Simple Matrix Scheme for Encryption

Chengdong Tao[1], Adama Diene[2], Shaohua Tang[3], and Jintai Ding[4,⋆]

[1] South China University of Technology, China
chengdongtao2010@gmail.com
[2] Department of Math. Sciences, UAE University - Al-Ain, United Arab Emirates
adiene@uaeu.ac.ae
[3] South China University of Technology, China
csshtang@gmail.com
[4] University of Cincinnati, Ohio, USA and ChongQing University,China
jintai.ding@gmail.com

Abstract. There are several attempts to build asymmetric pubic key encryption schemes based on multivariate polynomials of degree two over a finite field. However, most of them are insecure. The common defect in many of them comes from the fact that certain quadratic forms associated with their central maps have low rank, which makes them vulnerable to the MinRank attack. We propose a new simple and efficient multivariate pubic key encryption scheme based on matrix multiplication, which does not have such a low rank property. The new scheme will be called Simple Matrix Scheme or ABC in short. We also propose some parameters for practical and secure implementation.

Keywords: Multivariate Public Key Cryptosystem, Simple Matrix Scheme, MinRank Attack.

1 Introduction

Public key cryptography plays an important role in secure communication. The most widely used nowadays are the number theoretical based cryptosystems such as RSA, DSA, and ECC. However, due to Shor's Algorithm, such cryptosystems would become insecure if a large Quantum computer is built. Recent progress made in this area makes this threat realer than ever before. Moreover, the computing capacity of these Number Theoretic based systems is proved to be limited. These are some reasons which motivate researchers to develop a new family of cryptosystems that can resist quantum computers attacks and that are more efficient in terms of computation. Researchers usually use Post Quantum Cryptography (PQC) to denote this new family.

Multivariate public key cryptosystems (MPKC) belong to the PQC family. If well designed, they can be a good candidate for PQC. The public key of an MPKC is a system of multivariate polynomials, usually quadratic, over a finite field. The security of MPKCs is based on the knowledge that solving a set of

⋆ Corresponding author.

P. Gaborit (Ed.): PQCrypto 2013, LNCS 7932, pp. 231–242, 2013.

multivariate polynomial equations over a finite field, in general, is proven to be an NP-hard problem [9]. In fact quantum computers do not appear to have an advantage when dealing with NP-hard problems. However, this does not guarantee that these cryptosystems are secure. The first such practical system was proposed in 1988 by Matsumoto and Imai with their scheme called C* or MI. Nonetheless, Jacques Patarin proved it insecure using linearization equations attack a few years later [18].

In [5], the authors showed that the rank of the quadratic form associated to the central map of C* is only two and therefore the private key could be also recovered with the help of the MinRank Attack.

In [19] Patarin extended the C* scheme by using a new central map to construct a new encryption scheme called Hidden Field Equations (HFE). But Kipnis and Shamir found a way to recover the private keys using the MinRank Attack [13]. Furthermore, it is showed in [8] that inverting HFE is quasi-polynomial if the size of the field and the degree of the HFE polynomials are fixed.

In [15], T.T. Moh proposed a multivariate asymmetric encryption scheme called TTM.

But again, it was broken by exploiting the fact that some quadratic form associated to the central map is of low rank [3].

In the last two decades, many other MPKCs have been proposed for encryption but almost all of them are proven to be insecure and many of them share a common defect; that is some quadratic forms associated to their central maps have low rank and therefore are vulnerable to the MinRank Attack. In consequence, for a MPKC to be secure, it is necessary that all quadratic forms associated with the central map have a rank high enough.

This paper will propose a new multivariate public key scheme for encryption having the property that the quadratic forms associated to the central map do not have a low rank but a rank related to a certain parameter n. The scheme is constructed using some simple matrix multiplications and it will be called Simple Matrix encryption scheme or ABC in short.

This paper is organized as follows. In Section 2 we give an illustration of the MinRank attack using HFE. In Section 3, we describe the construction of the ABC scheme. The security analysis is presented in Section 4. Section 5 shows a practical implementation of the ABC scheme while Section 6 discusses the efficiency and Section 7 concludes the paper.

2 MinRank Attack

The MinRank attack is a cryptanalysis tool that can be used to recover the secret key of MPKCs whose quadratic form associated to the central map is of low rank. In this section, we give an illustration by describing the MinRank attack on the HFE scheme. The attack was first performed by Kipnis and Shamir [13] who showed that the security of HFE can be reduced to a MinRank problem.

2.1 The HFE Scheme

The HFE cryptosystem was proposed by Jacques Patarin in [19]. It can be described as follow. Let $q = p^e$, where p is a prime and $e \geq 1$. Let K be an extension of the finite field $k = \mathbb{F}_q$ of degree n. Clearly, $K \cong k^n$.

Let $\phi : K \to k^n$ be the k-linear isomorphism map between the finite field K and the n-dimensional vector space k^n. The central map of HFE is a univariate polynomial $P(x)$ of the following form

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

where $p_{ij} \in K$ and r is a small constant chosen in a way such that $P(x)$ can efficiently inverted. The public key is given to be

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

where $T : k^n \longrightarrow k^n$ and $S : k^n \longrightarrow k^n$ are two invertible linear transformations and the private key consist of T, P and S.

2.2 MinRank Attack on HFE

In [14], 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. More precisely,

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

and $G^*(x) = T^*(P(S^*(x)))$. We can express $G^*(x)$ in the 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 $\underline{x} = (x, x^q, \ldots, x^{q^{n-1}})$ is a vector over K, $\underline{x}^t$ is the transposition of $\underline{x}$ and $G = [g_{ij}]$ is a matrix over K. The identity $T^{*-1}(G^*(x)) = P(S^*(x)$ implies that

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

where $P = [p_{ij}]$ over K, G^{*k} and W are two matrices over K whose repective (i, j) entries are $g^{q^k}_{i-k,j-k}$ and $s^{q^i}_{i-j}$, with $i - k$, $j - k$ and $i - j$ computed modulo n. Since the rank of WPW^t is not more than r, recovering $t_0, t_1, \ldots, t_{n-1}$ can be reduced to solving a MinRank problem, that is, to find $t_0, t_1, \ldots, t_{n-1}$ such that

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

Methods to solve the MinRank problem for small r can be found in [11]. Once the values $t_0, t_1, \ldots, t_{n-1}$ are found, T and S will be then easily computed. Therefore, the key point to attack HFE is to solve the MinRank problem.

The Kipnis-Shamir attack was improved by Courtois using a different method to solve the MinRank problem [3]. However, Ding et al. showed that the original Kipnis-Shamir attack and the improvement of Courtois are not valid in [4]. Later, Faugère et al. proposed a more comprehensive improvement of the Kipnis-Shamir attack against HFE [2].

3 Construction of ABC Cryptosystem

Let $n, m, s \in \mathbb{Z}$ be integers satisying $n = s^2$ and $m = 2n$. For a given integer s, let k^s denote the set of all s-tuples of elements of k. We denote the plaintext by $(x_1, x_2, \ldots, x_n) \in k^n$ and the ciphertext by $(y_1, y_2, \ldots, y_m) \in k^m$. The polynomial ring with n variables in k will be denoted by $k[x_1, \ldots, x_n]$. Let $\mathcal{L}_1 : k^n \to k^n$ and $\mathcal{L}_2 : k^m \to k^m$ be two linear transformations, i.e.

$$\mathcal{L}_1(x) = L_1 x \quad \text{and} \quad \mathcal{L}_2(y) = L_2 y,$$

where L_1 and L_2 are respectively an $n \times n$ matrix and an $m \times m$ matrix with entries in k, $x = (x_1, x_2, \ldots, x_n)^t$, $y = (y_1, y_2, \ldots, y_m)^t$, and t denote the matrix transposition.

The Central map Let

$$A = \begin{pmatrix} x_1 & x_2 & \cdots & x_s \\ x_{s+1} & x_{s+2} & \cdots & x_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ x_{(s-1)s+1} & x_{(s-1)s+2} & \cdots & x_{s^2} \end{pmatrix}; \quad B = \begin{pmatrix} b_1 & b_2 & \cdots & b_s \\ b_{s+1} & b_{s+2} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{(s-1)s+1} & b_{(s-1)s+2} & \cdots & b_{s^2} \end{pmatrix};$$

and $C = \begin{pmatrix} c_1 & c_2 & \cdots & c_s \\ c_{s+1} & c_{s+2} & \cdots & c_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ c_{(s-1)s+1} & c_{(s-1)s+2} & \cdots & c_{s^2} \end{pmatrix}$ be three $s \times s$ matrices, where $x_i \in k$, b_i and c_i are randomly chosen as linear combination of elements from the set $\{x_1, \ldots, x_n\}$, where $i = 1, 2, \ldots, n$. Define $E_1 = AB$, $E_2 = AC$ and let $f_{(i-1)s+j}$ and $f_{s^2+(i-1)s+j} \in k[x_1, \ldots, x_n]$ be respectively the (i, j) element of E_1 and E_2 $(i, j = 1, 2, \ldots, s)$. Then we obtain with this notation m polynomials $f_1, f_2, \ldots, f_m$, and we define the central map to be

$$\mathcal{F}(x_1, \ldots, x_n) = (f_1(x_1, x_2, \ldots, x_n), \ldots, f_m(x_1, x_2, \ldots, x_n)).$$

We note that for any $1 \le i \le m$, the rank of the quadratic form f_i which is associated with the central map $\mathcal{F}$ is close to or equal to $2s$. Define

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

where $\mathcal{L}_1 : k^n \to k^n$ and $\mathcal{L}_2 : k^m \to k^m$ are as above, $\bar{f}_i \in k[x_1, \ldots, x_n]$ are m multivariate polynomials of degree two. The secret key and the public key are given by:

Secret Key The secret key is made of the following two parts:

1) The invertible linear transformations $\mathcal{L}_1, \mathcal{L}_2$.
2) The coefficients of x_i of the elements in matrices B, C.

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 $\bar{\mathcal{F}}$ or equivalently, its m total degree two components

$$\bar{f}_1(x_1, x_2, \ldots, x_n), \ldots, \bar{f}_m(x_1, x_2, \ldots, x_n) \in k[x_1, \ldots, x_n].$$

Encryption
Given a message $x_1, x_2, \ldots, x_n$, the corresponding ciphertext is

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

Decryption
To decrypt the ciphertext $(y_1, y_2, \ldots, y_m)$, one need to perform the following steps:

1 Compute $(\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_m) = \mathcal{L}_2^{-1}(y_1, y_2, \ldots, y_m)$.
2 Put

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

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

Since $E_1 = AB, E_2 = AC$, 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 $x_1, \ldots, x_n$.

(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 $x_1, \ldots, x_n$.

(iii) If both E_1 and E_2 are not invertible but A is invertible, then $A^{-1}E_1 = B$, $A^{-1}E_2 = C$. We interpret the elements of A^{-1} as the new variables W_i and we end up with $m = 2n$ linear equations in m unknowns. Then we eliminate the new variables to derive n linear equations in the x_i.

(iv) If A is a singular matrix and the rank of A is $n - r$, then there exits a nonsingular matrix W such that $WA = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$, where I is a $(n - r) \times (n - r)$ identity matrix, 0 is a zero matrix. Let $W = \begin{pmatrix} W_1 & W_2 \\ W_3 & W_4 \end{pmatrix}$, $B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}$, $C = \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix}$, $E_1 = \begin{pmatrix} E_{11} & E_{12} \\ E_{13} & E_{14} \end{pmatrix}$, $E_2 = \begin{pmatrix} E_{21} & E_{22} \\ E_{23} & E_{24} \end{pmatrix}$, where $W_1, B_1, C_1, E_{11}, E_{21}$ are a $(n-r) \times (n-r)$ matrices. Since $WE_1 =$

$WAB, WE_2 = WAC$, that is $W_1E_{11} + W_2E_{13} = B_1$, $W_1E_{12} + W_2E_{14} = B_2$, $W_1E_{21} + W_2E_{23} = C_1$, $W_1E_{22} + W_2E_{24} = C_2$.
We interpret the elements of W_1, W_2 as the new variables and we end up with $2s(s-r)$ linear equations in $s(s-r)+n$ unknowns. Then we eliminate the $s(s-r)$ elements of W_1, W_2 in these equations. If these $2s(s-r)$ linear equations are independent, we gain $n-sr$ linear equations with the variables $x_1, x_2, ..., x_n$.

The dimension of the solution space of the linear equations with the variables $x_1, x_2, ..., x_n$ is in general very small. Solving this system by Gaussian elimination enables us to eliminate most of the unknowns, say Z of them. Then we write these Z variables as linear combinations of the remaining unknown variables and then substitute them into the central equations. We then obtain a new system of equations of degree two in the remaining $n-Z$ unknowns which can be easily solved since the number of variables of this new system of equations is very small. Sometimes we may have more than one solution, but the probability is very small.

3 Compute the plaintext $(x_1, x_2, \ldots, x_n) = \mathcal{L}_1^{-1}(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n)$.

Our experiments show that even if A is a singular matrix, decryption remains successful as long as the rank of A is no less than $s-2$. When the rank of A is less than $s-2$, decryption may fail. Let $r > 0$ be the rank of A, then the number of $s \times s$ matrix of rank r over k is $\frac{q^{r(r-1)/2} \prod_{i=s-r+1}^{s} (q^i-1)^2}{\prod_{i=1}^{r} (q^i-1)}$, thus for any $s \times s$ matrix A, the probability of A of rank r is $\frac{q^{r(r-1)/2} \prod_{i=s-r+1}^{s} (q^i-1)^2}{q^{s^2} \prod_{i=1}^{r} (q^i-1)}$. Therefore, the probability of A of rank less than r is $1 - \sum_{j=r}^{s} \frac{q^{j(j-1)/2} \prod_{i=s-j+1}^{s} (q^i-1)^2}{q^{s^2} \prod_{i=1}^{j} (q^i-1)}$. For example, let $q = 2^8, s = 8$, then the probability of A of rank less than 6 is about 2.125919×10^{-22}, thus, in this case, the probability of decryption failure is about 2.125919×10^{-22}. This means that we can adjust the parameters to make sure that decryption will not be a problem.

4 Security Analysis

In this section, we will study the security of the ABC scheme in order to able us to choose the appropriate parameters for a secure encryption.

4.1 High Order Linearization Equation Attack

Linearization equation attack was first discussed in [18] to attack MI [16]. Later, high order linerlization equation attack was proposed to attack MFE cryptosystem [6]. We use this method to attack our scheme. Since $BE_1^{-1}E_2 = C$ (the case where $CE_2^{-1}E_1 = B$ is similar), there exists polynomial g_1, with $deg(g_1) \leq s$, such that $Bg_1(E_1)E_2 = Cdet(E_1)$. Therefore, the plaintext and the ciphertext satisfy the equation:

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

which means that we derive linearization equations with order $n+1$. The coefficients $\mu_{i_0,i_1,\ldots,i_s}, \nu_{i_0,i_1,\cdots,i_{s-1}}, \ldots, \gamma_{i_0}, \xi_{i_1}, \theta$ are variables taking value in k. The number of variables 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-ciphertxet pairs. By substituting these plaintext-ciphertxet pairs into the equations, we have $n\binom{m+s}{s}+m+1$ linear equations with $n\binom{m+s}{s}+m+1$ variables. However, the computation complexity of solving this linearization equation is $\left(n\binom{m+s}{s}+m+1\right)^{\omega}$, where $\omega = 3$ in the usual Gaussian elimination algorithm and $\omega = 2.3766$ in improved algorithm which is impractical for a bit size greater than or equal to 64. Note here that the computation complexity is even high in the case where E_1 and E_2 are not invertible.

4.2 Rank Attack

There are two different methods of using the rank attack. The first one is called MinRank attack or Low Rank attack and an illutration was discussed in section 2. The other one is called the High Rank Attack. We will look at these two attacks against the ABC scheme. For the MinRank attack, let us assume without lost of generality that the public key polynomials and the secret polynomials are homogeneous quadratic polynomials. Let $\mathcal{L}_1, \mathcal{L}_2$ be two invertible linear transformations. Let $\bar{Q}_1, \bar{Q}_2, \ldots, \bar{Q}_m$ be the symmetric matrices associated with the public key quadratic polynomials and $Q_1, Q_2, \ldots, Q_m$ be the symmetric matrices associate with the secret key quadratic polynomials. Clearly, the rank of Q_i is bounded by $2s$. With the MinRank attack, one tries to find $(t_1, t_2, \ldots, t_m) \in k^m$ such that the rank of the linear combinations $\sum_{i=1}^{m} t_i \bar{Q}_i$ is no more than $2s$. In order to find such a linear combination, one can choose any vector $v \in k^n$ and try to solve the equations $(\sum_{i=1}^{m} t_i \bar{Q}_i)v = 0$ with the unknowns $t_1, \ldots, t_m$. After finding at least one linear combination of this form, attacker can recover $\mathcal{L}_2$. The attacker can recover $\mathcal{L}_1$ and $Q_1, \ldots, Q_m$ when $\mathcal{L}_2$ is known. More detail about the MinRank attack can be found in [3,10]. The complexity of this attack against the ABC scheme is $O(q^{\lceil \frac{m}{n} \rceil 2s} m^3)$.

For the High Rank Attack, we form an arbitrary linear combinations $Q = \sum_{i=1}^{m} \alpha_i \bar{Q}_i$, then we find $V = Ker(Q)$. If Q have a nontrivial kernel, set $\sum_{i=1}^{m} \lambda_i \bar{Q}_i V = 0$ and check if the solution set $\hat{V}$ of λ_i has a dimension $n - 2s$. This attack uses about $O(n^6 q^{2s})$ field multiplications. Moreover, note that for every vector v of dimension n, there exists a linear combination of the 2^n secret polynomials that yields zero with probability roughly $1 - \frac{1}{q^n}$. So we are faced with a lot of parasitic solutions, which have to be ruled out at the end. Also as it was mentioned earlier the rank of the Q_i is associated with $2\sqrt{n}$ which means that the complexity of the rank attack may not be polynomial time in the number of variables. These facts prove that the Rank attack is really inefficient against the ABC scheme.

4.3 Algebraic Attack

Let $\bar{f}_1(x_1, \ldots, x_n), \ldots, \bar{f}_m(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ be the public key polynomials. Let $y_1, y_2, \ldots, y_m$ be the ciphertext. We try to solve the system of equations

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

directly by Gröbner bases or XL method and its variations Mutant XL algorithm[25][26][27].

We carried out a number of experiments with MAGMA [1], which contains an efficient implementation of F4 algorithm [9] for computing Gröbner bases. Table 1 shows the results of our experiments to attack an instance of ABC scheme in a finite field k of 3 elements.

Table 1. Result of experiments with direct attack using MAGMA(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

As the table 1 shows, the time and memory complexity increase as n grows. Also the degree of regularity increases as n grows which indicated that complexity is exponential.

4.4 Special Attacks

In terms of the design, one may think that maybe we can choose B and C such that their entries are randomly selected sparse linear functions or even monomials, which will allow us to have smaller secret key. However in the case of using only monomials, there is a possible new risk, namely there is a possibility that the central map polynomials are so sparse that they may have hidden UOV structures, that is there are no quadratic terms of a set of variables in the central map polynomials. One may then use UOV Reconciliation attack to find such structure [23][24]. It is not a good ideal to use monomials for B and C, such a distinguished feature is in general not desired. But in the case of general B and C such a feature does not exist. It is an open interesting problem to find out what really happens in the case of sparse B and C.

On the other hand, one may say that how about making A also more general, namely entries are selected as random linear functions. It is clear this is not needed since a linear transformation will easily remove such a feature. Using a matrix A of variables and L_1 is equivalent to using a matrix A of linear functions, without any transformation L_1. In the case of A also more general, one may consider certain tensor related attack, but we cannot see yet any effective way to do so.

5 A Practical Implementation for Encryption

For a practical implementation, we let k be the finite field of $q = 2^8$ elements and $n = 64$. In this case, the plaintext consist of the message $(x_1, \ldots, x_{64}) \in k^{64}$. The public map is $\bar{F} : k^{64} \to k^{128}$ and the central map is $F : k^{64} \to k^{128}$.

The public key consists of 128 quadratic polynomials with 64 variables. The number of coefficients for the public key polynomials is

$$128 \times 66 \times 65/2 \in \{274560, \text{or about } 280KB \text{ of storage}\}.$$

The private key consists of the coefficients of the x_i of the entries of the matrices B and C. and the two linear transformations $\mathcal{L}_1, \mathcal{L}_2$. The total size is about $30KB$.

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

Based on the preceding discussion in section 4, security level for this implementation is lager than 2^{86}. Using odd characteristic field may be good to resist algebraic attack, but it requires more storage.

6 Efficiency of ABC Scheme

In this section, we will compare the efficiency of decryption in ABC scheme with HFE challenge 1 by Patarin [19]. This HFE was broken using algebraic attack [13]. In this HFE scheme, J.Patarin chose the parameters as follow: $q = 2, n = 80$, the degree of central map is 96. Let $P(x)$ be the central map of HFE, the main computation of decryption is to solve the equation $P(x) = y$ over the finite field of 2^{80} elements. In [20], J.Patarin estimated that the complexity of solving this equation is about $O(d^2n^3)$ or $O(dn^3+d^3n^2)$–depending on the chosen algorithms, where d is the degree of $P(x)$. Thus the decryption process needs about 6.4×10^9 times field multiplication over the finite field of 2^{80} elements.

For the proposed parameters of the ABC scheme above, $q = 2^8, n = 64$ and $m = 128$, the steps of decryption were presented in section 3. The computation of step 1) and step3) of decryption are very fast. The main computation of decryption is step 2), solving a set of linear equations. Therefore, we only need about $128^3 = 2^{21} \approx 2.1 \times 10^6$ times field multiplications over the finite field of 2^8 elements for decryption. It is much faster than HFE scheme.

7 Conclusion

In this paper, we propose a new multivariate algorithm for encryption called ABC. A highlight of ABC scheme is that all the quadratic forms associated with the central map are not of low rank but related to some variable integer n. Therefore, it is immune to the MinRank Attack. Another highlight of ABC scheme is that the computation of decryption is very fast, because the main computation is to solve certain linear equations. However we still cannot show that ABC is provably secure.

Acknowledgment. The authors are grateful to the referees for constructive suggestion on special attack and the design which helped to improve the paper. The work was partially supported by **Charles Phelps Taft Foundation** and the NSF of China under the grant #60973131 and the National Natural Science Foundation of China under grant No. U1135004.

References

1. Bosma, W., Cannon, J.J., Playoust, C.: The Magma algebra system I: the user language. J. Symb. Comput. 24(3-4), 235–265 (1997)
2. Bettale, L., Faugère, J.-C., Perret, L.: Cryptanalysis of multivariate and odd-characteristic HFE variants. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 441–458. Springer, Heidelberg (2011)
3. Goubin, L., Courtois, N.T.: Cryptanalysis of the TTM cryptosystem. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 44–57. Springer, Heidelberg (2000)
4. Ding, J., Schmidt, D., Werner, F.: Algebraic attack on HFE revisited. In: Wu, T.-C., Lei, C.-L., Rijmen, V., Lee, D.-T. (eds.) ISC 2008. LNCS, vol. 5222, pp. 215–227. Springer, Heidelberg (2008)
5. Ding, J., Gower, J., Schmidt, D.: Multivariate Public Key Cryptography. Advances in Information Security series. Springer, Heidelberg (2006)

6. Ding, J., Yang, B.-Y., Chen, C.-H.O., Chen, M.-S., Cheng, C.-M.: New Differential-Algebraic Attacks and Reparametrization of Rainbow. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 242–257. Springer, Heidelberg (2008)
7. Ding, J., Hu, L., Nie, X., Li, J., Wagner, J.: High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 233–248. Springer, Heidelberg (2007)
8. Ding, J., Hodges, T.J.: Inverting HFE systems is quasi-polynomial for all fields. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 724–742. Springer, Heidelberg (2011)
9. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases (F4). J. Pure Appl. Algebra 139, 61–88 (1999)
10. Faugère, J.-C., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of minRank. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 280–296. Springer, Heidelberg (2008)
11. Kipnis, A., Shamir, A.: Cryptanalysis of the Oil & Vinegar Signature Scheme. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 257–267. Springer, Heidelberg (1998)
12. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced Oil and Vinegar Signature Schemes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 206–222. Springer, Heidelberg (1999)
13. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 19–30. Springer, Heidelberg (1999)
14. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and its applications, vol. 20. Cambridge University Press
15. Moh, T.T.: A fast public key system with signature and master key functions. In: Proceedings of CrypTEC 1999, International Workshop on Cryptographic Techniques and E-Commerce, pp. 63–69. Hong-Kong City University Press (July 1999), http://www.usdsi.com/cryptec.ps
16. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988)
17. Patarin, J.: The Oil and Vinegar Signature Scheme. Presented at the Dagstuhl Workshop on Cryptography (September 1997) (transparencies)
18. Patarin, J.: Cryptoanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 248–261. Springer, Heidelberg (1995)
19. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg (1996)
20. Rivest, R., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(2), 120–126
21. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing 26(5), 1484–1509 (1997)
22. Wang, L.-C., Yang, B.-Y., Hu, Y.-H., Lai, F.: A "Medium-Field" Multivariate Public-Key Encryption Scheme. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 132–149. Springer, Heidelberg (2006)

23. Ding, J., Yang, B.-Y., Chen, C.-H.O., Chen, M.-S., Cheng, C.-M.: New differential-algebraic attacks and reparametrization of rainbow. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M., et al. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 242–257. Springer, Heidelberg (2008)
24. Thomae, E.: A Generalization of the Rainbow Band Separation Attack and its Applications to Multivariate Schemes. IACR Cryptology ePrint Archive (2012)
25. Buchmann, J.A., Ding, J., Mohamed, M.S.E., et al.: MutantXL: Solving multivariate polynomial equations for cryptanalysis. Symmetric Cryptography, 09031 (2009)
26. Mohamed, M.S.E., Mohamed, W.S.A.E., Ding, J., Buchmann, J.: *MXL2*: Solving polynomial equations over GF(2) using an improved mutant strategy. In: Buchmann, J., Ding, J., et al. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 203–215. Springer, Heidelberg (2008)
27. Mohamed, M.S.E., Cabarcas, D., Ding, J., Buchmann, J., Bulygin, S.: MXL3: An efficient algorithm for computing gröbner bases of zero-dimensional ideals. In: Lee, D., Hong, S., et al. (eds.) ICISC 2009. LNCS, vol. 5984, pp. 87–100. Springer, Heidelberg (2010)