Dimension of the Linearization Equations of the Matsumoto-Imai Cryptosystems

Adama Diene*, Jintai Ding, Jason E. Gower,
Timothy J. Hodges, and Zhijun Yin

Department of Mathematical Sciences
University of Cincinnati
Cincinnati, OH 45221-0025, USA
adiene@centralstate.edu, ding@math.uc.edu, gowerj@math.uc.edu,
timothy.hodges@uc.edu, yinzhi@math.uc.edu

Abstract. The Matsumoto-Imai (MI) cryptosystem was the first multivariate public key cryptosystem proposed for practical use. Though MI is now considered insecure due to Patarin's linearization attack, the core idea of MI has been used to construct many variants such as Sflash, which has recently been accepted for use in the New European Schemes for Signatures, Integrity, and Encryption project. Linearization attacks take advantage of the algebraic structure of MI to produce a set of equations that can be used to recover the plaintext from a given ciphertext. In our paper, we present a solution to the problem of finding the dimension of the space of linearization equations, a measure of how much work the attack will require.

1 Introduction

In the last two decades, public key cryptography has become an indispensable part of most modern communication systems. However, due to the threat that quantum computers pose to cryptosystems based on "hard" number theory problems, there has recently been great effort put into the search for alternative public key cryptosystems. Multivariate cryptosystems provide a promising alternative since solving a set of multivariate polynomial equations over a finite field appears to be difficult, analogous to integer factorization, though it is unknown precisely how difficult either problem is.

One of the first implementations of a multivariate public key cryptosystem was suggested by Matsumoto and Imai [8]. Fixing a finite field k of characteristic two and cardinality 2^q, they suggested using a bijective map M defined over K, a degree n extension of k. By identifying K with k^n, we see that M induces a multivariate polynomial map $\tilde{M}$. We can "hide" this map by composing on the left by L_1 and on the right by L_2, where the $L_i : k^n \longrightarrow k^n$ are invertible affine linear maps. This gives a map $\bar{M} : k^n \longrightarrow k^n$ defined by

$$\bar{M}\left(x_1, \ldots, x_n\right) = L_1 \circ \tilde{M} \circ L_2\left(x_1, \ldots, x_n\right) = \left(y_1, \ldots, y_n\right).$$

* *Current address*: Department of Mathematics and Computer Science, Central State University, Wilberforce, OH 45384.

Ø. Ytrehus (Ed.): WCC 2005, LNCS 3969, pp. 242–251, 2006.

The map originally suggested by Matsumoto and Imai is the map

$$M : X \longmapsto X^{1+2^{q\theta}},$$

where $\gcd(2^{q\theta}+1, 2^{qn}-1) = 1$. The resulting system is the Matsumoto-Imai (C^* or MI) cryptosystem. The public key for MI is the system of n quadratic polynomials $y_1, \ldots, y_n$.

Even for a large finite field K, MI is efficient. Unfortunately this scheme was proven insecure under an algebraic attack [9] that produces so-called "linearization equations." These linearization equations can be swiftly generated from the public key and known plaintext/ciphertext pairs, and have the form:

$$\sum a_{ij} x_i y_j + \sum b_i x_i + \sum c_j y_j + d = 0,$$

where $x_1, \ldots, x_n$ are the plaintext variables corresponding to the ciphertext variables $y_1, \ldots, y_n$. Once we have found enough of these equations, and hence the a_{ij}, b_i, c_j and d, we can substitute in the ciphertext to produce a system of linear equations in the plaintext variables. Patarin showed that there are enough linearization equations to produce enough linearly independent linear equations in the plaintext variables, which can then be used to find the plaintext.

After introducing his linearization attack, Patarin posed the general question of how we can find the maximum number of linearly independent linearization equations for MI. The answer to this question is necessary for a complete understanding of both MI and the linearization attack, and may provide valuable insight into related systems derived from MI, such as the Sflash signature schemes [1, 2], PMI and PMI+ [3, 4], HFE [10] and others. In this paper, we use the method developed in [6] to attack the HFE cryptosystem (another generalization of MI), to find the exact dimension of the space of linearization equations.

The complete result, given in Theorems 2 and 3, involves a number of exceptional cases. Let us summarize here the result ignoring the case $n = 2\theta$, which has no cryptographic applications, and some exceptional cases when n is $2, 3$ or 6. Let δ be the dimension of the space of linearization equations. If $q > 1$, then

$$\delta = \begin{cases} \frac{2n}{3}, & \text{if } \theta = n/3 \text{ or } 2n/3; \\ n, & \text{otherwise.} \end{cases}$$

On the other hand, if $q = 1$,

$$\delta = \begin{cases} \frac{2n}{3}, & \text{if } \theta = n/3 \text{ or } 2n/3; \\ 2n, & \text{if } \theta = 1, n-1 \text{ or } (n \pm 1)/2; \\ \frac{3n}{2}, & \text{if } n = 2\theta \pm 2; \\ n, & \text{otherwise.} \end{cases}$$

Computer simulations for the cases $n \leq 15$ have confirmed these results.

Before getting into the technical details we outline the idea of the proof. Let $X \in K$ and let $Y = X^{2^{q\theta}+1}$. Then $Y^{2^{q\theta}-1} = X^{(2^{q\theta}+1)(2^{q\theta}-1)}$. Multiplying each

side by XY, we obtain $Y^{2^{q\theta}}X = YX^{2^{2q\theta}}$. Since K has characteristic two, $Y^{2^{q\theta}}$ and $X^{2^{2q\theta}}$ are linear functions of Y and X respectively. This equation is thus a version of a linearization equation for K. Using the identification of K with k^n and looking at coordinate components yields a set of n (not necessarily independent) linearization equations in the above sense. Moreover, for any integer $m = 0, 1, \ldots, n-1$, we further have

$$(XY^{2^{q\theta}} - YX^{2^{2q\theta}})^{2^{qm}} = 0.$$

Looking at coordinate components yields further linearization equations. When $q > 1$, it turns out that all linearization equations arise in this way. When $q = 1$, there are additional identities that arise for certain exceptional values of θ. For instance, if $\theta = 1$, then $XY = X^4$.

The proof proceeds in the following way. We first define a notion of linearization equation for K and use a simple algebraic trick (exactness of the tensor product) to show that the dimension of the space of linearization equations is the same over both k and K. We then show that the equations above span all possible linearization equations for K and count carefully the dimension of this space.

Note that we only need to do this calculation for M. The composition with the invertible affine linear maps L_i does not affect the dimension of the associated space of linearizations equations.

2 The Linearization Problem

We begin by placing the problem in a general context. Let V be a vector space over k and denote by $\mathrm{Fun}(V, V)$ the set of functions from V to V. If V is the plaintext/ciphertext space of a cryptosystem, then a cipher is an element $M \in \mathrm{Fun}(V, V)$.

More generally, for any pair of sets V and W, denote by $\mathrm{Fun}(V, W)$, the set of all functions from V to W. Define a function

$$\psi_M : \mathrm{Fun}(V \times V, k) \to \mathrm{Fun}(V, k)$$

by

$$\psi_M(f)(v) = f(v, Mv).$$

Recall that for any pair of vector spaces V and W, the set $\mathrm{Fun}(V, W)$ is again a vector space in the usual way:

$$(\lambda f)(v) = \lambda f(V), \qquad (f + g)(v) = f(v) + g(v).$$

Thus both $\mathrm{Fun}(V \times V, k)$ and $\mathrm{Fun}(V, k)$ are vector spaces. It is easily checked that ψ_M is a linear transformation between these spaces. Denote by $\mathcal{A}(V)$ the subspace of $\mathrm{Fun}(V, k)$ consisting of affine linear functions (polynomials of degree less than or equal to one). Note that there is a natural embedding of $\mathcal{A}(V) \otimes \mathcal{A}(V)$ into $\mathrm{Fun}(V \times V, k)$ given by $(f \otimes g)(v, v') = f(v)g(v')$.

Definition 1. *The subspace* $\mathcal{L}_M = \ker \psi_M|_{\mathcal{A}(V)\otimes\mathcal{A}(V)}$ *is defined to be the space of* linearization equations *associated to* M.

Let's see how this definition ties up with the usual definition of linearization equation. Let $\{f_i \mid i = 0, 1, \ldots, n-1\}$ be a basis for the dual space V^*. Then $\mathcal{A}(V)$ has a basis consisting of the f_i and the constant function 1. So the $(n+1)^2$ elements $f_i \otimes f_j$, $f_i \otimes 1$, $1 \otimes f_j$, $1 \otimes 1$ form a basis for $\mathcal{A}(V) \otimes \mathcal{A}(V)$ and an arbitrary element of $\mathcal{A}(V) \otimes \mathcal{A}(V)$ is a bi-affine linear function of the form:

$$\eta = \sum a_{ij}(f_i \otimes f_j) + \sum b_i(f_i \otimes 1) + \sum c_j(1 \otimes f_j) + d(1 \otimes 1).$$

Let $x \in V$ have coordinates $x_i = f_i(x)$ and let $y = M(x)$ have coordinates $y_i = f_i(y)$. Thus $\eta \in \mathcal{L}_M$ if and only if for all $x \in V$,

$$\psi_M(\eta)(x) = \sum a_{ij}x_iy_j + \sum b_ix_i + \sum c_jy_j + d = 0.$$

That is, $\eta \in \mathcal{L}_M$ if and only if $\psi_M(\eta)(x) = 0$ is a linearization equation in the usual sense.

We are now in a position to state the problem that we solve in this article.

Linearization problem. Let q be a positive integer, let k be a finite field of order 2^q, and let K be an extension field of k with $[K : k] = n$. Let θ be an integer such that $1 \leq \theta < n$, and let $M\colon K \to K$ be the map $M(X) = X^{1+2^{q\theta}}$. Find $\dim \mathcal{L}_M$, the dimension of the space of linearization equations associated to M.

Note that the condition $\gcd(2^{q\theta}+1, 2^{qn}-1) = 1$ is required in the MI cryptosystem, though this assumption is not needed in order to calculate the dimension of $\mathcal{L}_M$.

3 Lifting to K

In order to simplify the calculations, we work inside the larger algebra $\mathrm{Fun}(K \times K, K)$ which we can realize as a homomorphic image of the polynomial ring $K[X, Y]$. Let us recall some general facts about this algebra. Since K is finite of cardinality 2^{qn}, the natural homomorphism $K[X] \to \mathrm{Fun}(K, K)$ is surjective and its kernel is the ideal $(X^{2^{qn}} - X)$. Similarly, the natural homomorphism $K[X, Y] \to \mathrm{Fun}(K \times K, K)$ is also surjective and has kernel $(X^{2^{qn}} - X, Y^{2^{qn}} - Y)$. Let G be the Galois group $\mathrm{Gal}(K, k)$. One of the key observations used in [6], is the following standard result from Galois theory (see for instance [5, Theorem 2]).

Lemma 1. *Denote by* $Fun_k(K, K) \subset Fun(K, K)$ *the subspace of* k*-linear endomorphisms of* K*. Then* $Fun_k(K, K)$ *is naturally isomorphic as a vector space to the group algebra* KG*.*

Similarly the subset of linear functions $\mathrm{Fun}_k(K \times K, K) \subset \mathrm{Fun}(K \times K, K)$ can be identified with $K(G \times G)$. The group G is cyclic, generated by the polynomial

function X^{2^q}. The space of affine linear functions from $K \times K$ to K can be viewed, by extension of coefficients, as $K \otimes \mathcal{A}(K) \otimes \mathcal{A}(K)$. From the above discussion, the elements of $K \otimes \mathcal{A}(K) \otimes \mathcal{A}(K)$, viewed as polynomial functions, have the form

$$\sum_{i,j=0}^{n-1} A_{ij} \otimes X^{2^{qi}} \otimes X^{2^{qj}} + \sum_{i=0}^{n-1} B_i \otimes X^{2^{qi}} \otimes 1 + \sum_{j=0}^{n-1} C_j \otimes 1 \otimes X^{2^{qj}} + D \otimes 1 \otimes 1,$$

for some $A_{ij}, B_i, C_j, D \in K$. As above, for any $M \in \mathrm{Fun}(K, K)$, we may define a map $\hat{\psi}_M : \mathrm{Fun}(K \times K, K) \to \mathrm{Fun}(K, K)$ by $\hat{\psi}_M(f)(x) = f(x, M(x))$. Set $\hat{\mathcal{L}}_M = \ker \hat{\psi}_M|_{K \otimes \mathcal{A}(K) \otimes \mathcal{A}(K)}$. This yields the following exact commutative diagram:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathcal{L}_M & \longrightarrow & \mathcal{A}(K) \otimes \mathcal{A}(K) & \xrightarrow{\psi_M} & \mathrm{Fun}(K, k) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \hat{\mathcal{L}}_M & \longrightarrow & K \otimes \mathcal{A}(K) \otimes \mathcal{A}(K) & \xrightarrow{\hat{\psi}_M} & \mathrm{Fun}(K, K)
\end{array}$$

Observe that the bottom line is the image of the top line under the exact functor $K \otimes -$. For $\mathrm{Fun}(K, K)$ is naturally isomorphic to $K \otimes \mathrm{Fun}(K, k)$ and under this identification $\hat{\psi}_M$ identifies with $K \otimes \psi_M$, the image of ψ_M under the functor $K \otimes -$. The exactness of $K \otimes -$ implies that $\ker(K \otimes \psi_M) \cong K \otimes \ker(\psi_M)$ (see, for instance [7]); so $\hat{\mathcal{L}}_M \cong K \otimes \mathcal{L}_M$. Hence $\dim_k \mathcal{L}_M = \dim_K \hat{\mathcal{L}}_M$.

4 Statement of Main Theorems

To find the dimension of the space of linearization equations we must find the dimension of the kernel of the map

$$\hat{\psi}_M \colon K \otimes \mathcal{A}(K) \otimes \mathcal{A}(K) \to \mathrm{Fun}(K, K).$$

This amounts to finding linearly independent identities of the form

$$\sum_{i,j=0}^{n-1} A_{ij} X^{2^{qi}} Y^{2^{qj}} + \sum_{i=0}^{n-1} B_i X^{2^{qi}} + \sum_{j=0}^{n-1} C_j Y^{2^{qj}} + D = 0,$$

where $Y = X^{2^{q\theta}+1}$, $X^{2^n} = X$ and $Y^{2^n} = Y$ and $A_{ij}, B_i, C_j, D \in K$. As noted above, it is easy to see that $Y = X^{2^{q\theta}+1}$ implies that $Y^{2^{q\theta}} X = Y X^{2^{2q\theta}}$ and hence more generally that

$$(XY^{2^{q\theta}} - YX^{2^{2q\theta}})^{2^{qm}} = 0,$$

for $m = 0, \ldots, n-1$. Generically these will be distinct identities. However, if $n = 3\theta$ or $3\theta/2$, the identities $XY^{2^{q\theta}} - YX^{2^{2q\theta}}$, $X^{2^{q\theta}} Y^{2^{2q\theta}} - Y^{2^{q\theta}} X$, and $X^{2^{2q\theta}} Y - Y^{2^{2q\theta}} X^{2^{q\theta}}$ are evidently dependent, yielding only $2n/3$ independent

identities. The case $n = 2\theta$ is an exceptional, highly degenerate case. In this situation, $Y^{2^{q\theta}} = Y$, yielding $(n^2 + n)/2$ identities of the form

$$(Y^{2^{q\theta+l}} - Y^{2^{ql}})X^{2^{qm}} = 0,$$

for $l = 0, \ldots n/2 - 1$ and $m = 0, \ldots n - 1$.

When $q > 1$, these identities are independent and span the set of all identities.

Theorem 2. *If $q > 1$, then the dimension of the space of linearization equations is given by*

$$\dim \hat{\mathcal{L}}_M = \begin{cases} 2n/3, & \text{if } \theta = n/3 \text{ or } 2n/3; \\ (n^2 + n)/2, & \text{if } \theta = n/2; \\ n, & \text{otherwise.} \end{cases}$$

When $q = 1$, further identities occur for special values of θ.

- When $\theta = 1$, $XY = XX^{2+1} = X^4$ yielding n identities of the form $(XY - X^4)^{2^m} = 0$ for $m = 0, \ldots, n - 1$.
- When $\theta = n - 1$, $Y^2 = (X^{2^{n-1}+1})^2 = X^{2^n} X^2 = X^3$, yielding n identities of the form $(XY^2 - X^4)^{2^m} = 0$ for $m = 0, \ldots, n - 1$.
- When $n = 2\theta + 1$, $Y^{2^{\theta+1}} = (X^{2^\theta+1})^{2^{\theta+1}} = X^{2^{2\theta+1}+2^{\theta+1}} = X^{2^{\theta+1}+1} = YX^{2^\theta}$ yielding n identities of the form $(YX^{2^\theta} - Y^{2^{\theta+1}})^{2^m} = 0$ for $m = 0, \ldots, n-1$.
- When $n = 2\theta - 1$, $Y^{2^\theta} = (X^{2^\theta+1})^{2^\theta} = X^{2^{2\theta}+2^\theta} = X^{2\theta}(X^{2^{2\theta-1}})^2 = X^{2\theta}X^2 = XY$, yielding n identities of the form $(Y^{2^\theta} - XY)^{2^m} = 0$ for for $m = 0, \ldots, n-1$.
- When $n = 2\theta + 2$, $Y^{2^{\theta+2}}X = X^{2^{2\theta+2}+2^{\theta+2}+1} = X^{2^{\theta+2}+2} = X^{2^{\theta+1}}Y^2$, yielding $n/2$ identities of the form $(Y^{2^{\theta+2}}X - X^{2^{\theta+1}}Y^2)^{2^m} = 0$ for $m = 0, \ldots, n/2 - 1$.
- When $n = 2\theta - 2$, $Y^{2^{\theta-1}}X^{2^{\theta-1}} = (X^{2^\theta+1})^{2^{\theta-1}}X^{2^{\theta-1}} = X^{2^{2\theta-1}+2^\theta} = X^{2+2^\theta} = XY$, yielding $n/2$ identities of the form $(Y^{2^{\theta-1}}X^{2^{\theta-1}} - XY)^{2^m}$ for $m = 0, \ldots, n/2 - 1$.

Again these turn out to be all identities and they are linearly independent.

Theorem 3. *If $q = 1$, the dimension of the space of linearization equations is as follows. When $\theta = n/3$ or $2n/3$,*

$$\dim \hat{\mathcal{L}}_M = \begin{cases} 7, & \text{if } n = 6,\ \theta = 2 \text{ or } 4; \\ 8, & \text{if } n = 3,\ \theta = 1 \text{ or } 2; \\ \frac{2n}{3}, & \text{otherwise.} \end{cases}$$

When $\theta = n/2$,

$$\dim \hat{\mathcal{L}}_M = \begin{cases} 5, & \text{if } n = 2,\ \theta = 1; \\ (n^2 + n)/2, & \text{otherwise.} \end{cases}$$

When $\theta \neq n/3, 2n/3, n/2$,

$$\dim \hat{\mathcal{L}}_M = \begin{cases} 10, & \text{if } n = 4 \text{ and } \theta = 1 \text{ or } 3; \\ 2n, & \text{if } \theta = 1, n-1 \text{ or } (n \pm 1)/2; \\ \frac{3n}{2}, & \text{if } \theta = n/2 \pm 1; \\ n, & \text{otherwise.} \end{cases}$$

5 Proofs of Main Theorems

An arbitrary element of $K \otimes \mathcal{A}(K) \otimes \mathcal{A}(K)$ is of the form

$$\sum_{i,j=0}^{n-1} A_{ij} \otimes X^{2^{qi}} \otimes X^{2^{qj}} + \sum_{i=0}^{n-1} B_i \otimes X^{2^{qi}} \otimes 1 + \sum_{j=0}^{n-1} C_j \otimes 1 \otimes X^{2^{qj}} + D \otimes 1 \otimes 1$$

and its image under $\hat{\psi}_M$ is

$$\sum_{i,j=0}^{n-1} A_{ij} X^{2^{qi}} (X^{2^{q\theta}+1})^{2^{qj}} + \sum_{i=0}^{n-1} B_i X^{2^{qi}} + \sum_{j=0}^{n-1} C_j (X^{2^{q\theta}+1})^{2^{qj}} + D,$$

where because of the relation $(X^{2^{qn}} - X)$ in $\mathrm{Fun}(K, K)$, we may consider the exponents as elements of $\mathbb{Z}_{2^{qn}-1}$. If such a polynomial is in the kernel, its constant term must be zero, so it suffices to look at terms of the form

$$\sum_{i,j=0}^{n-1} A_{ij} \otimes X^{2^{qi}} \otimes X^{2^{qj}} + \sum_{i=0}^{n-1} B_i \otimes X^{2^{qi}} \otimes 1 + \sum_{j=0}^{n-1} C_j \otimes 1 \otimes X^{2^{qj}}.$$

Lemma 4. *Let* $\mathcal{M} = \{X^{2^{qi}} \otimes X^{2^{qj}}, X^{2^{qi}} \otimes 1, 1 \otimes X^{2^{qj}} \mid i, j = 0, \ldots n-1\}$. *Then* $\dim \hat{\mathcal{L}}_M = n^2 + 2n - |\hat{\psi}_M(\mathcal{M})|$.

Proof. Let $\mathcal{N} = \{X^{2^{qi}} \mid i = 0, \ldots n-1\}$. Then $\mathcal{N} \cup \{1\}$ forms a basis for $K \otimes \mathcal{A}(K)$ and $\mathcal{M} \cup \{1 \otimes 1\}$ forms a basis for $K \otimes \mathcal{A}(K) \otimes \mathcal{A}(K)$. It is clear from the defintion of $\hat{\psi}_M$ that $\hat{\psi}_M(1 \otimes 1) = 1$ and that $\hat{\psi}_M(\mathcal{M}) \subset \mathcal{N}$. Hence

$$\mathrm{rank}(\hat{\psi}_M) = |\hat{\psi}_M(\mathcal{M} \cup \{1 \otimes 1\})| = |\hat{\psi}_M(\mathcal{M})| + 1$$

Hence

$$\begin{aligned} \dim \hat{\mathcal{L}}_M &= \dim(K \otimes \mathcal{A}(K) \otimes \mathcal{A}(K)) - \mathrm{rank}(\hat{\psi}_M) \\ &= (n+1)^2 - |\hat{\psi}_M(\mathcal{M})| + 1 \\ &= n^2 + 2n - |\hat{\psi}_M(\mathcal{M})| \end{aligned}$$

Thus the problem reduces to the calculation of $|\hat{\psi}_M(\mathcal{M})|$. In the case $q > 1$, this calculation is fairly straightforward, but when $q = 1$, it is a little more intricate.

We can reset the problem in the following way. Define $\mathbb{Z}_n^1$ and $\mathbb{Z}_n^2$ to be two copies of $\mathbb{Z}_n$. Define

$$\phi : (\mathbb{Z}_n \times \mathbb{Z}_n) \cup \mathbb{Z}_n^1 \cup \mathbb{Z}_n^2 \to \mathbb{Z}_{2^{qn}-1}$$

by

$$\begin{aligned}
&\phi(i,j) = 2^{qi} + 2^{qj} + 2^{q(\theta+j)}, \text{ for } (i,j) \in (\mathbb{Z}_n \times \mathbb{Z}_n) \\
&\phi(k) = 2^{qk} \text{ for } k \in \mathbb{Z}_n^1 \\
&\phi(l) = 2^{ql} + 2^{q(\theta+l)} \text{ for } l \in \mathbb{Z}_n^2
\end{aligned}$$

Clearly $|\hat{\psi}_M(\mathcal{M})| = |\text{Im } \phi|$.

The elements of $\mathbb{Z}_{2^{qn}-1}$ can be represented uniquely in a 2^q-ary expansion of length less than or equal to n. It is convenient to represent this expansion as a circular graph with n vertices representing the place holders and the digits of the expansion as labels on these vertices. For example in the case when $n = 8$, the element 02100301 is represented by the labelled graph in figure 1.

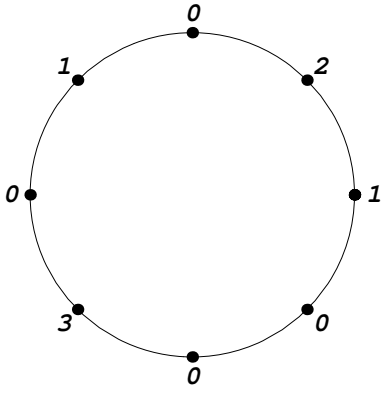

Fig. 1. The representation of the number with 2^q-ary expansion 02100301

Theorem 5. *If $q > 1$, then*

$$|Im\ \phi| = \begin{cases} n^2 + 4n/3, & \text{if } n = 3\theta,\ 3\theta/2; \\ (n^2 + 3n)/2, & \text{if } n = 2\theta; \\ n^2 + n, & \text{otherwise.} \end{cases}$$

Proof. The elements of Im ϕ considered as diagrams consist of

1. diagrams with all labels 0 except one label of 1
2. diagrams with all labels 0 except two labels of 1, spaced θ apart.
3. diagrams with all labels 0 except one label of 1 and one label of 2, spaced θ apart.
4. diagrams with all labels 0 except three labels of 1, of which at least one pair is spaced θ apart.

There are n diagrams of type (1). There are n diagrams of type (2) except if $n = 2\theta$ in which case there are only $n/2$ diagrams. There are $2n$ diagrams of type (3), unless $n = 2\theta$, in which case there are only n diagrams.

Consider diagrams of type (4). Consider first diagrams with exactly one pair of labeled vertices spaced θ apart and assume that $n \neq 2\theta$. For each such pair, there are $n-4$ possible locations for the third labeled vertex if $n \not\equiv 3\theta$ and $n-3$ locations if $n \equiv 3\theta$. Thus there are $n(n-4)$ and $n(n-3)$ total such diagrams respectively. If $n = 2\theta$, there are $n/2$ such pairs and $n-2$ locations for the third vertex, so there are $n(n-2)/2$ diagrams.

If n does not divide 3θ and $n \neq 2\theta$, then we can have exactly two pairs of vertices spaced by θ. There are n such diagrams. If $n|3\theta$, we can have all three vertices spaced by θ and there are $n/3$ of these diagrams.

Thus when $n = 2\theta$, $|\text{Im } \phi| = n + n/2 + n + n(n-2)/2 = (n^2 + 3n)/2$. When $3\theta \equiv 0 \pmod{n}$, $|\text{Im } \phi| = n + n + 2n + (n^2 - 3n) + n/3 = n^2 + 4n/3$. Otherwise $|\text{Im } \phi| = n + n + 2n + (n^2 - 4n) + n = n^2 + n$.

Theorem 6. *Suppose that $q = 1$. If $3\theta \equiv 0 \pmod{n}$, then*

$$|Im\ \phi| = \begin{cases} 41, & \text{if } n = 6,\ \theta = 2 \text{ or } 4; \\ 7, & \text{if } n = 3,\ \theta = 1 \text{ or } 2; \\ n^2 + \frac{4n}{3}, & \text{otherwise.} \end{cases}$$

If $2\theta = n$, then

$$|Im\ \phi| = \begin{cases} 3, & \text{if } n = 2; \\ (n^2 + 3n)/2, & \text{otherwise.} \end{cases}$$

Otherwise,

$$|Im\ \phi| = \begin{cases} 14, & \text{if } n = 4 \text{ and } \theta = 1 \text{ or } 3; \\ n^2, & \text{if } \theta = 1; \\ n^2, & \text{if } \theta > 1 \text{ and } n = 2\theta \pm 1 \text{ or } \theta + 1; \\ n^2 + \frac{n}{2}, & \text{if } n = 2\theta \pm 2; \\ n^2 + n, & \text{otherwise.} \end{cases}$$

Proof. The elements of Im ϕ considered as diagrams consist of essentially the same cases as in the previous proof except that a vertex with a label of 2 transforms into the next vertex moving clockwise around the diagram, labeled with a 1. Thus the possible configurations are now:

1. diagrams with all labels 0 except one label of 1
2. diagrams with all labels 0 except two labels of 1, spaced θ, $\theta - 1$ or $\theta + 1$ apart.
3. diagrams with all labels 0 except three labels of 1, of which at least one pair is spaced θ apart.

The counting of diagrams of type (1) and (3) is the same as in above. Similarly for the diagrams of type (2) spaced θ apart there are again n of these if $n \neq 2\theta$

and $n/2$ if $n = 2\theta$. In the generic case there are an additional n digrams with each of the other two spacing options. However, there are now a number of exceptional cases when a pair of θ, $\theta - 1$ or $\theta + 1$ coincide, or one of them equals $n/2$.

If $\theta = 1$, then the $\theta - 1$ spacing does not occur and when $\theta = n - 1$, the $\theta + 1$ spacing does not occur.

If $n = 2\theta + 2$, then $\theta + 1$ is $n/2$ so there are only $n/2$ diagrams with this spacing. So there are $5n/2$ diagrams of type (2) in total. Similarly, if $n = 2\theta - 2$.

If $n = 2\theta \pm 1$, then the three spacing options become only two and there are $2n$ diagrams of type (2).

The numbers stated in the result are then obtained by adding up the number of diagrams of each type as in the previous proof.

Subtracting these numbers from $n^2 + 2n$ yields the dimension of the space of linearization equations given in the previous section.

References

1. M.-L. Akkar, N. T. Courtois, R. Duteuil and L. Goubin. A Fast and Secure Implementation of Sflash. In *PKC 2003*, LNCS 2567:267–278.
2. N. Courtois, L. Goubin, and J. Patarin. FLASH, a Fast Multivariate Signature Algorithm. In *CT-RSA 2001*, LNCS 2020:298–307.
3. J. Ding. A New Variant of the Matsumoto-Imai Cryptosystem Through Perturbation. In *PKC 2004*, LNCS 2947:305–318.
4. J. Ding and J. E. Gower, Innoculating Multivariate Schemes against Differential Attacks, in Cryptology ePrint archive, report 2005/255`http://eprint.iacr.org/`, 2005.
5. N. Jacobson. *Lectures in Abstract Algebra III*, Springer-Verlag, 1964.
6. A. Kipnis and A. Shamir. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In *Crypto 1999*, LNCS 1666:19–30.
7. S. Lang. *Algebra*, Springer-Verlag, 2002.
8. T. Matsumoto and H. Imai. Public Quadratic Polynomial-tuples for Efficient Signature-verification and Message-encryption. In *Eurocrypt 1988*, LNCS 330: 419–453.
9. J. Patarin. Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In *Crypto 1995*, LNCS 963:248–261.
10. J. Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In *Eurocrypt 1996*, LNCS 1070: 33–48.