

## Simple Matrix Scheme for Encryption

Adama Diene (United Arab Emirates University)

Chengdong Tao (South China University of Technology)  
Jintai Ding (University of Cincinnati)

March 03, 2013

# Some Motivations to study MPKC

- MPKQ are Good Candidates for Post Quantum Cryptography (PQC)
- MPKQ are Much More Computationally Efficient than Number Theoric based Schemes

# Some of the Main Problems associated to MPKQ

- Size of their Keys: The size of MPKQ are usually very big compare to other types of schemes. But lately some improvement to reduced them were proposed
- Insecurity: In recent years, several MPKCs were proposed and most of them end up being insecure
- The Main Defect for insecurity for most of these MPKQ is that some Quadratic Forms associated with their central maps are of Low Rank.

# Some Examples of Schemes with the Low Rank Problem.

- The Matsumoto-Imai Scheme ( $MI$  or  $C^*$ ): initially broken by Pattarin using Linearization Equations. But Ding and et. have also shown that  $C^*$  has some quadratic form associated with the central map which has only Rank 2.
- Hidden Field Equation ( $HFE$ ): was proposed by Pattarin. But Kipnis and Shamir found a way to recover the key with the help of the MinRank Attack.
- TTM scheme: proposed by T. T. Mon but broken after by Courtois and Goubin who exploited the fact that some quadratic form associated with the central map has low rank.

# Illustration of the MinRank Attack with HFE

Let  $p$  is a prime,  $q = p^e$  and  $k = F_q$  be a finite field with  $q$  elements. Let  $K$  be  $n$  degree extension of  $k$ , then  $K \cong k^n$ , where  $k^n$  is the  $n$  dimension vector space over  $k$ .

Let  $\phi : K \rightarrow k^n$  be the isomorphism map and its inverse be  $\phi^{-1}$ .

The central map of HFE is a univariate polynomial  $P(x)$  over  $K$  of the form

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

where  $p_{ij} \in K$  and  $r$  is a small constant such that  $P(x)$  can be inverted efficiently. Let

$$\bar{F} = T \circ \phi \circ P \circ \phi^{-1} \circ S,$$

where  $T, S$  are two invertible affine transformations over  $k^n$ . Then the public key is  $\bar{F}$ , which are  $n$  quadratic polynomials. The private key are  $T, P, S$ .

# Illustration of the MinRank Attack with HFE

Kipnis and Shamir showed that the public key  $\bar{F}$  and the transformations  $S, T, T^{-1}$  can be viewed as maps  $G^*, S^*, T^*, T^{*-1}$  over  $K$  with

$$S^*(x) = \sum_{i=0}^{n-1} s_i x^{q^i}, \quad T^{*-1}(x) = \sum_{i=0}^{n-1} t_i x^{q^i}.$$

Thus  $G^*(x) = T^*(P(S^*(x)))$ . Write  $G^*(x)$  as the following form:

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

where  $\underline{x} = (x, x^q, \dots, x^{q^{n-1}})$  is a vector over  $K$ ,  $\underline{x}^t$  is the transformation of  $\underline{x}$  and  $G = [g_{ij}]$  is a matrix over  $K$ .

# Illustration of the MinRank Attack with HFE

Therefore, the identity  $T^{*-1}(G^*(x)) = P(S^*(x))$  implies that

$$G' = \sum_{i=0}^{n-1} t_k G^{*k} = WPW^t.$$

where  $G^{*k}$  is the matrix over  $K$  whose  $(i, j)$  entry is  $g_{i-k, j-k}^{q^k}$ ,  $i - k$  and  $j - k$  are computed modulo  $n$ ,  $W$  is a matrix over  $K$  whose  $(i, j)$  entry is  $s_{i-j}^{q^i}$ ,  $i - j$  is computed modulo  $n$ , and  $P = [p_{ij}]$  is a matrix over  $K$ .

# Illustration of the MinRank Attack with HFE

Since the rank of  $WPW^t$  is not more than  $r$ , recovering  $t_0, t_1, \dots, t_{n-1}$  can be reduced to solve a MinRank problem, that is, to find  $t_0, t_1, \dots, t_{n-1}$  such that

$$\text{Rank}\left(\sum_{i=0}^{n-1} t_k G^{*k}\right) \leq r.$$

If we find the values  $t_0, t_1, \dots, t_{n-1}$ , we can easily recover  $T$  and  $S$ .

Therefore, the key point is to solve the MinRank problem. Since  $r$  is small, we can solve the MinRank problem by known methods.



# Illustration of the MinRank Attack with HFE

- The Kipnis-Shamir attack was improved by Courtois using a different methods to solve the MinRank problem.
- Ding et al. showed that the original Kipnis-Shamir attack and the improvement of Courtois are not valid in [4].
- Faugère et al. proposed later a valid improvement of Kipnis-Shamir attack against HFE in [2].

# Motivation of the New proposed MPKQ

The main motivation of this work is to:

- Design a scheme such that all Quadratic forms associated with the central map have relatively high Rank.
- Design a scheme that can resist all known attacks if parameters are chosen properly.

## Main Idea

Create some Matrices having high rank and use some Simple Matrix Multiplication to get a Multivariate Publick Key Scheme that we denote in short by the SM cryptosystem.

# Construction of the SM Cryptosystem

Let  $k = F_q$  be a finite field with  $q$  elements and  $p$  be the characteristic of  $k$ .

Let  $n, m$  be a integer, where  $n = s^2, m = 2n$ .

We denote by  $k^n$  the set of all  $n$ -tuples of elements of  $k$  and by  $k^m$  the set of all  $m$ -tuples of elements of  $k$ .

The plaintext will be represented by  $(x_1, x_2, \dots, x_n) \in k^n$ .

The ciphertext will be represented by  $(y_1, y_2, \dots, y_m) \in k^m$ .

# Construction of the SM Cryptosystem

Let  $k[x_1, x_2, \dots, x_n]$  be a polynomial ring with  $n$  variables in  $k$ .

Let  $\mathcal{L}_1 : k^n \rightarrow k^n$  and  $\mathcal{L}_2 : k^m \rightarrow k^m$  be 2 affine transformations,

i.e.  $\mathcal{L}_1(x) = L_1x + u$  and  $\mathcal{L}_2(y) = L_2y + v$

where  $L_1$  and  $L_2$  are respectively an  $n \times n$  and  $m \times m$  matrix with entries in  $k$ ,  $x = (x_1, x_2, \dots, x_n)^t$ ,  $u = (u_1, u_2, \dots, u_n)^t$ ,  $y = (y_1, y_2, \dots, y_m)^t$ ,  $v = (v_1, v_2, \dots, v_m)^t$  and  $t$  denotes the transpose of matrix.



# Construction of the SM Cryptosystem

## Central map

Let

$$A = \begin{pmatrix} x_1 & x_2 & \cdots & x_s \\ x_{s+1} & x_{s+2} & \cdots & x_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ x_{(s-1)s+1} & x_{(s-1)s+2} & \cdots & x_{s^2} \end{pmatrix},$$

$$B = \begin{pmatrix} b_1 & b_2 & \cdots & b_s \\ b_{s+1} & b_{s+2} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{(s-1)s+1} & b_{(s-1)s+2} & \cdots & b_{s^2} \end{pmatrix} \quad \text{and}$$

$$C = \begin{pmatrix} c_1 & c_2 & \cdots & c_s \\ c_{s+1} & c_{s+2} & \cdots & c_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ c_{(s-1)s+1} & c_{(s-1)s+2} & \cdots & c_{s^2} \end{pmatrix}$$

# Construction of the SM Cryptosystem

## Central map

$A$ ,  $B$ , and  $C$  defined above are  $3 \times s$  matrices with  $x_i \in k$  ( $i = 1, 2, \dots, n$ ),  $b_i$  and  $c_i$  ( $i = 1, 2, \dots, n$ ) are chosen randomly from the set  $\{x_1, x_2, \dots, x_n\}$ .

$$\text{Let } E_1 = AB, \quad E_2 = AC,$$

we denote by  $f_{(i-1)s+j} \in k[x_1, x_2, \dots, x_n]$

the  $(i, j)$  element of  $E_1$  ( $i, j = 1, 2, \dots, s$ ).

and

$$f_{s^2+(i-1)s+j} \in k[x_1, x_2, \dots, x_n]$$

the  $(i, j)$  element of  $E_2$  ( $i, j = 1, 2, \dots, s$ ).



# Construction of the SM Cryptosystem

## Central map

With the notation above, we obtain  $m$  polynomials  $f_1, f_2, \dots, f_m$

We define then

$$\mathcal{F}(x_1, x_2, \dots, x_n) = (f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_m(x_1, x_2, \dots, x_n))$$

and

$$\bar{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1 = (\bar{f}_1, \bar{f}_2, \dots, \bar{f}_m),$$

### Secret Key:

The secret key is made of the following two parts:

- 1) The invertible affine transformations  $\mathcal{L}_1, \mathcal{L}_2$ .
- 2) The matrices  $B, C$ .

# FrameConstruction of the SM Cryptosystem Title

## Key

### Public Key

The public key is made of the following two parts:

1) The field  $k$ , including the additive and multiplicative structure;

2) The maps  $\bar{\mathcal{F}}$ , equivalently, its  $m$  total degree two components

$$\bar{f}_1(x_1, x_2, \dots, x_m), \bar{f}_2(x_1, x_2, \dots, x_n), \dots, \bar{f}_m(x_1, x_2, \dots, x_n) \in$$

$$k[x_1, x_2, \dots, x_n].$$

## Encryption

Given a message  $x_1, x_2, \dots, x_n$ , the corresponding ciphertext is:

$$(y_1, y_2, \dots, y_m) = \tilde{\mathcal{F}}(x_1, x_2, \dots, x_n).$$

## Decryption

Given the ciphertext  $(y_1, y_2, \dots, y_m)$ , decryption includes the following steps:

1) Compute  $(y'_1, y'_2, \dots, y'_m) = \mathcal{L}_2^{-1}(y_1, y_2, \dots, y_m)$ .

2) Let

$$E_1 = \begin{pmatrix} y'_1 & y'_2 & \cdots & y'_s \\ y'_{s+1} & y'_{s+2} & \cdots & y'_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ y'_{(s-1)s+1} & y'_{(s-1)s+2} & \cdots & y'_{s^2} \end{pmatrix},$$

$$E_2 = \begin{pmatrix} y'_{s^2+1} & y'_{s^2+2} & \cdots & y'_{s^2+s} \\ y'_{s^2+s+1} & y'_{s^2+s+2} & \cdots & y'_{s^2+2s} \\ \vdots & \vdots & \ddots & \vdots \\ y'_{s^2+(s-1)s+1} & y'_{s^2+(s-1)s+2} & \cdots & y'_{2s^2} \end{pmatrix}.$$

# Decryption

Since  $E_1 = AB$ ,  $E_2 = AC$  and set  $A$  is an  $s \times s$  nonsingular matrix, we consider the following cases:

(i) If  $E_1$  is invertible, then  $BE_1^{-1}E_2 = C$ . We have  $n$  linear equations with  $n$  unknowns  $x_i, i = 1, 2, \dots, n$ .

(ii) If  $E_2$  is invertible, but  $E_1$  is not invertible, then  $CE_2^{-1}E_1 = B$ . We also have  $n$  linear equations with  $n$  unknowns  $x_i, i = 1, 2, \dots, n$ .

(iii) If both  $E_1$  and  $E_2$  are not invertible, then  $A^{-1}E_1 = B, A^{-1}E_2 = C$ . We interpret the elements of  $A^{-1}$  as the new variables, then we have  $m$  linear equations with  $m$  unknowns.

We note that, if  $A$  is a singular matrix, we may decrypt failure. The probability of  $A$  is invertible is  $(1 - \frac{1}{q})(1 - \frac{1}{q^2}) \cdots (1 - \frac{1}{q^n})$ . Therefore, the probability of decryption failure is  $1 - (1 - \frac{1}{q})(1 - \frac{1}{q^2}) \cdots (1 - \frac{1}{q^n}) \approx \frac{1}{q}$ .

# A Practical Implementation

For a practical implementation, we let  $k = GF(q)$  be a finite field of  $q = 127$  elements and  $n = 64$ . In this case, the plaintext consist of the message  $(x_1, x_2, \dots, x_{64}) \in k^{64}$ . The public map is  $\bar{F} : k^{64} \rightarrow k^{128}$  and the central map is  $F : k^{64} \rightarrow k^{128}$ .

The public key consists of 128 quadratic polynomials with 64 variables. The number of coefficients for the public key polynomials is  $128 \times 64 \times 65/2 = 266,240$ , or about *2MB* of storage.

The private key consists of two matrices  $B, C$  and two affine linear transformations  $\mathcal{L}_1, \mathcal{L}_2$ . The total size is about *162.5KB*.

The size of document is  $8n = 8 \times 64 = 512$  bits. The total size of the ciphertext is *1024bits*.



# Security Analysis

## High order linearization equation attack

Since  $BE_1^{-1}E_2 = C$  or  $CE_2^{-1}E_1 = B$ ,

If  $BE_1^{-1}E_2 = C$  then there exist polynomials  $g_1, \deg(g_1) \leq s$ , such that

$$Bg_1(E_1)E_2 = C \det(E_1)$$

Thus we have linearization equation with order  $n + 1$ . Specifically, the plaintext and the ciphertext satisfy the following equation:

$$\sum_{i_0=1}^n \sum_{i_1, \dots, i_s=1}^m \mu_{i_0, i_1, \dots, i_s} x_{i_0} y_{i_1} \cdots y_{i_s} + \sum_{i_0=1}^n \sum_{i_1, \dots, i_{s-1}=1}^m \nu_{i_0, i_1, \dots, i_{s-1}} x_{i_0} y_{i_1} \cdots y_{i_{s-1}} + \dots + \sum_{i_0=1}^n \gamma_{i_0} x_{i_0} + \sum_{i_1=1}^m \zeta_{i_1} y_{i_1} + \theta = 0.$$

We treat the coefficients  $\mu_{i_0, i_1, \dots, i_s}, \nu_{i_0, i_1, \dots, i_{s-1}}, \dots, \gamma_{i_0}, \zeta_{i_1}, \theta$  as variables taking value in  $k$ .

# Security Analysis

## High order linearization equation attack

The number of variables in the above equation is

$$n \sum_{j=0}^s \binom{m}{j} + m + 1 = n \binom{m+s}{s} + m + 1.$$

Using the public key we can generate many plaintext-ciphertext pairs. By substituting these plaintext-ciphertext pairs to the equations, we have  $n \binom{m+s}{s} + m + 1$  linear equations in  $n \binom{m+s}{s} + m + 1$  variables.

However, the computation complexity of solving this linearization equation is  $(n \binom{m+s}{s} + m + 1)^\omega$ , where  $\omega = 3$  in the usual Gaussian elimination algorithm and  $\omega = 2.3766$  in

improved algorithm. Therefore, security level for the implementation proposed in section 4 is about  $2^{108}$ .

# Security Analysis

## Rank attack

For the 2 rank attacks, we have:

- The complexity of MinRank attack against our scheme is  $O(q^{\lceil \frac{m}{n} \rceil 2^s m^3})$ . Therefore, security level for the implementation proposed in section 4 is larger than  $2^{240}$ .
- For the High Rank Attack. We will need about  $O(n^6 q^{2s})$  field multiplications, and the security level require is about  $2^{140}$  wich is less than the security level of the proposed implementation.

In fact, since the rank of  $Q_i$  is associate with  $2\sqrt{n}$ , the complexity of the rank attack may not be polynomial time. Therefore, the rank attack is not applicable for our scheme.

# Security Analysis

## Algebraic Attack

Let  $\bar{f}_1(x_1, x_2, \dots, x_n), \bar{f}_2(x_1, x_2, \dots, x_n), \dots, \bar{f}_m(x_1, x_2, \dots, x_n)$  be the public key and  $y_1, y_2, \dots, y_m$  be the ciphertext. We obtain the system

$$\begin{cases} \bar{f}_1(x_1, x_2, \dots, x_n) = y_1 \\ \bar{f}_2(x_1, x_2, \dots, x_n) = y_2 \\ \dots\dots\dots \\ \bar{f}_m(x_1, x_2, \dots, x_n) = y_m \end{cases}$$

For  $k = GF(3)$ , we obtain the following results with a direct attack using MAGAMA(2.12-16) on a 1.80GHz Intel(R) Atom(TM) CPU

$n$	9	16	25
time(s)	0.016	3.494	17588.380
memory(MB)	3.4	8.1	1111.7
degree of regularity	4	5	6

We can notice that the degree of regularity increases with  $n$  which tells us that the time and memory complexity are exponential.

# Efficiency of SM scheme

A comparison with HFE challenge 1 by Patarin shows that

For HFE with  $q = 2, n = 80$ , the degree of central map is 96. The authors estimated that the complexity of solving  $P(x) = y$  over the finite field  $2^{80}$  is about  $O(d^2 n^3)$  or  $O(dn^3 + d^3 n^2)$ —depending on the chosen algorithms, where  $d$  is the degree of  $P(x)$ .

Thus the decryption process needs about  $6.4 \times 10^9$  times field multiplication over the finite field  $GF(2^{80})$ .

For the SM scheme with  $q = 127, n = 64, m = 128$ , the steps of decryption presented earlier need only about  $128^3 = 2^{21} \approx 2.1 \times 10^6$  times field multiplication over the finite field  $GF(127)$ .

We propose here a new multivariate algorithm for encryption called SM  
wich has the follow properties with some well chosen parameters:

- can resist to all known attack.
- all the quadratic forms associate with the central map are not of low rank but related to some variable integer  $n$ .
- computation of decryption is very fast.

THANK YOU