum.** Let p be a prime (2 or odd) and $q = p^n$ for integer n. We denote the finite field of q elements by F_q. F_q is often regarded as a vector space F_p^n over F_p of dimension n with some basis. A trace function $Tr_t : F_q \to F_{p^t}$ for some integer t which divides n, is defined by $Tr_t(x) = x + x^{p^t} + x^{p^{2t}} + \ldots + x^{p^{(n/t-1)t}}$ for all $x \in F_q$, and the absolute trace function is simply denoted by Tr (when $t = 1$). Since we identify F_p with $Z/(p)$, the image of absolute trace function of any $x \in F_q$ are merely the integers in $[0, p-1]$. The trace function satisfies: $Tr_t(ax) = aTr_t(x)$, $Tr_t(x + y) = Tr_t(x) + Tr_t(y)$ and $Tr_t(x^{p^t}) = Tr_t(x)$ for all $x, y \in F_q$ and $a \in F_{p^t}$ (Theorem 2.23. [13]). We denote the canonical additive character by $\chi_1(x) = \exp(2\pi i Tr(x)/p)$ for $x \in F_q$. From Theorem 5.7 [13], any additive character χ_a of F_q is obtained from $\chi_a(x) = \chi_1(ax)$ for all $x \in F_q$ with some $a \in F_q$. From the properties of trace function, we have: $\chi_1(x + y) = \chi_1(x)\chi_1(y)$ and $\chi_1(x^p) = \chi_1(x)$ for all $x, y \in F_q$. With a nontrivial additive character χ of F_q, the sum:

$$\sum_{x \in F_q} \chi(f(x)),$$

is called a *Weil sum* of a polynomial $f(x)$ (Chapter 5. [13]).

1.2. **Multivariate Quadratic Problem and Central Polynomial.** Multivariate quadratic cryptosystems (e.g., HFE system and variations: [15, 8, 6]. Tame transformation and variations: [1, 10]. Others: [11, 16, 17]) rely their security on the computational hardness (cf. [15, 9]) of a problem to solve randomly generated systems of multivariate quadratic polynomials over finite fields. This problem can be formally described as follows.

Received by the editors February 22, 2006.

Key words and phrases. MQ problem, MQ-trapdoor function, multivariate quadratic cryptosystem, Dembowski-Ostrom polynomial, central polynomial, character and Weil sum.

Definition 1.2.1. (MQ Problem. cf. [5, 6]). Let $P_1, \ldots, P_m \in F_q[x_1, \ldots, x_n]$ m polynomials of n variables over F_q, each of which has form:

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

whereby $\alpha_{i,j}^{(k)}, \beta_i^{(k)}, \gamma_i^{(k)} \in F_q$ for all $1 \leq k \leq n$. Then, a *MQ problem* denoted by $MQ(q, n, m)$ is a problem of solving indeterminates $x_i \in F_q$ of the random system of m polynomial equations $y_i = P_i(x_1, \ldots, x_n)$ for $1 \leq i \leq m$.

Now, let ϕ be the standard linear bijection $\phi : F_{q^n} \to F_q^n$ (with some fixed basis of F_{q^n} over F_q). We introduce an important fact about this MQ problem.

Lemma 1.2.2. *(Kipnis and Shamir, 1999.* [12]*). Let* $F = (P_1(x_1, \ldots, x_n), \ldots, P_n(x_1, \ldots, x_n))$ *be a system of* n *multivariate polynomials of MQ Problem* $MQ(q, n, n)$ *as is in Definition 1.2.1. Then, there exists an univariate polynomial over* F_{q^n}*:*

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

where $D, L \in N$*,* $a_i, b_j, c \in F_{q^n}, \alpha_i \geq \beta_i$*,* $q^{\alpha_i} + q^{\beta_i}, q^{\gamma_j} \leq q^n - 1$ *for each* $1 \leq i \leq D, 1 \leq j \leq L$*, such that*

$$\phi \circ f \circ \phi^{-1}(v_1, \ldots, v_n) = (P_1(v_1, \ldots, v_n), \ldots, P_n(v_1, \ldots, v_n)),$$

for $\forall (v_1, \ldots, v_n) \in F_p^n$*.*

In this paper, we name the univariate polynomial associated with the $MQ(q, n, n)$ in Lemma 1.2.2 as follows.

Definition 1.2.3. (Central Polynomial). Given a system of n multivariate polynomials $(P_1(x_1, \ldots, x_n), \ldots, P_n(x_1, \ldots, x_n))$ of MQ problem $MQ(q, n, n)$. A *central polynomial* of multivariate quadratic cryptosystem based on $MQ(q, n, n)$ is the univariate polynomial in $F_{q^n}[x]$ of the form:

$$f(x) = \sum_{i=1}^{D} a_i x^{q^{\alpha_i} + q^{\beta_i}} + \sum_{j=1}^{L} b_j x^{q^{\gamma_j}} + c, \tag{1.2.1}$$

where $D, L \in N$, $a_i, b_i, c \in F_{q^n}, \alpha_i \geq \beta_i$, $q^{\alpha_i} + q^{\beta_i}, q^{\gamma_j} \leq q^n - 1$ for each $1 \leq i \leq D, 1 \leq j \leq L$, which are obtained from Lemma 1.2.2.

The term "central" purely comes from a cryptographic reason for the design methods of trapdoor structures commonly built in the concrete multivariate quadratic cryptosystems. In such systems the central polynomial of Definition 1.2.3 often appears at the center of the composition of 3 secret mappings over $F_{q^n} \cong F_q^n$ (in particular, for HFE systems [15, 8]). We can also apply Kipnis and Shamir's Lemma 1.2.2 to express $MQ(q, n, n)$ itself by this central polynomial. When a central polynomial has no linearized and constant terms, the polynomial has a special name in the following.

Definition 1.2.4. (Dembowski-Ostrom Polynomial. [7, 2, 3, 4, 14]) . A polynomial in $F_{q^n}[x]$ of the form:

$$f(x) = \sum_{i=1}^{D} a_i x^{q^{\alpha_i}+q^{\beta_i}},$$

where $D \in N$, $a_i \in F_{q^n}, \alpha_i \geq \beta_i$, $q^{\alpha_i} + q^{\beta_i} \leq q^n - 1$ for each $1 \leq i \leq D$, is called a *Dembowski-Ostrom* polynomial.

This quadratic *multinomial* is the source of the computational hardness gained in the MQ problem and MQ trapdoor function. We note that a Dembowski-Ostrom polynomial can be expressed by a product of two linearized polynomials (Definition 3.58. [13]) and from Kipnis-Shamir's Lemma 1.2.2 it corresponds to a homogeneous system over F_p in the multivariate representation.

As a result, regardless of the concrete type of trapdoor structures designed in MQ problem, we can always work on the corresponding univariate polynomial over the extension field F_{q^n} of form: $f(x) = \sum_{i=1}^{D} a_i x^{q^{\alpha_i}+q^{\beta_i}} + \sum_{j=1}^{L} b_j x^{q^{\gamma_j}} + c$ which is identical to that of central polynomial in Definition 1.2.3 for the system $F = (P_1(x_1, \ldots, x_n), \ldots, P_n(x_1, \ldots, x_n))$ over F_q. Similarly, we may have Dembowski-Ostrom polynomial: $f(x) = \sum_{i=1}^{D} a_i x^{q^{\alpha_i}+q^{\beta_i}}$, when each multivariate polynomial P_k of the system is a quadratic form (i.e. homogeneous quadratic polynomial).

2. Weil Sum Evaluation of Central Polynomial

Let F_q be a finite field of characteristic p (2 or any odd prime) and order $q = p^n$. We fix the two finite fields F_p (Galois field) and F_q (its extension) in this chapter. F_q is regarded as a vector space F_p^n over F_p of dimension n with some basis.

First we extend the previously known proof methods of *explicit Weil sum evaluation* of Dembowski-Ostrom polynomials [2, 3, 4, 14] to central polynomials in Definition 1.2.3.

2.1. **Simplification of Central Polynomial.** Let $S(a_1, \ldots, a_D, b_1, \ldots, b_L, c)$ (or simply S) denote the Weil sum of a central polynomial $f(x) = \sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}} + \sum_{j=1}^{L} b_j x^{p^{\gamma_j}} + c \in F_q[x]$ (Definition 1.2.3). Explicitly, with canonical additive character χ_1 of F_q, we consider:

$$S = S(a_1, \ldots, a_D, b_1, \ldots, b_L, c) = \sum_{x \in F_q} \chi_1(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}} + \sum_{j=1}^{L} b_j x^{p^{\gamma_j}} + c).$$

Applying the property of additive character to the *constant* term c of $f(x)$ in the Weil sum S yields an equivalent Weil sum:

$$S = \chi_1(c)\{\sum_{x \in F_q} \chi_1(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}} + \sum_{j=1}^{L} b_j x^{p^{\gamma_j}})\}.$$

I.e., one can separately treat the image of c by character χ_1 when we evaluate the Weil sum value S. Therefore, without loss of generality, we can always assume that the constant term of central polynomials be zero ($f(0) = c = 0$) and may separately deal with the value $\chi_1(c) = \chi_1(f(0))$ at the final step of Weil sum evaluation algorithm.

In the following we will show that we can also simplify the *linearized* terms $\sum_{j=1}^{L} b_j x^{p^{\gamma_j}}$ in the central polynomial $f(x) = \sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}} + \sum_{j=1}^{L} b_j x^{p^{\gamma_j}}$. The newly introduced coefficients $A_i \in F_q$ and parameters $t_i, y_i, s_i \in Z$ and $b \in F_q$ in the following theorem will be later justified in the specification of the subsequent Theorem 2.2.1 regarding the auxiliary linearized polynomial of central polynomial.

Theorem 2.1.1. *(Simplification of Central Polynomial). Let $f(x)$ be a central polynomial over F_q of Definition 1.2.3 (with $f(0) = 0$). Assume that we set the new coefficients A_i such that $A_i^{p^{t_i}} = a_i \in F_q$ $(1 \leq i \leq D)$ and parameters $t_i, y_i, s_i \in Z$, and $b \in F_q$ such that $t_i \equiv \beta_i - \beta_1 \mod n$ $(1 \leq i \leq D)$, and $y_i = n - s_i$ $(2 \leq i \leq D)$, $s_i = \alpha_i - \beta_i \geq 0$ $(1 \leq i \leq D)$ and $b = \sum_{j=1}^{L} b_j^{p^{e-\gamma_j}}$. Then, we can express the Weil sum $S = S(a_1, \ldots, a_D, b_1, \ldots, b_L)$ of $f(x)$ as:*

$$S = \sum_{x \in F_q} \chi_1\Big(\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x\Big).$$

We call the polynomial $\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x$ the simplified central polynomial of $f(x)$.

Proof. The proof of the simplification consists of the two parts. First, we simplify the linearized terms $\sum_{j=1}^{L} b_j x^{p^{\gamma_j}}$ in central polynomial $f(x)$ into a *single linear* term. In the transformations below, we repeatedly apply the properties of additive character when splitting and joining the arguments of χ_1 and taking the various powers of p inside the each argument. The first transformation is the following.

$$\begin{aligned}
\sum_{x \in F_q} \chi_1\Big(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}} + \sum_{j=1}^{L} b_j x^{p^{\gamma_j}}\Big) &= \sum_{x \in F_q} \chi_1\Big(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}}\Big)\chi_1\Big(\sum_{j=1}^{L} b_j x^{p^{\gamma_j}}\Big) \\
&= \sum_{x \in F_q} \chi_1\Big(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}}\Big) \prod_{j=1}^{L} \chi_1(b_j x^{p^{\gamma_j}}) \\
&= \sum_{x \in F_q} \chi_1\Big(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}}\Big) \prod_{j=1}^{L} \chi_1(b_j^{p^{e-\gamma_j}} x^{p^e}) \\
&= \sum_{x \in F_q} \chi_1\Big(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}}\Big) \prod_{j=1}^{L} \chi_1(b_j^{p^{e-\gamma_j}} x) \\
&= \sum_{x \in F_q} \chi_1\Big(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}}\Big)\chi_1\Big(\sum_{j=1}^{L} b_j^{p^{e-\gamma_j}} x\Big) \\
&= \sum_{x \in F_q} \chi_1\Big(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}}\Big)\chi_1(bx) \\
&= \sum_{x \in F_q} \chi_1\Big(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}} + bx\Big).
\end{aligned}$$

Therefore, the linearized terms $\sum_{j=1}^{L} b_j x^{p^{\gamma_j}}$ of $f(x)$ is turned into a single linear term bx where $b = \sum_{j=1}^{L} b_j^{p^{e-\gamma_j}}$ and thus we have $S = S(a_1, \ldots, a_D, b_1, \ldots, b_L) = S(a_1, \ldots, a_D, b)$.

Next, we replace the coefficients a_i's with the new coefficients $A_i \in F_q$ under the new integer parameters $t_i \equiv \beta_i - \beta_1 \mod n$ $(1 \leq i \leq D)$, $y_i = n - s_i$ $(2 \leq i \leq D)$,

$s_i = \alpha_i - \beta_i \geq 0$ $(1 \leq i \leq D)$. I.e., We have:

$$\begin{aligned}
S(a_1, \ldots, a_D, b) &= \sum_{x \in F_q} \chi_1(\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}} + bx) \\
&= \sum_{x \in F_q} \prod_{i=1}^{D} \chi_1(a_i x^{p^{\alpha_i}+p^{\beta_i}})\chi_1(bx) \\
&= \sum_{x \in F_q} \prod_{i=1}^{D} \chi_1(a_i x^{p^{\beta_i}(p^{s_i}+1)})\chi_1(bx) \\
&= \sum_{x \in F_q} \prod_{i=1}^{D} \chi_1(A_i^{p^{t_i}} (x^{p^{\beta_1}})^{p^{t_i}(p^{s_i}+1)})\chi_1(b^{p^{\beta_1}} x^{p^{\beta_1}}) \\
&= \sum_{u \in F_q} \prod_{i=1}^{D} \chi_1((A_i u^{p^{s_i}+1})^{p^{t_i}})\chi_1(b^{p^{\beta_1}} u) \text{ [Note: } u = x^{p^{\beta_1}}] \\
&= \sum_{u \in F_q} \chi_1(\sum_{i=1}^{D} A_i u^{p^{s_i}+1} + b^{p^{\beta_1}} u).
\end{aligned}$$

Therefore, we obtain the simplification $S(a_1, \ldots, a_D, b) = S(A_1, \ldots, A_D, b)$, i.e., the equivalent Weil sum of the form:

$$S = \sum_{x \in F_q} \chi_1(\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x),$$

with the simplified central polynomial $\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x$. We obtained the desired result. $\square$

This theorem says that at the level of Weil sum values the Weil sum of generic central polynomial is equal to that of special type of central polynomial of form

$$\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x.$$

This is the reason we name this type a simplified central polynomial.

2.2. **Weil Sum of Central Polynomial.** It is shown that in Theorem 2.1.1 the Weil sum of an arbitrary central polynomial $\sum_{i=1}^{D} a_i x^{p^{\alpha_i}+p^{\beta_i}} + \sum_{j=1}^{L} b_j x^{p^{\gamma_j}}$ (no constant term) over F_q is equivalent to that of the corresponding simplified central polynomial of the form $\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x$ with specially introduced new coefficients $A_i \in F_q$ and parameters $t_i, y_i, s_i \in Z$ and $b \in F_q$. In the following theorem, we will justify their occurrences. We will deduce the *auxiliary linearized polynomial*, denoted by $T_D(x)$ in $F_q[x]$. This linearized polynomial naturally appears during the calculation in the proof and afterward enables us to compute the concrete absolute value of the Weil sum. As is common in the proof techniques of explicit evaluation of Weil sum, we start with taking the *product* of the Weil sum and its *conjugate.* Note that the p can be either 2 or any odd prime.

Theorem 2.2.1. *(Auxiliary Linearized Polynomial. cf. Theorem 1.4.* [14]*). Let $f(x)$ be a central polynomial over F_q of Definition 1.2.3 (with $f(0) = 0$), and S be the Weil sum of $f(x)$. Then, the product $|S|^2 = S\overline{S}$ is:*

$$|S|^2 = q \sum_{T_D(w)=0, w \in F_q} \chi_1(\sum_{i=1}^{D} A_i w^{p^{s_i}+1} + b^{p^{\beta_1}} w),$$

whereby A_i's are the new coefficients such that $A_i^{p^{t_i}} = a_i$ $(1 \leq i \leq D)$, t_i, y_i, s_i and b are the new parameters such that $t_i \equiv \beta_i - \beta_1 \mod n$ $(1 \leq i \leq D)$, $y_i = n - s_i$ $(2 \leq i \leq D)$, $s_i = \alpha_i - \beta_i \geq 0$ $(1 \leq i \leq D)$ and $b = \sum_{j=1}^{L} b_j^{p^{e-\gamma_j}}$. The index w of the outer sum runs throughout the set of roots in F_q of a linearized polynomial defined as:

$$T_D(w) = A_1^{p^{s_1}} w^{p^{2s_1}} + A_1 w + \sum_{i=2}^{D} [A_i^{p^{s_1}} w^{p^{s_1+s_i}} + (A_i w)^{p^{s_1+y_i}}].$$

Proof. From Theorem 2.1.1 we can work on the simplified central polynomial $\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x$ over F_q. I.e., the Weil sum is expressed by:

$$S = S(A_1, \ldots, A_D, b^{p^{\beta_1}}) = \sum_{x \in F_q} \chi_1(\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x).$$

Now, let us take the product $|S|^2 = S(A_1, \ldots, A_D, b^{p^{\beta_1}}) \overline{S(A_1, \ldots, A_D, b^{p^{\beta_1}})}$. We will show that the linearized polynomial $T_D(x)$ naturally appears during the course of simplification of this product. As is in the transformation in Theorem 2.1.1, we repeatedly apply the properties of additive character when splitting and joining the arguments of χ_1 and taking the various powers of p inside the each argument. First we have:

$$\begin{aligned}
|S|^2 &= S\overline{S} \\
&= \{\sum_{u \in F_q} \chi_1(\sum_{i=1}^{D} A_i u^{p^{s_i}+1} + b^{p^{\beta_1}} u)\} \cdot \{\sum_{v \in F_q} \overline{\chi_1}(\sum_{i=1}^{D} +A_i v^{p^{s_i}+1} + b^{p^{\beta_1}} v)\} \\
&= \{\sum_{u \in F_q} \chi_1(\sum_{i=1}^{D} A_i u^{p^{s_i}+1} + b^{p^{\beta_1}} u)\} \cdot \{\sum_{v \in F_q} \chi_1(\sum_{i=1}^{D} -A_i v^{p^{s_i}+1} - b^{p^{\beta_1}} v)\} \\
&= \sum_{u,v \in F_q} \chi_1(\sum_{i=1}^{D} A_i [u^{p^{s_i}+1} - v^{p^{s_i}+1}] + b^{p^{\beta_1}} (u - v)) \\
&= \sum_{w,v \in F_q} \chi_1(\sum_{i=1}^{D} A_i [(w + v)^{p^{s_i}+1} - v^{p^{s_i}+1}] + b^{p^{\beta_1}} w) \\
&= \sum_{w,v \in F_q} \chi_1(\sum_{i=1}^{D} A_i (w^{p^{s_i}+1} + w v^{p^{s_i}+1} + v w^{p^{s_i}+1}) + b^{\beta^{s_1}} w) \\
&= \sum_{w,v \in F_q} \chi_1(\sum_{i=1}^{D} A_i w^{p^{s_i}+1} + b^{p^{\beta_1}} w) \cdot \chi_1(\sum_{i=1}^{D} A_i (w v^{p^{s_i}} + v w^{p^{s_i}})).
\end{aligned}$$

We can further simplify the character $C_{w,v} = \chi_1(\sum_{i=1}^{D} A_i(wv^{p^{s_i}} + vw^{p^{s_i}}))$ as follows.

$$\begin{aligned}
C_{w,v} &= \chi_1(\sum_{i=1}^{D} A_i(wv^{p^{s_i}} + vw^{p^{s_i}})) \\
&= \chi_1(A_1 vw^{p^{s_1}} + A_1 wv^{p^{s_1}} + \sum_{i=2}^{D} A_i vw^{p^{s_i}} + \sum_{i=2}^{D} A_i wv^{p^{s_i}}) \\
&= \chi_1(A_1^{p^{s_1}} v^{p^{s_1}} w^{p^{2s_1}} + A_1 wv^{p^{s_1}} + \sum_{i=2}^{D} A_i^{p^{s_1}} v^{p^{s_1}} w^{p^{s_i+s_1}} + \sum_{i=2}^{D} (A_i w)^{p^{s_1+y_i}} v^{p^{s_1}}) \\
&= \chi_1(v^{p^{s_1}} T_D(w)).
\end{aligned}$$

Therefore, we have:

$$|S|^2 = \sum_{w\in F_q} \chi_1(\sum_{i=1}^{D} A_i w^{p^{s_i}+1} + b^{p^{\beta_1}} w) \cdot \sum_{v\in F_q} \chi_1(v^{p^{s_1}} T_D(w)).$$

Recall that $v^{p^{s_1}}$ runs throughout F_q as v runs throughout F_q. Also, the inner sum $\sum_{v\in F_q} \chi_1(v^{p^{s_1}} T_D(w))$ is zero unless $T_n(w) = 0$ for the index $w \in F_q$ of the outer sum, because otherwise $v^{p^{s_1}} T_D(w)$ also runs throughout F_q as v runs throughout F_q. Therefore we have:

$$|S|^2 = q \sum_{T_D(w)=0, w\in F_q} \chi_1(\sum_{i=1}^{D} A_i w^{p^{s_i}+1} + b^{p^{\beta_1}} w),$$

which is the desired result. $\square$

Finally, we will show a lemma regarding the set of roots of the auxiliary linearized polynomial of central polynomial.

Lemma 2.2.2. *(Roots of Auxiliary Linearized Polynomial. Lemma 3.4* [14]*). Let $T_D(x)$ be an auxiliary linearized polynomial over F_q defined in Theorem 2.2.1. Suppose that $\varepsilon = \gcd_{2\le i\le D}(2s_1, s_1+s_i, s_1+y_i, n)$. Then, the set of roots of $T_D(x)$ forms a linear subspace of F_q over F_{p^ε} and is isomorphic to $F_{p^{t\varepsilon}}$ for some integer $t \in Z$.*

Proof. For any monomial x^{p^α} in $T_D(x) = A_1^{p^{s_1}} x^{p^{2s_1}} + A_1 x + \sum_{i=2}^{D} [A_i^{p^{s_1}} x^{p^{s_1+s_i}} + (A_i x)^{p^{s_1+y_i}}]$, the exponent α is divisible by the greatest common divisor ε. Therefore for any $u \in F_{p^\varepsilon}$, $u^{p^\alpha} = (((u^{p^\varepsilon})^{p^\varepsilon})\cdots)^{p^\varepsilon} = u$ (α/ε times). Hence we have:

$$\begin{aligned}
T_D(ux) &= A_1^{p^{s_1}} (ux)^{p^{2s_1}} + A_1 ux + \sum_{i=2}^{D} [A_i^{p^{s_1}} (ux)^{p^{s_1+s_i}} + (A_i ux)^{p^{s_1+y_i}}] \\
&= A_1^{p^{s_1}} ux^{p^{2s_1}} + A_1 ux + \sum_{i=2}^{D} [A_i^{p^{s_1}} ux^{p^{s_1+s_i}} + u(A_i x)^{p^{s_1+y_i}}] \\
&= uT_D(x),
\end{aligned}$$

for all $u \in F_{p^\varepsilon}$. That is, the set of roots of $T_D(x)$ is a linear subspace of F_q over F_{p^ε}. By setting $t \in Z$ the dimension of this subvector space over F_{p^ε}, the set of the roots of $T_D(x)$ is $F_{p^\varepsilon}^t \simeq F_{p^{t\varepsilon}}$ and its cardinality is $p^{\varepsilon t}$. $\square$

2.3. **Weil Sum Algorithm for Central Polynomial.** For finite fields of characteristic $p = 2$, the Weil sum with canonical additive character is guaranteed to be *real*. It should be noted that this fact is quite different from those in the cases when p is odd prime [14]. We have the following lemma for $p = 2$.

Lemma 2.3.1. *(Character ($p = 2$)). Let F_q be of characteristic $p = 2$. Then, for any $u \in F_q$, $\chi_1(u)$ is real.*

Proof. It is a simple matter to show that from the definition of canonical additive character, for any $u \in F_q$, we have:

$$\chi_1(u) = \exp(\frac{2\pi i}{p} Tr(u)) = \exp(\pi i Tr(u)).$$

Since the image of $u \in F_q$ by the absolute trace function $Tr(u) = Tr_1(u)$ is in $\{0, 1\} = F_2$, the value $\chi_1(u)$ is either 1 or -1, which is real. $\square$

It is followed that by Lemma 2.3.1 when $p = 2$ we also have:

Corollary 2.3.2. *Let $p = 2$ and S the Weil sum of central polynomial $f(x)$ as is in Theorem 2.2.1. Then, S is real and $|S|^2 = S^2$.*

This corollary readily embraces the important idea for the efficient Weil sum algorithm (for $p = 2$). I.e., for finite fields of $p = 2$, if we can compute the product of the Weil sum S and its conjugate $\overline{S}$ as is in Theorem 2.2.1, then we can obtain the absolute value of the Weil sum $|S|$. To see this more specifically, let $f(x)$ be a central polynomial

$$f(x) = \sum_{i=1}^{D} a_i x^{p^{\alpha_i} + p^{\beta_i}} + \sum_{j=1}^{L} b_j x^{p^{\gamma_j}} \in F_q[x].$$

Theorem 2.1.1 says that we can express its Weil sum $S = S(a_1, \ldots, a_D, b_1, \ldots, b_L)$ as

$$S = \sum_{x \in F_q} \chi_1(\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x),$$

where $\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x$ is the simplified central polynomial with coefficients $A_i^{p^{t_i}} = a_i$ $(1 \le i \le D)$ and parameters $t_i \equiv \beta_i - \beta_1 \mod n$ $(1 \le i \le D)$, $y_i = n - s_i$ $(2 \le i \le D)$, $s_i = \alpha_i - \beta_i \ge 0$ $(1 \le i \le D)$, and $b = \sum_{j=1}^{L} b_j^{p^{e-\gamma_j}}$ as usual. By the theorem of auxiliary linearized polynomial Theorem 2.2.1, the product $|S|^2 = S\overline{S}$ is expressed by:

$$|S|^2 = q \sum_{T_D(w)=0, w \in F_q} \chi_1(\sum_{i=1}^{D} A_i w^{p^{s_i}+1} + b^{p^{\beta_1}} w),$$

where $T_D(w) = A_1^{p^{s1}} w^{p^{2s_1}} + A_1 w + \sum_{i=2}^{D} [A_i^{p^{s1}} w^{p^{s_1+s_i}} + (A_i w)^{p^{s_1+y_i}}]$ is the auxiliary linearized polynomial in $F_q[x]$, and also Corollary 2.3.2 yields

$$S = \pm\sqrt{S^2} = \pm\sqrt{|S|^2}.$$

Now, let us consider some basis $\{\omega_1, \ldots, \omega_n\}$ of F_q as a vector space $F_q \cong F_p^n$. Then, T_D is actually a linear mapping over F_p^n by the same reason in Lemma 2.2.2. More specifically, we have:

$$T_D(ux) = uT_D(x),$$

for all $u \in F_p$ and $x \in F_q$. (Obviously, the exponent $p^0 = 1$ of $u = u^{p^0}$ divides the exponents of any monomial appearing in $T_D(x)$.) Let us take a $n \times n$ matrix $B = (b_{ik}), 1 \leq i, k \leq n$ over F_p which represents the corresponding mapping T_D over F_q. In other words, we have for each ω_i in $\{\omega_1, \ldots, \omega_n\}$,

$$T_D(\omega_i) = \sum_{k=1}^{n} b_{ik}\omega_k,$$

$b_{ik} \in F_p$ and equivalently:

$$y_1\omega_1 + \cdots + y_n\omega_n = T_D(x_1\omega_1 + \cdots + x_n\omega_n) \Longleftrightarrow (y_1, \ldots, y_n) = (x_1, \ldots, x_n)B,$$

for $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in F_p^n$.

In order to actually compute the partial sum in the product $|S|^2$, we need some representation of the set of the roots of the equation $T_D(x) = 0$. Suppose $r = rank(B)$ be the rank of the matrix B. Then, there are p^{n-r} roots of $T_D(w) = 0$ in F_q (Note that $w = 0$ is always a root). So let $l = n - r$ and assume that some basis $\{\eta_1, \ldots, \eta_l\} \subset F_q$ forms the set of the roots of $T_D(w) = 0$ which is a subvector space of F_p^n. Then, from the properties of linearity and powers of p of trace function we have, for any $\eta = \sum_{i=1} x_i\eta_i \in ker(T_D)$ with each $x_i \in F_p$:

$$\begin{aligned}
Tr(\sum_{i=1}^{D} A_i\eta^{p^{s_i}+1} + b^{p^{\beta_1}}\eta) &= Tr(\sum_{i=1}^{D} A_i(\sum_{j=1}^{l} x_j\eta_j)^{p^{s_i}+1} + b^{p^{\beta_1}}(\sum_{j=1}^{l} x_j\eta_j)) \\
&= Tr(\sum_{i=1}^{D} A_i(\sum_{j_1=1}^{l} x_{j_1}\eta_{j_1}) \cdot (\sum_{j_2=1}^{l} x_{j_2}\eta_{j_2})^{p^{s_i}} + b^{p^{\beta_1}}(\sum_{j=1}^{l} x_j\eta_j)) \\
&= Tr(\sum_{i=1}^{D} A_i(\sum_{j_1=1}^{l} x_{j_1}\eta_{j_1}) \cdot (\sum_{j_2=1}^{l} x_{j_2}^{p^{s_i}}\eta_{j_2}^{p^{s_i}}) + b^{p^{\beta_1}}(\sum_{j=1}^{l} x_j\eta_j)) \\
&= \sum_{i=1}^{D}\sum_{j_1=1}^{l}\sum_{j_2=1}^{l} Tr(A_i x_{j_1} x_{j_2}^{p^{s_i}} \eta_{j_1}\eta_{j_2}^{p^{s_i}}) + \sum_{j=1}^{l} Tr(b^{p^{\beta_1}} x_j\eta_j) \\
&= \sum_{i=1}^{D}\sum_{j_1=1}^{l}\sum_{j_2=1}^{l} x_{j_1} x_{j_2}^{p^{s_i}} Tr(A_i\eta_{j_1}\eta_{j_2}^{p^{s_i}}) + \sum_{j=1}^{l} x_j Tr(b^{p^{\beta_1}}\eta_j) \\
&= \sum_{i=1}^{D}\sum_{j_1=1}^{l}\sum_{j_2=1}^{l} x_{j_1} x_{j_2} Tr(A_i\eta_{j_1}\eta_{j_2}^{p^{s_i}}) + \sum_{j=1}^{l} x_j Tr(b^{p^{\beta_1}}\eta_j).
\end{aligned}$$

Therefore, we have:

$$\chi_1(\sum_{i=1}^{D} A_i\eta^{p^{s_i}+1}+b^{p^{\beta_1}}\eta) = \exp(\frac{2\pi i}{p}(\sum_{i=1}^{D}\sum_{j_1=1}^{l}\sum_{j_2=1}^{l} x_{j_1}x_{j_2}Tr(A_i\eta_{j_1}\eta_{j_2}^{p^{s_i}})+\sum_{j=1}^{l} x_j Tr(b^{p^{\beta_1}}\eta_j))).$$

Henceforth, let us consider the case $\mathbf{p = 2}$. Now we have:

$$\chi_1(\sum_{i=1}^{D} A_i\eta^{2^{s_i}+1}+b^{2^{\beta_1}}\eta) = \exp(\pi i(\sum_{i=1}^{D}\sum_{j_1=1}^{l}\sum_{j_2=1}^{l} x_{j_1}x_{j_2}Tr(A_i\eta_{j_1}\eta_{j_2}^{2^{s_i}})+\sum_{j=1}^{l} x_j Tr(b^{2^{\beta_1}}\eta_j))).$$

By pre-computing the trace values:

$$\begin{cases} \gamma_{i,j_1,j_2} = Tr(A_i\eta_{j_1}\eta_{j_2}^{2^{s_i}}), \\ \rho_j = Tr(b^{2^{\beta_1}}\eta_j), \end{cases}$$

for $1 \le i \le D, 1 \le j_1, j_2 \le l$, we can evaluate the *parity* $C_{(x_1,\ldots,x_l)}$:

$$C_{(x_1,\ldots,x_l)} = \sum_{i=1}^{D} \sum_{j_1=1}^{l} \sum_{j_2=1}^{l} x_{j_1} x_{j_2} \gamma_{i,j_1,j_2} + \sum_{j=1}^{l} x_j \rho_j \in F_2 = \{0,1\}$$

for each $(x_1, \ldots, x_l) \in F_2^l$. Therefore, for the image of χ_1 on the argument with $\eta \in \ker(T_D)$, we have either:

$$\chi_1(\sum_{i=1}^{D} A_i \eta^{2^{s_i}+1} + b^{2^{\beta_1}} \eta) = \exp(\pi i C_{(x_1,\ldots,x_l)}) = 1,$$

if $C_{(x_1,\ldots,x_l)} = 0$, or:

$$\chi_1(\sum_{i=1}^{D} A_i \eta^{2^{s_i}+1} + b^{2^{\beta_1}} \eta) = \exp(\pi i C_{(x_1,\ldots,x_l)}) = -1,$$

if $C_{(x_1,\ldots,x_l)} = 1$. We can combine these two cases as:

$$\chi_1(\sum_{i=1}^{D} A_i \eta^{2^{s_i}+1} + b^{2^{\beta_1}} \eta) = \exp(\pi i C_{(x_1,\ldots,x_l)}) = 1 - 2C_{(x_1,\ldots,x_l)},$$

for each root $\eta = \sum_{i=1}^{l} x_i \eta_i \in ker(T_D)$. As a result, we obtain:

$$\begin{aligned}
|S|^2 &= |S(A_1, \ldots, A_D, b^{2^{\beta_1}})|^2 \\
&= 2^n \sum_{T_D(w)=0, w \in F_q} \chi_1(\sum_{i=1}^{D} A_i w^{2^{s_i}+1} + b^{2^{\beta_1}} w) \\
&= 2^n \sum_{(x_1,\ldots,x_l)\in F_2^l, \eta = \sum_{i=1}^{l} x_i \eta_i} \chi_1(\sum_{i=1}^{D} A_i \eta^{2^{s_i}+1} + b^{2^{\beta_1}} \eta) \\
&= 2^n \sum_{(x_1,\ldots,x_l)\in F_2^l} (1 - 2C_{(x_1,\ldots,x_l)}) \\
&= 2^n (2^l - 2 \sum_{(x_1,\ldots,x_l)\in F_2^l} C_{(x_1,\ldots,x_l)}).
\end{aligned}$$

Note that since $p = 2$, the simple parity check of the value $C_{(x_1,\ldots,x_l)}$ is sufficient for obtaining the value $\chi_1(\sum_{i=1}^{D} A_i \eta^{2^{s_i}+1} + b^{2^{\beta_1}} \eta) = \exp(\pi i C_{(x_1,\ldots,x_l)})$, rather than performing complex number calculation with $\exp(\frac{2\pi}{p} i Tr_p(X))$ as is in p odd prime. We can formulate the above Weil sum algorithm in the following.

Algorithm 2.3.3. *(Weil Sum Algorithm ($p = 2$)). Assume that a basis $\{\omega_1, \ldots, \omega_n\}$ of $F_{2^n} \cong F_2^n$ is available before computation.*

INPUT: $f(x) = \sum_{i=1}^{D} a_i x^{2^{\alpha_i}+2^{\beta_i}} + \sum_{i}^{L} b_i x^{2^{\gamma_i}}$ *: central polynomial in* $F_{2^n}[x]$.
OUTPUT: $|S|$*: the absolute value of Weil sum* S *of* $f(x)$.

1. *Compute the associated auxiliary linearized polynomial $T_D(x) \in F_{2^n}[x]$ as in Theorem 2.2.1 (Suppose the rank of the kernel is l).*
2. *Compute the basis $\{\eta_1, \ldots, \eta_l\}$ of $ker(T_D)$.*
3. *Let U be $0 \in Z$.*
4. *Compute $\gamma_{i,j_1,j_2} = Tr(A_i \eta_{j_1} \eta_{j_2}^{2^{s_i}})$ for $1 \le i \le D, 1 \le j_1, j_2 \le l$*

(5) *Compute* $\rho_j = Tr(b^{2^{\beta_1}}\eta_j)$ *for* $1 \le j \le l$.
(6) *For each* $(x_1, \dots, x_l) \in F_2^l$, *evaluate:*

$$C_{(x_1,\dots,x_l)} = \sum_{i=1}^{D}\sum_{j_1=1}^{l}\sum_{j_2=1}^{l} x_{j_1}x_{j_2}\gamma_{i,j_1,j_2} + \sum_{j=1}^{l} x_j\rho_j \in F_2$$

and set $U = U + C_{(x_1,\dots,x_l)}$. *(Note: integer addition.)*
(7) *Return* $2^{n/2}\sqrt{2^l - 2U}$.

Theorem 2.3.4. *(Validity and Complexity). The Weil sum algorithm in Algorithm 2.3.3 computes the absolute value* $|S|$ *of Weil sum* S *of the input central polynomial* $f(x) = \sum_{i=1}^{D} a_i x^{2^{\alpha_i}+2^{\beta_i}} + \sum_i^L b_i x^{2^{\gamma_i}}$ *in* $F_{2^n}[x]$ *in time:*

$$O(C_{DL}l^2(n^3 + 2^l)),$$

where l *is the dimension of the kernel of the auxiliary linearized polynomial* $T_D(x)$ *and* $C_{DL} = D + L$ *is the sparsity of* $f(x)$.

Proof. Suppose that the basic arithmetic operations for the elements in F_q costs $O(\log^2 q)$-time in RAM. When $q = 2^n$, it takes $O(n^2)$-time. The estimate of each step of the algorithm is:

(1) A_i is obtained from 2^{n-t_i}-th power of a_i, thus in $O(C_{DL}n^3)$ time.
(2) Performing Gaussian Elimination on B to obtain the basis $\{\eta_1, \dots, \eta_l\}$ takes $O(n^3)$ time.
(3) $O(1)$ time.
(4) Trace $Tr(x) = x + x^2 + \cdots + x^{2^{n-1}}$ has $n-1$ additions and $n-1$ squarings in F_{2^n} in $O(n^3)$ time. Thus, we have $Dl^2 \times O(n^3) = O(Dl^2n^3)$-time.
(5) $l \times O(n^3) = O(ln^3)$-time.
(6) $3 \times Dl^2 + 1 \times l + 1$ ops in F_2. So $O(2^l Dl^2)$-time.

Therefore we have:

$$O(C_{DL}l^2(n^3 + 2^l))\text{-time}.$$

The input size (number of bits required to represent f) is about $C_{DL}n\log p = C_{DL}n\log 2$ and clearly the complexity does not depend on the degree of $f(x)$ while it primarily depends on the dimension l of the kernel of $T_D(x)$ and the extension degree n of F_{2^n}. □

Note that Algorithm 2.3.3 does not resolve the *sign* of the Weil sum S since the return value is the absolute value $|S|$. As is stated in the beginning of this chapter, if central polynomial has a nonzero constant term, we can separately calculate the character value of the constant and multiply by it the result obtained from the Algorithm 2.3.3.

In practice, the dimension l of the kernel of the matrix B of $T_D(x)$ is usually small so that the parity checking Step (6) in Algorithm 2.3.3 can be feasible for randomly generated central polynomials with larger n of a cryptographic interest.

3. Conclusion

We developed parity checking-styled Weil sum Algorithm 2.3.3 which avoid the complex number calculation for finite fields of characteristic $p = 2$. The algorithm computes the absolute values of the Weil sums of the generic univariate polynomials which fully characterize MQ problem of n polynomials in n indeterminates over F_2.

The proof method in the simplification procedures of Theorem 2.1.1 is a natural extension of the combined results of Theorem 1.4. [14] and [3]. We showed that at the level of Weil sum values we can work on the simplified form of central polynomials in stead of dealing each coefficients appearing in the linearized terms of the central polynomials. The auxiliary linearized polynomial turns into the index set of partial Weil sum in Algorithm 2.3.3 whereby the dimension of its kernel dominates the time complexity of the algorithm.

For many of the randomly generated central polynomials and their auxiliary linearized polynomials, the kernels are often of dimension much smaller than the extension degree n. We do not claim that this algorithm is optimal. It remains an open question to improve the efficiency of the algorithm in addition to resolve the sign of the absolute values.

Acknowledgment. The results of this paper were obtained during my Ph.D. studies at Texas A&M University. I would like to express deep gratitude to my supervisor Dr. Donald K. Friesen whose guidance and support were crucial for the successful completion of this project.

References

1. Jiun-Ming Chen and Bo-Yin Yang, *A more secure and efficacious TTS signature scheme*, ICISC, Lecture Notes in Computer Science, vol. 3574, Springer, 2003, pp. 320–338.
2. Robert S. Coulter, *Explicit evaluations of some Weil sums*, Acta Arithmetica **83** (1998), 241–251.
3. ______, *Further evaluations of Weil sums*, Acta Arithmetica **86** (1998), 217–226.
4. ______, *On the evaluation of a class of Weil sums in characteristic 2*, NZ J. Mathematics **28** (1999), no. 2, 171–184.
5. Nicolas Courtois, Magnus Daum, and Patrick Felke, *On the security of HFE, HFEv- and Quartz*, Public Key Cryptography, Lecture Notes in Computer Science, vol. 2567, Springer, 2003, pp. 337–350.
6. Nicolas T. Courtois, *Short signatures, provable security, generic attacks and computational security of multivariate polynomial schemes such as HFE, Quartz and Sflash*, Cryptology ePrint Archive, Report 2004/143, 2004, http://eprint.iacr.org/.
7. Peter Dembowski and TG Ostrom, *Planes of order n with collineation groups of order n^2*, Math Z **103** (1968), 239–258.
8. Jintai Ding and Dieter Schmidt, *Cryptanalysis of HFEv and internal perturbation of HFE*, Public Key Cryptography, Lecture Notes in Computer Science, vol. 3386, Springer, 2005, pp. 288–301.
9. Michael R. Garey and David S. Johnson, *Computer and intractability: A guide to the theory of NP-completeness*, W. H. Freeman, 1979.
10. Louis Goubin and Nicolas Courtois, *Cryptanalysis of the TTM cryptosystem*, ASIACRYPT, Lecture Notes in Computer Science, vol. 1976, Springer, 2000, pp. 44–57.
11. Aviad Kipnis, Jacques Patarin, and Louis Goubin, *Unbalanced Oil and Vinegar signature schemes*, EUROCRYPT, Lecture Notes in Computer Science, vol. 1592, Springer, 1999, pp. 206–222.
12. Aviad Kipnis and Adi Shamir, *Cryptanalysis of the HFE public key cryptosystem by relinearization*, CRYPTO, Lecture Notes in Computer Science, vol. 1666, Springer, 1999, pp. 19–30.
13. Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.
14. Donald Mills, *On the evaluation of Weil sums of Dembowski-Ostrom polynomials*, Journal of Number Theory **92** (2002), no. 1, 87–98.
15. Jacques Patarin, *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two new families of asymmetric algorithms*, EUROCRYPT, Lecture Notes in Computer Science, vol. 1070, Springer.

16. Jacques Patarin, Louis Goubin, and Nicolas Courtois, *Improved algorithms for Isomorphisms of Polynomials*, EUROCRYPT, Lecture Notes in Computer Science, vol. 1403, Springer, 1998, pp. 184–200.
17. ———, $\mathcal{C}^*_{-+}$ *and HM: Variations around two schemes of T. Matsumoto and H. Imai*, ASIACRYPT, Lecture Notes in Computer Science, vol. 1514, Springer, 1998, pp. 35–49.

Department of Computer Science, Texas A&M University
E-mail address: harayama@tamu.edu