Recent attacks against HFE/Multi-HFE MQ cryptosystems and Connection with Ore's p-polynomial decomposition

Bilal Alam, Oğuz Yayla

***Abstract*—In this article we review some recent attacks against HFE and Multi-HFE cryptosystems and also a possible new direction proposed by Coulter et al. relating the security of HFE cryptosystems to the Ore's p-polynomial decomposition algorithm.**

***Index Terms*—HFE, multi-HFE, multivariate quadratic cryptosystems, Min-Rank problem, IP-problem, Ore's p-polynomial decomposition.**

I. Introduction

Hidden Field Equations (HFE) based Multivariate Quadratic (MQ) cryptosystems were proposed by Patarin [32] after he successfully attacked the MIA scheme [35]. HFE is a generalisation of the MIA scheme with the central trapdoor using a univariate quadratic polynomial over finite field $\mathbb{E}$ i.e. n degree extension of $\mathbb{F}$, instead of a monomial x^{q^h+1} used as a permutation map in MIA. There have been various practical attacks on this scheme, however some standard variations render those attacks in-efficient. Hence, we can consider HFE still a viable candidate with suitable parameter and variation choice. In this article, we review some recent cryptanalytic attacks on these HFE schemes and their relation to other mathematical problems.

The outline of the paper is as follows. In section II, we define HFE and multi-HFE multi-variate quadratic cryptosystems. Section III discusses some recent cryptanalytic structural attacks against HFE in which the problem is reduced to an instance of polynomial time solvable Min-Rank problem. In section IV, cryptanalytic attack by reduction to polynomial time solvable Isomorphism of Polynomials (IP) Problem is discussed. A new approach of analyzing the security of HFE while examining the significance of Ore's p-polynomial decompositions relevant to this case is discussed in section V followed by conclusion.

II. HFE and Multi-HFE

Patarin in [32] defined the basic HFE as follows.

Definition II.1. Let $\mathbb{F}$ be a finite field and $\mathbb{E}$ its n degree extension such that $|\mathbb{F}| := q$, then

$$P(X) = \sum_{0\leq i,j\leq D} A_{i,j} X^{q^i+q^j} + \sum_{0\leq k\leq D} B_k q^k + C \;\forall\; X \in \mathbb{E}$$

Bilal Alam and Oğuz Yayla: Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bul., No:1, 06800, Ankara, Turkey, e-posta: {e159447, yayla}@metu.edu.tr.

such that $q^i + q^j, q^k \leq D$ and co-efficients $A_{i,j}, B_i, C \in \mathbb{E}$ define the central quadratic polynomial map P for the HFE scheme. Using the canonical bijective map ϕ from $\mathbb{E}$ to $\mathbb{F}^n$ i.e. n-dimensional vector space over $\mathbb{F}$ and it's inverse we get the corresponding multivariate representation as $P' := \phi \circ P \circ \phi^{-1}(x)$ for $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$.

The degree of the polynomial P is upper bounded by D to allow efficient inversion of the equation $P(X) = Y$ for given $Y \in \mathbb{E}$. There are deterministic algorithms [32] for this inversion in time polynomial in D and the dimension n of extension field $\mathbb{E}$ over $\mathbb{F}$. HFE cryptosystems are susceptible to Gröbner bases attacks [20]. A thorough investigation of the Gröbner bases attack was given by Granboulan in [23] for HFE based MQ systems over finite fields of characteristic 2 and later by J.Ding and J.Hodges in [16] for those over finite fields of characteristic any prime p. The attack exploits the fact that the univariate equation in the extension field has a total degree that is much lower than the one for a randomly chosen equation. In order to improve upon this degree of the univariate polynomial representation over extension field $\mathbb{E}$, Patarin [2], [32] proposed a generalization of HFE that uses instead of a single univariate quadratic polynomial over extension field $\mathbb{E}$, a system of N quadratic polynomials in N variables over an extension field of degree d over $\mathbb{F}$. The basic HFE in Definition II.1 is an instance of Multi-HFE with $N = 1$, $d = n$.

Definition II.2. Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^d}$ its d degree extension. Let N be the number of variables and the number of secret quadratic polynomials in the polynomial ring $\mathbb{F}_{q^d}[X_1, \ldots, X_N]$ and D be their degree. Then the polynomial map $\mathcal{F} : (\mathbb{F}_{q^d})^N$ to $(\mathbb{F}_{q^d})^N$ given by

$$\mathcal{F} : (X_1, \ldots, X_N) \to (F_1(X_1, \ldots, X_N), \ldots, F_N(X_1, \ldots, X_N)$$

where

$$F_k = \sum_{1\leq i,j\leq N} \sum_{0\leq u,v<d} A_{k,i,j,u,v} X_i^{q^u} X_j^{q^v} + \sum_{1\leq i\leq N} \sum_{0\leq l<d} B_{k,i,l} X_i^{q^l} + C_k$$

such that $A_{k,i,j,u,v}, B_{k,i,u}, C_k \in \mathbb{F}_{q^d}$ for all $1 \leq i, j \leq N$, $0 \leq u, v, l < d$ and $q^l, q^u + q^v \leq D$ with $n = Nd$, defines the central quadratic polynomial map P for multi-HFE scheme.

III. Min-Rank Attacks against HFE

Min-Rank problem over finite field $\mathbb{F}$ is defined as

Definition III.1. Let $n, r, k \in \mathbb{N}$ and given matrices $M_0, M_1, \ldots, M_k \in \mathcal{M}_{n\times n}(\mathbb{F})$ where $\mathcal{M}_{n\times n}(\mathbb{F})$ denote the $n \times n$ matrices with co-efficients in $\mathbb{F}$. The (square) MinRank Problem relates to finding any k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}^k$ such that linear combination of the matrices M_i for $0 \leq i \leq k$ given as

$$\sum_{i=1}^{k} \lambda_i M_i - M_0$$

has rank $\leq r$.

A. Relinearization Attack

The attack was proposed by Kipnis and Shamir in [24] as the first key recover attack on the HFE systems. For private key central quadratic polynomial (cf. Definition II.1) over E i.e. n degree extension of finite field $\mathbb{F}$ given as

$$P(X) = \sum_{0\leq i\leq r-1} \sum_{0\leq j\leq r-1} p_{i,j} X^{q^i+q^j}$$

such that $q^i + q^j, q^k \leq D$ and co-efficients $p_{i,j} \in \mathbb{E}$, the corresponding public key polynomial map is $G(X) = \phi^{-1} \circ T \circ \phi \circ P \circ \phi^{-1} \circ S \circ \phi(X)$ with T, S as randomly chosen invertible linear transformations over $\mathbb{F}^n$. In matrix form over $\mathbb{E}$ this is equivalent to

$$G(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} g_{ij} X^{q^i+q^j} = \underline{X} G \underline{X}^t$$

with g_{ij} as the (i, j)-th entry and $\underline{X} = (X^{q^0}, X^{q^1}, \ldots, X^{q^{n-1}}) \in \mathbb{E}$ with $\underline{X}^t$ as its transpose. Thus, we can write

$$T^{-1}(G(X)) = \sum_{k=0}^{n-1} t_k \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (g_{i-k,j-k})^{q^k} X^{q^i+q^j}$$

and

$$P(S(X)) = \underline{X} W P W^t \underline{X}^t$$

where $P = [p_{ij}]$ and $W = [W_{ij}] = s_{j-i}^{q^i}$ are the matrices over $\mathbb{E}$. Let G^k denote the matrix over $\mathbb{E}$ obtained from G by raising all the entries of G to q^k-th power and cyclically rotating all rows and columns of G forward k times. Then $T^{-1}(G(X)) = \underline{X} G' \underline{X}^t$ where

$$G' = \sum_{k=0}^{n-1} t_k G^k = W P W^t \qquad \text{(III.1)}$$

The $n \times n$ matrix P can only have its top left $r \times r$ block as non-zero where $r << n$. Similarly the matrix $G' = WPW^t$ has each entry as the linear combination of the t_k variables. Thus, the rank of both P and G' cannot exceed r. The main principle of the attack is to express this rank condition of $r \approxeq log(D)$ as a large number of equations in small number of variables. Kipnis and Shamir observed that every correct choice for n variables $t_0, t_1, \ldots, t_{n-1}$ results in the rank of G' not more than r and any other random choice results in rank close to n.

Now, the matrix G can be easily obtained from the public key of the HFE cryptosystem and G^k is derived from G as explained earlier. Taking $t_0, t_1, \ldots, t_{n-1}$ as n variables and under the condition that its rank does not exceed r establishes the fact that its left kernel $\widetilde{X} : \widetilde{X} G' = 0$ is at least an $(n - r)$ dimensional vector subspace. Thus, there exist at least $\underbrace{n - r}$ linearly independent n-dimensional vectors $\widetilde{X_1}, \ldots, \widetilde{X_{n-r}}$ over $\mathbb{E}$ such that one can assign random values to their first $n-r$ entries still keeping them linearly independent. Assuming the remaining r entries as new variables overall we have $r(n-r)$ new variables added to the system. Each $\widetilde{X_i} G' = 0$ gives n scalar equations and in total, we have $n(n-r)$ equations in $n + r(n - r)$ variables. This gives an overdefined system of about n^2 equations in about rn variables where $r << n$ which is an instance of MinRank problem for a set of multivariate quadratic equations i.e.

$$\begin{pmatrix} 1 & & & X_{1,1} & \ldots & X_{1,r} \\ & \ddots & & \vdots & \ldots & \vdots \\ & & 1 & X_{n-r,1} & \ldots & X_{n-r,r} \end{pmatrix} \Big(\sum_{i=1}^{n} \lambda_i G^i - G^0 \Big) = 0_n$$

But these equations are quadratic and general technique to solve this system of equations by linearization is to replace any product of two variables $X_i X_j$ for $i \leq j$ by a new variable X_{ij} which are in total $n(n + 1)/2$. In general, the resultant system is no more overdefined and by normal linearization we are not expected to obtain a unique solution.

To filter the correct solutions from many parasitic solutions obtained by Gaussian elimination of linear system of equations obtained after linearization, Kipnis and Shamir performed the technique of relinearization. In relinearization technique, they add additional constraints to relate the new variable X_{ij} with each other and obtain additional equations. For example, in degree 4 relinearization any 4-tuple of indices $1 \leq i, j, k, l \leq m$, where m is the number of total variables, can be parenthesized as follows

$$(X_i X_j)(X_k X_l) = (X_i X_k)(X_j X_l) = (X_i X_l)(X_j X_k)$$
$$\Rightarrow X_{ij} X_{kl} = X_{ik} X_{jl} = X_{il} X_{jk}.$$

Hence, there are about $m^4/4!$ ways to choose 4-tuple of indices with each choice resulting in 2 quadratic equations in new variables introduced by re-linearization. Further optimization of the basic technique was also suggested by choosing degree 6 relinearization of indices and obtaining further set of equations. However in [6], it was pointed out by Curtois that degree 6 and higher relinearizations result in far less linearly independent equations and require far more computational power becoming less useful. The overall complexity of this attack was estimated by Curtois in [11] as $n^{log^2 d}$ where d is the degree of the central quadratic polynomial P over $\mathbb{E}$ of extension degree n.

B. Faugere Attack: Using Matrix/Vector Operations

To further improve the complexity of the attack in section III-A Faugere, Betttale and Perret [1] proposed to reduce this problem of computing Gröbner bases of a polynomial system to one with computations over smaller field $\mathbb{F}_q$ instead of $\mathbb{F}_{q^n}$. In order to achieve this they introduce the change of basis

matrix $M_n \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ where $\mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ is the set of $n \times n$ matrices with co-efficients in $\mathbb{F}_{q^n}$ such that

$$M_n = \begin{pmatrix} \theta_1 & \theta_1^q & \dots & \theta_1^{q^{n-1}} \\ \theta_2 & \theta_2^q & \dots & \theta_2^{q^{n-1}} \\ \vdots & & \ddots & \vdots \\ \theta_n & \theta_n^q & \dots & \theta_n^{q^{n-1}} \end{pmatrix}$$

and $(\theta_1, \dots, \theta_n) \in (\mathbb{F}_{q^n})^n$ is the vector basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Using M_n, one gets the following morphism $\phi_1 : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$

$$X \rightarrowtail (X, X^q, \dots, X^{q^{n-1}})M_n^{-1}$$

and its inverse $\phi_1^{-1} : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$

$$(x_1, \dots, x_n) \rightarrowtail ((x_1, \dots, x_n)M_n)[1]$$

where $((x_1, \dots, x_n)M_n)[1]$ denotes the first component of resultant vector $(x_1, \dots, x_n)M_n$. Using this change of basis matrix M_n, they obtained the following useful result.

Lemma III.2. *Let $M_n \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$. Let the symmetric matrices $(B_1, \dots, B_n) \in (\mathcal{M}_{n\times n}(\mathbb{F}_q))^n$ be associated to the multivariate secret central quadratic polynomials in the small field $(b_1, \dots, b_n) \in (\mathbb{F}_q[x_1, \dots, x_n])^n$ i.e. $b_i = \underline{x}B_i\underline{x}^t$ for $1 \le i \le n$. Then*

$$(B_1, \dots, B_n) = (M_nP^{*0}M_n^t, \dots, M_nP^{*n-1}M_n^t)M_n^{-1}$$

where $P = [p_{ij}] \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$ is the matrix associated to the univariate secret central quadratic polynomial in the big field

$$P(X) = \sum_{0\le i\le r-1} \sum_{0\le j\le r-1} p_{i,j}X^{q^i+q^j} \in \mathbb{F}_{q^n}[X]$$

and

$$P^{*k} = p_{(i-k) mod\, n,(j-k) mod\, n}^{q^k} \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})\ \forall k \in \mathbb{N}.$$

In order to relate the small field matrix representation of public key polynomial map in HFE to the big field matrix representation of private key, Lemma III.2 can be used. Let $G(\underline{x})$ and $(g_1(\underline{x}), \dots, g_n(\underline{x})$ be the univariate and multivariate small field representations of public key and $(b_1(\underline{x}), \dots, b_n(\underline{x}))$ as the corresponding multivariate small field representation of private key such that $\underline{x} = (x^{q^0}, x^{q^1}, \dots, x^{q^{n-1}})$ then we have

$$\begin{aligned} G(\underline{x}) &= T(P(S(\underline{x}))) \\ (g_1(\underline{x}), \dots, g_n(\underline{x})) &= (b_1(\underline{x}S), \dots, b_n(\underline{x}S))T \\ (\underline{x}G_1\underline{x}^t, \dots, \underline{x}G_n\underline{x}^t) &= (\underline{x}SB_1S^t\underline{x}^t, \dots, \underline{x}SB_nS^t\underline{x}^t)T \\ (G_1, \dots, G_n) &= (SB_1S^t, \dots, SB_nS^t)T \\ (G_1, \dots, G_n)U &= (WP^{*0}W^t, \dots, WP^{*n-1}W^t) \end{aligned}$$

for $T^{-1}M_n = U$ and $SM_n = W$ where the matrices $U = [u_{ij}], W = [w_{ij}] \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^n})$. Let $(u_{0,0}, \dots, u_{n-1,0}) \in (\mathbb{F}_{q^n})^n$ represent the first column of matrix U, then this can be expressed as:

$$\sum_{i=0}^{n-1} u_{i,0}G_{i+1} = WP^{*0}W^t = WPW^t.$$

As observed by Kipnis and Shamir, the rank of the matrices on right hand side of equations is $\log(D)$ where D is the degree bound of the secret central quadratic polynomial P. This equation is very similar to Kipnis and Shamir equation in (III.1). However, the co-efficients of the quadratic equations originating from equation (III-B) are in small field $\mathbb{F}_q$ unlike equation (III.1) where the co-efficients are in the big field $\mathbb{F}_{q^n}$. Hence, they obtained the following result.

Theorem III.3. *[1, Theorem 2] In HFE cryptosystems, the problem of key recovery reduces to solution of MinRank problem with $k = n$ and $r = \lceil \log_q(D) \rceil$ on the public matrices $(G_1, \dots, G_n) \in \mathcal{M}_{n\times n}(\mathbb{F}_q)^n$. The solutions of this MinRank are in $(\mathbb{F}_{q^n})^n$.*

From here on, the attack proceeds by computing the gröbner bases of the system of quadratic equations and then its variety. However, the cost of operations compared to Kipnis-Shamir attack is reduced by an expected factor equivalent to the cost of multiplication of two univariate polynomials of degree n over big field.

In multi-HFE cryptosystems (cf. Definition II.2) a multivariate quadratic system of polynomials is used as the secret central private key P rather than a single univariate polynomial as in HFE. For $n = Nd$, the general form of this polynomial map $P : (\mathbb{F}_{q^d})^N$ to $(\mathbb{F}_{q^d})^N$ for homogeneous system is as follows

$$P : (X_1, \dots, X_N) \to (P_1(X_1, \dots, X_N), \dots, P_N(X_1, \dots, X_N)$$

where

$$P_k = \sum_{1\le i,j\le N} \sum_{0\le u,v<d} A_{k,i,j,u,v}X_i^{q^u}X_j^{q^v}$$

such that $A_{k,i,j,u,v} \in \mathbb{F}_{q^d}$ for all $1 \le i, j \le N$, $0 \le u, v, l < d$ and $q^u + q^v \le D$. In order to extend the attack to multi-HFE case the change of basis matrix is generalised to the following form

$$M_{N,d} = \begin{pmatrix} \theta_1 & \theta_1^q & \dots & \theta_1^{q^{d-1}} & & & \\ \theta_2 & \theta_2^q & \dots & \theta_2^{q^{d-1}} & & & \\ \vdots & & \ddots & \vdots & & & \\ \theta_d & \theta_d^q & \dots & \theta_d^{q^{d-1}} & & 0 & \\ & & & & & & \\ & & \ddots & & & & \\ & & & & \theta_1 & \theta_1^q & \dots & \theta_1^{q^{d-1}} \\ & & & & \theta_2 & \theta_2^q & \dots & \theta_2^{q^{d-1}} \\ & 0 & & & \vdots & & \ddots & \vdots \\ & & & & \theta_d & \theta_d^q & \dots & \theta_d^{q^{d-1}} \end{pmatrix}$$

Using $M_{N,d}$, one gets the following morphism $\phi_N : (\mathbb{F}_{q^d})^N \to \mathbb{F}_{q^n}$

$$(X_1, \dots, X_N) \to (V_1, V_1^q, \dots, V_N^{q^{d-1}}, \dots, V_N, V_N^q, \dots, V_N^{q^{d-1}})M_{N,d}^{-1}$$

and its inverse $\phi_N^{-1} : \mathbb{F}_{q^n} \to (\mathbb{F}_{q^d})^N$

$$(x_1, \dots, x_n) \rightarrowtail (X_1, X_{d+1}, \dots, X_{d(N-1)+1}) = (x_1, \dots, x_n)M_{N,d}$$

Lemma III.2 can be generalized using these morphisms as

Lemma III.4. *Let $M_{N,d} \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^d})$. Let the symmetric matrices $(\mathbf{P_1},\ldots,\mathbf{P_N}) \in (\mathcal{M}_{n\times n}(\mathbb{F}_{q^d}))^n$ be associated to the multivariate secret central quadratic polynomials $(P_1,\ldots,P_N) \in (\mathbb{F}_{q^d}[x_1,\ldots,x_n])^N$ such that $P_i = \underline{X}\mathbf{P_i}\underline{X}^t$ where $\underline{X} = (X_1, X_1^q, \ldots, X_1^{q^{d-1}}, \ldots, X_N, X_N^q, \ldots, X_N^{q^{d-1}})$. Let ${\mathbf{P_i}}^{*d,k} \in \mathcal{M}_{n\times n}(\mathbb{F}_{q^d})$ be the matrix obtained from $\mathbf{P_i}$ by rotating the rows and columns of each $d\times d$ blocks by k positions and raising each entry in the matrix to the power q^k. Also, let the symmetric matrices $(B_1,\ldots,B_n) \in (\mathcal{M}_{n\times n}(\mathbb{F}_q))^n$ be associated to the multivariate secret central quadratic polynomials in the small field $(b_1,\ldots,b_n) \in (\mathbb{F}_q[x_1,\ldots,x_n])^n$ i.e. $b_i = \underline{x}B_i\underline{x}^t$ for $1\le i\le n$. Then*

$$\begin{aligned}(B_1,\ldots,B_n) = \\ (M_{N,d}{\mathbf{P_1}}^{*d,0}M_{N,d}^t,\ldots,M_{N,d}{\mathbf{P_1}}^{*d,d-1}M_{N,d}^t,\ldots\ldots \\ ,M_{N,d}{\mathbf{P_N}}^{*d,0}M_{N,d}^t,\ldots,M_{N,d}{\mathbf{P_N}}^{*d,d-1}M_{N,d}^t)M_{N,d}^{-1}.\end{aligned}$$

Thus, the relation among the small field public matrices $(G_1,\ldots,G_n) \in (\mathcal{M}_{n\times n}(\mathbb{F}_q))^n$ and the big field private matrices $(\mathbf{P_1},\ldots,\mathbf{P_N}) \in (\mathcal{M}_{n\times n}(\mathbb{F}_{q^d}))^N$ can be expressed using Lemma III.4 for multi-HFE systems using change of basis matrix $M_{N,d}$ as follows

$$\begin{aligned}(G_1,\ldots,G_n)T^{-1}M_{N,d} = \\ (SM_{N,d}{\mathbf{P_1}}^{*d,0}S^tM_{N,d}^t,\ldots,SM_{N,d}{\mathbf{P_1}}^{*d,d-1}S^tM_{N,d}^t,\ldots \\ ,SM_{N,d}{\mathbf{P_N}}^{*d,0}S^tM_{N,d}^t,\ldots,SM_{N,d}{\mathbf{P_N}}^{*d,d-1}S^tM_{N,d}^t) \\ (G_1,\ldots,G_n)U = \\ (W{\mathbf{P_1}}^{*d,0}W^t,\ldots,W{\mathbf{P_1}}^{*d,d-1}W^t,\ldots,W{\mathbf{P_N}}^{*d,0}W^t, \\ \ldots,W{\mathbf{P_N}}^{*d,d-1}W^t)\end{aligned}$$

where $U = T^{-1}M_{N,d}$ and $W = SM_{N,d}$. As a generalisation of MinRank problem in the HFE case this can be written as

$$\sum_{k=0}^{n-1} u_{k,0}G_{k+1} = W{\mathbf{P_1}}^{*d,0}W^t,$$

$$\ldots,\sum_{k=0}^{n-1} u_{k,0}G_{k+1} = W{\mathbf{P_N}}^{*d,0}W^t$$

The following result for multi-HFE is a generalization of Theorem III.3 in HFE case.

Theorem III.5. *[1, Theorem 2] In multi-HFE cryptosystems, the problem of key recovery reduces to solution of MinRank problem N times with $k = n$ and $r = N\lceil\log_q(D)\rceil$ on the public matrices $(G_1,\ldots,G_n) \in \mathcal{M}_{n\times n}(\mathbb{F}_q)^n$. The solutions of this MinRank are in $(\mathbb{F}_{q^d})$.*

IV. IP Attack against HFE

In general, to un-relate the IP problem from the secret key recovery in HFE, the central quadratic polynomial is kept secret in the design of HFE systems. However, Bouillaguet, Charles, et al in [4] proposed the framework under which equivalent polynomial P' of high degree can be used to recover the private key polynomial triple (S,P,T) by reducing the key recovery problem to an instance of IP problem. The concept of equivalent keys for multivariate public key cryptosystems has been discussed in detail in [39].

In [4], authors considered the usefulness of commutation of secret central polynomial with Frobenius map $F : X \to X^q$ over a finite field $\mathbb{F}$. They also observed that such property holds for certain instances of secret central polynomial $P(X) \in \mathbb{E}[X]$ of the form

$$P(X) = \sum_{0\le i,j\le D} Ai,jX^{q^i+q^j} + \sum_{0\le k\le D} B_kq^k + C\ \forall\ X \in \mathbb{E}$$

where $A_{i,j}, B_k, C \in \mathbb{F}$ such that $\mathbb{E}$ is the n-dimensional extension of $\mathbb{F}$. Equivalently if the secret central polynomial P can be written as the product of same element $\omega \in \mathbb{E}$ with some element of $\mathbb{F}$, then by employing the concept of equivalent keys, by considering equivalent affine transformations S', T' composed of original transformations S, T and the multiplication factor ω, the secret central polynomial can be considered as having co-efficients in $\mathbb{F}$. Such secret central polynomials P are observed to commute with Frobenius map F i.e.

$$P \circ F(X) = F \circ P(X).$$

Based on such commutation property, certain automorphisms among the public key $\mathcal{P} = T \circ P \circ S$ can be observed. Precisely, $\psi(F),\ldots,\psi(F^{n-1})$ are the only solutions of such automorphism where

$$\psi : F \rightarrowtail (T.F^{-1}.T^{-1}, S^{-1}.F.S)$$

such that

$$\mathcal{P} = (T \circ F^{-1} \circ T^{-1})^{-1} \circ \mathcal{P} \circ (S^{-1} \circ F \circ S).$$

We assume to have found such an automorphism $(V,W) = \psi(F^u)$ of the public key P for some $u \in [1, n-1]$. It is also observed [4, Preposition 3] that if $gcd(u,n) = 1$ (which holds if V and F are similar) then there exist equivalent linear transformations $\overline{S}, \overline{T} \in GL_n(\mathbb{F})$ such that $F = \overline{S} \circ W^k \circ \overline{S}^{-1}$ and $F = \overline{T}^{-1} \circ V^k \circ \overline{T}$ for $k := u^{-1} \bmod n$ and $\overline{S}.S^{-1}$ and $\overline{T}.T^{-1}$ commute with F. Also, in practice $\overline{S}, \overline{T}$ can be found efficiently using knowledge of u.

The relationship among $\overline{S}, \overline{T}$ and S, T can be used to neutralize the action of S, T on the public key $\mathcal{P}$. Considering the matrix representation of Frobenius map F it can be trivially observed that other matrices commuting with F over $\mathcal{M}_{n\times n}\mathbb{F}$ (set of $n\times n$ matrices over $\mathbb{F}$) form a vector space of dimension n generated by $(F^0, F, \ldots, F^{n-1})$. Hence, $F_1 = \overline{S}.S^{-1}$ and $F_2 = \overline{T}.T^{-1}$ are linear combinations of powers of F over $\mathbb{F}$. The composition of public key $\mathcal{P}$ as

$$\mathcal{P} = T \circ P \circ S$$

$$\overline{T}^{-1} \circ \mathcal{P} \circ \overline{S}^{-1} = F_2^{-1} \circ P \circ F_1^{-1}$$

results in the equivalent private key

$$P' = F_2^{-1} \circ P \circ F_1^{-1}.$$

Hence we get the following equations:

$$F_1(X) = \sum_{k=0}^{n-1} a_k X^{q^k} \qquad F_1^{-1} = \sum_{k=0}^{n-1} b_k X^{q^k}$$
$$F_2(X) = \sum_{k=0}^{n-1} c_k X^{q^k} \qquad F_2^{-1} = \sum_{k=0}^{n-1} d_k X^{q^k}$$
$$P'(X) = \sum_{0\le i,j\le D} A_{ij} X^{q^i+q^j} + \sum_{0\le i\le D} B_i X^{q^i} + C$$
$$P(X) = \sum_{0\le i,j\le D} e_{ij} X^{q^i+q^j} + \sum_{0\le i\le D} f_i X^{q^i} + g$$

with unknowns $a_k, b_k, c_k, d_k, e_{ij}, f_i, g$. Composing both sides of equation (IV) with F_1, we can write

$$F_1 \circ P' = F_2^{-1} \circ P.$$

This can be expressed as follows for left hand side

$$F_1 \circ P' = \sum_{0\le i,j\le D} A_{ij} (\sum_{k=0}^{n-1} a_k X^{q^k})^{q^i+q^j} + \sum_{0\le i\le D} B_i (\sum_{k=0}^{n-1} a_k X^{q^k})^{q^i} + C$$
$$= \sum_{i,j,k,l} A_{ij}.a_k.a_l.X^{q^{i+k}+q^{j+l}} + \sum_{i,k} B_i.a_k.X^{q^{i+k}} + C$$

and for right hand side

$$F_2^{-1} \circ P = \sum_{k=0}^{n-1} d_k (\sum_{0\le i,j\le D} e_{ij} X^{q^i+q^j} + \sum_{0\le i\le D} f_i X^{q^i} + g)^{q^k}$$
$$= \sum_{i,j,k} d_k.e_{ij}.X^{q^{i+k}+q^{j+k}} + \sum_{i,k} d_k.f_i.X^{q^{i+k}} + g.\sum_k d_k.$$

Finally, we have a system of $O(n^2)$ equations in $O(n + D^2)$ unknowns which is highly overdetermined system of equations and can be solved efficiently using fast Gröbner bases algorithms [19]. Based on their simulation results, authors in [4] also conjecture about the upper bound of complexity for their attack while using fast gröbner bases algorithm F_5 as $O(n^{21})$.

The attack returns the private key $(T, P, S) = (\overline{T}.F_2^{-1}, P, F_1^{-1}.\overline{S})$ using knowledge of public key $\mathcal{P}$ and determining an equivalent private polynomial P' but proceeds under the assumption that co-efficients of the actual central private polynomial P are in ground field $\mathbb{F}$ rather than $\mathbb{E}$ which is meaningful assumption by considering the concept of equivalent keys and sustaining transformation [39].

V. Ore's p-polynomials and security of HFE

Coulter, Havas and Henderson [7] gave an interesting insight into the security of HFE cryptosystems that have Dembowski Ostrom(DO) polynomials as the private key central polynomial. Their observation is based on the alternative definition of DO polynomials stated in [8] that establishes an important connection between p-polynomials and DO polynomials. Using this relation they propose a partial attack on HFE cryptosystems that tries to recover one of the secret linear map T in the private key tuple (S, P, T). Hence the corresponding pubic key $\mathcal{P} = T \circ P \circ S$ gets partially factored and the resultant (expected) low degree factors can be evaluated for their inverses using efficient root finding algorithm [36], [37]

HFE cryptosystem are designed by choosing a relatively low degree central polynomial P of the form

$$P(X) = \sum_{0\le i,j\le D} A_{ij} X^{q^i+q^j} \qquad \forall \quad X \in \mathbb{F}_q$$

where $A_{ij} \in \mathbb{F}_q$ i.e. n-degree extension of $\mathbb{F}_p$. Then this polynomial is mixed using right and left composition with two linear transformations S, T such that the resultant public key $\mathcal{P}$ is again a DO polynomial of reasonably high degree making it infeasible to compute the inverse. This was independently observed by Kipnis and Shamir [24] earlier and they also proved that any linear map can be expressed as a p-polynomial of the form

$$\sum_{i=0}^{n-1} a_i X^{p^i}.$$

It is not difficult to observe that DO polynomials are closed w.r.t left and right composition with p-polynomials. Hence the resultant public key $\mathcal{P}$ was proved [24] to have an equivalent univariate representation in the form of DO polynomial but it may have an exponential number of co-efficients and even if sparse it may have an exponentially high degree which makes inversion infeasible. However, being a DO polynomial it is bounded to have $O(n^2)$ terms.

Coulter et al.[7] observed that there could be a possible way to reduce the degree of this resultant public key $\mathcal{P}$. Their observation is based on the following result in [8].

Theorem V.1. *[7, Theorem 1][8, Theorem 3.2] For $f \in \mathbb{F}_q[X]$ with degree less than q the following statements are equivalent*

1) *f = DO + L_p where DO is a Dembowski Ostrom polynomial and L_p is p-polynomial.*
2) *The difference polynomial $\triangle_{f,a} = L_{p_a}$ for each $a \in \mathbb{F}_q^*$ where $\triangle_{f,a} := f(X+a) - f(X) - f(a)$ is the difference polynomial of f with respect to a and L_{p_a} is the p-polynomial depending on a.*

Considering the structure of public key $\mathcal{P} = T \circ P \circ S$, it can be considered as a left composition of $f = P \circ S$ (which is a DO polynomial itself) with T. The difference polynomial $\triangle_{\mathcal{P},a}$ can be evaluated as follows

$$\begin{aligned}\triangle_{\mathcal{P},a} &= \mathcal{P}(X+a) - \mathcal{P}(X) - \mathcal{P}(a)\\ &= T(f(X+a)) - T(f(X)) - T(f(a))\\ &= T(f(X+a) - f(X) - f(a))\\ &= T \circ \triangle_{f,a}\end{aligned}$$

$\triangle_{f,a}$ is a p-polynomial that follows from Theorem V.1 and $\triangle_{\mathcal{P},a}$ is a p-polynomial as p-polynomials are closed w.r.t polynomial composition [28]. Ore in [28] extending his work in [29] on non-commutative polynomial rings described the algorithm to compute left and right decompositional factors of p-polynomials. In [7] authors suggested to use Ore's ideas to develop a variant of famous Euclidean algorithm [26] and evaluate Greatest Common Left Decompositional Factor (GCLDF) of the p-polynomial composition. Their proposed attack on HFE cryptosystems works as follows

1) Randomly choose distinct $a_1, a_2 \in \mathbb{F}_q^*$.
2) Calculate $L(X) = GCLDF(\triangle_{\mathcal{P},a_1}, \triangle_{\mathcal{P},a_2})$.
3) Check whether L is the left decompositional factor of $\mathcal{P}$ i.e $L(X) = T(X)$. If this holds then we are done. This can be checked with complexity $O(\log_p(deg(\mathcal{P})))$ where $deg(\mathcal{P})$ is the degree of public key DO polynomial [7].
4) If L is not the left decompositional factor of $\mathcal{P}$ then choose a different $a \in \mathbb{F}_q^*$ and calculate $L(X) = GCLDF(L(X), \triangle_{\mathcal{P},a})$. Re-evaluate (3).

Since Ore's arguments are restricted to non-commutative rings and p-polynomials and not applicable directly on the DO polynomials, hence it is not possible to use them and compute $GCLDF(L(X), \mathcal{P}(X))$ to obtain T [7]. It was also observed that Giesbrecht algorithm in [22] cannot be used to obtain the left decompositional factor of public key polynomial $\mathcal{P}$ though it does claim to provide a probabilistic polynomial time algorithm to determine complete decomposition of p-polynomial. Based on Ritt's theorem [40] many such decompositions exist that have equivalent factors permuted and the resultant factors from Giesbrecht's algorithm may not all fall on the left. Finally the evaluation in (3) may not be successful as the difference polynomial $\triangle_{\mathcal{P},a}$ may or may not have a non-trivial left decompositional factor and the resultant factors may still have reasonably high degree making inversion infeasible.

Though the attack seems probabilistic in nature but it would be interesting to perform some simulations on practical HFE parameters and evaluate success probability of the stated attack for such parameters.

VI. Conclusion

In this article, we review few recent attacks against HFE and Multi-HFE MQ cryptosystems and review possible new direction proposed by Coulter et al.[7] that can be pursued in order to reassess the NP-hardness of the MQ-problem in general. Also certain simulation results can be obtained for practical parameters of HFE cryptosystems in order to prove the validity of the relation among decomposition of Ore's p-polynomial and security of HFE cryptosystems.

References

[1] Bettale, Luk, Faugére, Jean-Charles, and Ludovic Perret. *Cryptanalysis of HFE, multi-HFE and Variants for Odd and Even Characteristic*. Designs, Codes and Cryptography (2012): 1-52.

[2] Billet, Olivier, J. Patarin, and Yannick Seurin. *Analysis of intermediate field systems*. Proceedings of the First International Conference on Symbolic Computation and Cryptography, Beijing, China. 2008.

[3] Blake, Ian F. *Applications of finite fields.* Ed. Alfred J. Menezes. Vol. 199. Springer, 1993.

[4] Bouillaguet, C., Fouque, P. A., Joux, A., Treger, J. *A family of weak keys in HFE and the corresponding practical key-recovery.* Journal of Mathematical Cryptology, 5(3-4), (2012), 247-275.

[5] Chen, C. H. O., Chen, M. S., Ding, J., Werner, F., Yang, B. Y. *Odd-Char Multivariate Hidden Field Equations.* IACR Cryptology ePrint Archive, 2008, 543

[6] Courtois, N., Klimov, A., Patarin, J., Shamir, A. *Efficient algorithms for solving overdefined systems of multivariate polynomial equations.* In Advances in CryptologyEUROCRYPT 2000 (2000, January), (pp. 392-407). Springer Berlin Heidelberg.

[7] Coulter, Robert S., George Havas, and Marie Henderson. *Giesbrecht's algorithm, the HFE cryptosystem, and Ore's ps-polynomials*. Lecture Notes Series of Computing 9 (2001): 36-45.

[8] Coulter, Robert S., and Rex W. Matthews. *Planar functions and planes of Lenz-Barlotti class II*. Designs, Codes and Cryptography 10.2 (1997): 167-184.

[9] Courtois, Nicolas T. *Efficient zero-knowledge authentication based on a linear algebra problem MinRank*. Advances in Cryptology - ASIACRYPT 2001. Springer Berlin Heidelberg, 2001. 402-421.

[10] Courtois, Nicolas T., Magnus Daum, and Patrick Felke. *On the security of HFE, HFEv-and Quartz*. Public Key Cryptography - PKC 2003. Springer Berlin Heidelberg, 2002. 337 - 350.

[11] Courtois, Nicolas T. *The security of hidden field equations (HFE)*. Topics in Cryptology - CT - RSA 2001. Springer Berlin Heidelberg, 2001. 266 - 281.

[12] Courtois, Nicolas T. *Decoding Linear and Rank-Distance Codes, MinRank problem and Multivariate Cryptanalysis*. (2006).

[13] Cox, David A., John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Vol. 10. Springer Verlag, 2007.

[14] Ding, Jintai, Dieter Schmidt, and Fabian Werner. *Algebraic attack on HFE revisited*. Information Security. Springer Berlin Heidelberg, 2008. 215-227.

[15] Ding, Jintai, and Bo-Yin Yang. *Multivariate public key cryptography*. Post-Quantum Cryptography. Springer Berlin Heidelberg, 2009. 193-241.

[16] Ding, Jintai, and Timothy J. Hodges. *Inverting HFE systems is quasi-polynomial for all fields*. Advances in Cryptology - CRYPTO 2011. Springer Berlin Heidelberg, 2011. 724-742.

[17] Ding, Jintai, and Dieter Schmidt. *Cryptanalysis of HFEv and internal perturbation of HFE*. Public Key Cryptography-PKC 2005. Springer Berlin Heidelberg, 2005. 288-301.

[18] Faugére, Jean-Charles, Françoise Levy-Dit-Vehel, and Ludovic Perret. *Cryptanalysis of minrank*. Advances in Cryptology - CRYPTO 2008. Springer Berlin Heidelberg, 2008. 280-296.

[19] Faugére, Jean-Charles. *A new efficient algorithm for computing Gröbner bases without reduction to zero F5*. Proceedings of the 2002 international symposium on Symbolic and algebraic computation. ACM, 2002.

[20] Faugére, Jean-Charles, and Antoine Joux. *Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases*. Advances in Cryptology - CRYPTO 2003, Lecture Notes in Computer Science, vol. 2729, pp. 44 - 60. Springer, Berlin (2003).

[21] Faugére, Jean-Charles, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. *Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): Algorithms and complexity.* Journal of Symbolic Computation 46.4 (2011): 406-437.

[22] Giesbrecht, Mark. *Factoring in skew-polynomial rings over finite fields*. Journal of Symbolic Computation 26.4 (1998): 463-486.

[23] Granboulan, Louis, Antoine Joux, and Jacques Stern. *Inverting HFE is quasipolynomial*. Advances in Cryptology - CRYPTO 2006. Springer Berlin Heidelberg, 2006. 345-356.

[24] Kipnis, Aviad, and Adi Shamir. *Cryptanalysis of the HFE public key cryptosystem by relinearization*. Advances in cryptology - CRYPTO 99. Springer Berlin Heidelberg, 1999.

[25] Kipnis, Aviad, Jacques Patarin, and Louis Goubin. *Unbalanced oil and vinegar signature schemes*. Advances in Cryptology - EUROCRYPT 99. Springer Berlin Heidelberg, 1999.

[26] Lidl, Rudolf, Harald Niederreiter, and P. M. Cohn, *Finite Fields, second edition, Encyclopedia Math. Applications* Vol 20. Cambridge University Press. Cambridge 1997.

[27] Matsumoto, Tsutomu, and Hideki Imai. *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*. Advances in Cryptology - EUROCRYPT 88. Springer Berlin Heidelberg, 1988.

[28] Ore, Oystein. *On a special class of polynomials*. Transactions of the American Mathematical Society 35.3 (1933): 559-584.

[29] Ore, Oystein. *Theory of non-commutative polynomials*. The Annals of Mathematics 34.3 (1933): 480-508.

[30] Patarin, Jacques. *Asymmetric cryptography with a hidden monomial*. Advances in Cryptology - CRYPTO 96. Springer Berlin Heidelberg, 1996.

[31] Patarin, Jacques, and Louis Goubin. *Trapdoor one-way permutations and multivariate polynomials*. Information and Communications Security (1997): 356-368.

[32] Patarin, Jacques. *Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms*. In Advances in Cryptology - EUROCRYPT 1996, volume 1070 of Lecture Notes in Computer Science, pages 33 - 48. Ueli Maurer, editor, Springer, 1996.

[33] Patarin, Jacques, and Louis Goubin. *Trapdoor one-way permutations and multivariate polynomials*. Information and Communications Security (1997): 356-368.

[34] Patarin, Jacques. *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'98*. Designs, codes and cryptography 20.2 (2000): 175 - 209.

[35] Patarin, Jacques. *The oil and vinegar signature scheme* Dagstuhl Workshop on Cryptography, September 1997.

[36] Van Oorschot, Paul C., and Scott A. Vanstone. *A geometric approach to root finding in* $GF(q^m)$. Information Theory, IEEE Transactions on 35.2 (1989): 444-453.

[37] Von Zur Gathen, Joachim, and Victor Shoup. *Computing Frobenius maps and factoring polynomials*. Computational complexity 2.3 (1992): 187-224.

[38] Wolf, Christopher. *Multivariate quadratic polynomials in public key cryptography*. PhD thesis, Department Electrical Engineering, Katholieke Universiteit Leuven, 2005.

[39] Wolf, Christopher, and Bart Preneel. *Equivalent keys in Multivariate quadratic public key systems*. Journal of Mathematical Cryptology 4.4 (2011): 375-415.

[40] Ritt, Joseph Fels. *Prime and composite polynomials*. Transactions of the American Mathematical Society 23.1 (1922): 51-66.

[41] Shamir, Adi. *Efficient signature schemes based on birational permutations*. Advances in Cryptology CRYPTO 93. Springer Berlin Heidelberg, 1994.