Simple Matrix Scheme for Encryption

Jintai Ding

Joint work with Chengdong Tao, Adama Diene, Albrecht Petzoldt

October, 2013

Outline

Outline

Post-quantum cryptography

Public key cryptosystems that could resist the future quantum computer attack.

- Code-based public key cryptosystems

Post-quantum cryptography

Public key cryptosystems that could resist the future quantum computer attack.

- Code-based public key cryptosystems
- Hash-based signature systems.

Post-quantum cryptography

Public key cryptosystems that could resist the future quantum computer attack.

- Code-based public key cryptosystems
- Hash-based signature systems.
- Lattice-based public key cryptosystems

Post-quantum cryptography

Public key cryptosystems that could resist the future quantum computer attack.

- Code-based public key cryptosystems
- Hash-based signature systems.
- Lattice-based public key cryptosystems
- Multivariate public key cryptosystems – MPKC

What is a MPKC ?

Multivariate Public Key Cryptosystems

- - *Cryptosystems with public keys as a set of multivariate functions*
  Public key: $G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1$.
  over k, a small finite field.

What is a MPKC ?

Multivariate Public Key Cryptosystems

- - *Cryptosystems with public keys as a set of multivariate functions*
  Public key: $G(x_1, \ldots, x_n) =$
  $(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1$.
  over k, a small finite field.
- G can be viewed as a map from k^n to k^m.
  G mostly quadratic maps, where g_i are quadratic polynomials:

$$g_i(x_1, ..x_n) = \sum_{i,j} \alpha_{lij} x_i x_j + \sum_i \beta_{li} x_i + \gamma_l.$$

What is MPKC for encryption

- The **public key** is given as:

$$G(x_1, ..., x_n) = (G_1(x_1, ..., x_n), ..., G_m(x_1, ..., x_n)) = L_2 \circ F \circ L_1.$$

F is called the central map and easy to invert. L_1 and L_2 serve as "locks".

What is MPKC for encryption

- The **public key** is given as:

$$G(x_1, ..., x_n) = (G_1(x_1, ..., x_n), ..., G_m(x_1, ..., x_n)) = L_2 \circ F \circ L_1.$$

F is called the central map and easy to invert. L_1 and L_2 serve as "locks".

- Any plaintext $M = (x'_1, ..., x'_n)$ is encrypted via polynomial evaluation:
$G(M) = G(x'_1, ..., x'_n) = (y'_1, ..., y'_m)$.

What is MPKC for encryption

- The **public key** is given as:

$$G(x_1, ..., x_n) = (G_1(x_1, ..., x_n), ..., G_m(x_1, ..., x_n)) = L_2 \circ F \circ L_1.$$

  F is called the central map and easy to invert. L_1 and L_2 serve as "locks".
- Any plaintext $M = (x'_1, ..., x'_n)$ is encrypted via polynomial evaluation:
  $G(M) = G(x'_1, ..., x'_n) = (y'_1, ..., y'_m)$.
- To decrypt the ciphertext $(y'_1, ..., y'_n)$, one needs to know a secret (**the private key**) to compute the inverse map

$$G^{-1} = L_1^{-1} \circ F^{-1} \circ L_2^{-1}$$

  to find the plaintext $(x'_1, ..., x'_n) = G^{-1}(y'_1, .., y'_n)$.

What is a MPKC for digital signature?

- **Public key**: $G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1$.

What is a MPKC for digital signature?

- **Public key**: $G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1$.
- **Private key**: a way to compute G^{-1} via the decomposition.

What is a MPKC for digital signature?

- **Public key**: $G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1$.
- **Private key**: a way to compute G^{-1} via the decomposition.

- **Signing (a hash of) a document**:

What is a MPKC for digital signature?

- **Public key**: $G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1$.
- **Private key**: a way to compute G^{-1} via the decomposition.

- **Signing (a hash of) a document**: $(x_1, \ldots, x_n) \in G^{-1}(y_1, \ldots, y_m)$.

What is a MPKC for digital signature?

- **Public key**: $G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1$.
- **Private key**: a way to compute G^{-1} via the decomposition.

- **Signing (a hash of) a document**: $(x_1, \ldots, x_n) \in G^{-1}(y_1, \ldots, y_m)$.
- **Verifying**: $(y_1, \ldots, y_m) \stackrel{?}{=} G(x_1, \ldots, x_n)$.

The Motivations for multivariate public key cryptography (MPKC)

- MPKC are Good Candidates for Post Quantum Cryptography (Post-Quantum Cryptography).

The Motivations for multivariate public key cryptography (MPKC)

- MPKC are Good Candidates for Post Quantum Cryptography (Post-Quantum Cryptography).
- MPKC, in general, are very computationally efficient. Great potential for small devices like RFIDs.

Current MPKCs

- Signature schemes: UOV, Rainbow, HFEv-
  Very efficient, short signatures.

Current MPKCs

- Signature schemes: UOV, Rainbow, HFEv-
  Very efficient, short signatures.
- Encryption schemes: PMI+, IPHFE+
  Efficient, but much slower than the multivariate signature schemes. due to cost from perturbation.

The Main Problems associated to Encryption scheme: Algebraic attack

- Direct algebraic attack by solving a set of algebraic equations.

  Low mutant degree (degree of regularity).

The Main Problems associated to Encryption scheme: Algebraic attack

- Direct algebraic attack by solving a set of algebraic equations.

  Low mutant degree (degree of regularity).

- Find special hidden algebraic structure such that we can solve it via a set of algebraic equations.

The Main Problems associated to Encryption scheme: Algebraic attack

- How to solve $\bar{F}_i(x_1, .., x_n) - y'_i = 0$?

  XL, Mutant XL, Groebner basis.

The Main Problems associated to Encryption scheme: Algebraic attack

- How to solve $\bar{F}_i(x_1, .., x_n) - y'_i = 0$?

  XL, Mutant XL, Groebner basis.

- Gaussian elimination on space of polynomials $\prod x_i^{a_i} \bar{F}_m$ under a fix degree.
  The key is the size of the matrix.

The Main Problems associated to Encryption scheme: Algebraic attack

- How to solve $\bar{F}_i(x_1, .., x_n) - y'_i = 0$?

  XL, Mutant XL, Groebner basis.

- Gaussian elimination on space of polynomials $\prod x_i^{a_i} \bar{F}_m$ under a fix degree.
  The key is the size of the matrix.
- The complexity is determined by the degree.

The Main Problems associated to Encryption scheme: Algebraic attack

- How to solve $\bar{F}_i(x_1, .., x_n) - y'_i = 0$?

  XL, Mutant XL, Groebner basis.

- Gaussian elimination on space of polynomials $\prod x_i^{a_i} \bar{F}_m$ under a fix degree.
  The key is the size of the matrix.
- The complexity is determined by the degree.
- Degree of regularity, Mutant degree.

The Main Problems associated to Encryption scheme: Algebraic attack

- How to solve $\bar{F}_i(x_1, .., x_n) - y'_i = 0$?

  XL, Mutant XL, Groebner basis.

- Gaussian elimination on space of polynomials $\prod x_i^{a_i} \bar{F}_m$ under a fix degree.
  The key is the size of the matrix.
- The complexity is determined by the degree.
- Degree of regularity, Mutant degree.
- Brutal force v. Algebraic Solvers

The Main Problems associated to Encryption scheme: Algebraic attack

- MI system was broken by linearization attack of Patarin

The Main Problems associated to Encryption scheme: Algebraic attack

- MI system was broken by linearization attack of Patarin
- HFE was broken by Groebner basis attack due to Joux and Faugere.

The Main Problems associated to Encryption scheme: Algebraic attack

- MI system was broken by linearization attack of Patarin
- HFE was broken by Groebner basis attack due to Joux and Faugere.
- MFE (Middle field equations) was defeated by high order linearizion attack of Ding etc

The Main Problems associated to Encryption scheme: Algebraic attack

- MI system was broken by linearization attack of Patarin
- HFE was broken by Groebner basis attack due to Joux and Faugere.
- MFE (Middle field equations) was defeated by high order linearizion attack of Ding etc
- Diophantine equation based system by Gao and Heindle was broken in 2013 by embedded surface attack of Tao, Adama, Ding.

The Main Problems associated to Encryption scheme: MinRank attack

- The problem: given a set of matrices M_i, i=1,..,n, find nontrivial solution $(a_1, .., a_n)$ such that

$$\sum a_i M_i$$

is of the minimum rank.

- Any homogeneous polynomial can be written as

$$X^t M X,$$

where $X^t = (x_1, .., x_n)$.

The Main Problems associated to Encryption scheme: MinRank attack

- The problem: given a set of matrices M_i, i=1,..,n, find nontrivial solution $(a_1, .., a_n)$ such that

$$\sum a_i M_i$$

  is of the minimum rank.
- It is in general a hard problem, is relatively easy if the minimum rank is very low (2,3,4).
- Any homogeneous polynomial can be written as

$$X^t M X,$$

  where $X^t = (x_1, .., x_n)$.

The Main Problems associated to Encryption scheme: MinRank attack

- 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.

$$F(x_1, .., x_n) = \sum_{i,j}^{l} a_{ij} X^{q^i + q^j} + \sum b_i X^{q^i} + c.$$

$$A = (a_i, j),$$

a matrix of small rank.

The Main Problems associated to Encryption scheme: MinRank attack

- 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.

$$F(x_1, .., x_n) = \sum_{i,j}^{l} a_{ij} X^{q^i + q^j} + \sum b_i X^{q^i} + c.$$

$$A = (a_i, j),$$

  a matrix of small rank.
- TTM scheme: proposed by T. T. Moh but broken after by Courtois and Goubin who exploited the fact that some quadratic form associated with the central map has low rank.

How to deal with Algebraic attack

- The suggestion of using odd characteristics by Ding, Schmidt, Warner

How to deal with Algebraic attack

- The suggestion of using odd characteristics by Ding, Schmidt, Warner
- The work of Ding, Hodges, Thorsten, Kleinjung on mutant degree of HFE, HFEv, HEEv-, IPHFE confirms this idea.

How to deal with Algebraic attack

- The suggestion of using odd characteristics by Ding, Schmidt, Warner
- The work of Ding, Hodges, Thorsten, Kleinjung on mutant degree of HFE, HFEv, HEEv-, IPHFE confirms this idea.
- A new design Multivariate HFE (MHFE) was showed to be secure against Algebraic attack.

How to deal with Algebraic attack

- The suggestion of using odd characteristics by Ding, Schmidt, Warner
- The work of Ding, Hodges, Thorsten, Kleinjung on mutant degree of HFE, HFEv, HEEv-, IPHFE confirms this idea.
- A new design Multivariate HFE (MHFE) was showed to be secure against Algebraic attack.
- But it was defeated again by MinRank method.

The goal

- Design a scheme such that all quadratic forms associated with the central map have relatively high Rank.

The goal

- Design a scheme such that all quadratic forms associated with the central map have relatively high Rank.
- Design a scheme that have a high computation efficiency.

Idea of the Simple Matrix Scheme for Encrypyion

- Create some Matrices having high rank and use some Simple Matrix Multiplication to construct a Multivariate Publick Key Scheme.

Idea of the Simple Matrix Scheme for Encrypyion

- Create some Matrices having high rank and use some Simple Matrix Multiplication to construct a Multivariate Publick Key Scheme.
- The name is called ABC cryptosystem.

Outline

The parameters

- $\mathbb{F}$ the finite field with q elements. hello

The parameters

- $\mathbb{F}$ the finite field with q elements. hello
- s the positive integer.

The parameters

- $\mathbb{F}$ the finite field with q elements. hello
- s the positive integer.
- $n = s^2$ the number of variables.

The parameters

- $\mathbb{F}$ the finite field with q elements. hello
- s the positive integer.
- $n = s^2$ the number of variables.
- $m = 2n$ the number of equations.

The parameters

- $\mathbb{F}$ the finite field with q elements. hello
- s the positive integer.
- $n = s^2$ the number of variables.
- $m = 2n$ the number of equations.
- $\mathbb{F}[x_1, \ldots, x_n]$ the multivariate polynomial ring.

Key Generation

1. Define three matrices A, B and C of the form

$$A = \begin{pmatrix} x_1 & \dots & x_s \\ \vdots & & \vdots \\ x_{(s-1)\cdot s+1} & \dots & x_n \end{pmatrix}, \; B = \begin{pmatrix} b_1 & \dots & b_s \\ \vdots & & \vdots \\ b_{(s-1)\cdot s+1} & \dots & b_n \end{pmatrix},$$

$$C = \begin{pmatrix} c_1 & \dots & c_s \\ \vdots & & \vdots \\ c_{(s-1)\cdot s+1} & \dots & c_n \end{pmatrix}.$$ Here, $b_1, \dots, b_n$ and $c_1, \dots, c_n$ are randomly chosen linear combinations of $x_1, \dots, x_n$.

Key Generation

1. Define three matrices A, B and C of the form
$$A = \begin{pmatrix} x_1 & \dots & x_s \\ \vdots & & \vdots \\ x_{(s-1)\cdot s+1} & \dots & x_n \end{pmatrix}, \; B = \begin{pmatrix} b_1 & \dots & b_s \\ \vdots & & \vdots \\ b_{(s-1)\cdot s+1} & \dots & b_n \end{pmatrix},$$
$$C = \begin{pmatrix} c_1 & \dots & c_s \\ \vdots & & \vdots \\ c_{(s-1)\cdot s+1} & \dots & c_n \end{pmatrix}.$$ Here, $b_1, \dots, b_n$ and $c_1, \dots, c_n$ are randomly chosen linear combinations of $x_1, \dots, x_n$.
2. One computes $E_1 = A \cdot B$ and $E_2 = A \cdot C$. The central map $\mathcal{F}$ of the scheme consists of the m components of E_1 and E_2.

$$F(x_1, .., x_n) = ((E_1)_{1,1}, ..., (E_1)_{s,s}, (E_2)_{1,1}, ..., (E_2)_{s,s}).$$

Key Generation

1. Define three matrices A, B and C of the form
$$A = \begin{pmatrix} x_1 & \dots & x_s \\ \vdots & & \vdots \\ x_{(s-1)\cdot s+1} & \dots & x_n \end{pmatrix}, \; B = \begin{pmatrix} b_1 & \dots & b_s \\ \vdots & & \vdots \\ b_{(s-1)\cdot s+1} & \dots & b_n \end{pmatrix},$$
$$C = \begin{pmatrix} c_1 & \dots & c_s \\ \vdots & & \vdots \\ c_{(s-1)\cdot s+1} & \dots & c_n \end{pmatrix}.$$ Here, $b_1, \dots, b_n$ and $c_1, \dots, c_n$ are randomly chosen linear combinations of $x_1, \dots, x_n$.
2. One computes $E_1 = A \cdot B$ and $E_2 = A \cdot C$. The central map $\mathcal{F}$ of the scheme consists of the m components of E_1 and E_2.
$$F(x_1, .., x_n) = ((E_1)_{1,1}, ..., (E_1)_{s,s}, (E_2)_{1,1}, ..., (E_2)_{s,s}).$$
3. Randomly chosen invertible linear maps $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$.

Key Generation

1. Define three matrices A, B and C of the form
$$A = \begin{pmatrix} x_1 & \dots & x_s \\ \vdots & & \vdots \\ x_{(s-1)\cdot s+1} & \dots & x_n \end{pmatrix}, \; B = \begin{pmatrix} b_1 & \dots & b_s \\ \vdots & & \vdots \\ b_{(s-1)\cdot s+1} & \dots & b_n \end{pmatrix},$$
$$C = \begin{pmatrix} c_1 & \dots & c_s \\ \vdots & & \vdots \\ c_{(s-1)\cdot s+1} & \dots & c_n \end{pmatrix}.$$ Here, $b_1, \dots, b_n$ and $c_1, \dots, c_n$ are randomly chosen linear combinations of $x_1, \dots, x_n$.
2. One computes $E_1 = A \cdot B$ and $E_2 = A \cdot C$. The central map $\mathcal{F}$ of the scheme consists of the m components of E_1 and E_2.
$$F(x_1, .., x_n) = ((E_1)_{1,1}, ..., (E_1)_{s,s}, (E_2)_{1,1}, ..., (E_2)_{s,s}).$$
3. Randomly chosen invertible linear maps $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$.
4. The *public key* : $\bar{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^m$

Key Generation

1. Define three matrices A, B and C of the form
$$A = \begin{pmatrix} x_1 & \dots & x_s \\ \vdots & & \vdots \\ x_{(s-1)\cdot s+1} & \dots & x_n \end{pmatrix}, \; B = \begin{pmatrix} b_1 & \dots & b_s \\ \vdots & & \vdots \\ b_{(s-1)\cdot s+1} & \dots & b_n \end{pmatrix},$$
$$C = \begin{pmatrix} c_1 & \dots & c_s \\ \vdots & & \vdots \\ c_{(s-1)\cdot s+1} & \dots & c_n \end{pmatrix}.$$ Here, $b_1, \dots, b_n$ and $c_1, \dots, c_n$ are randomly chosen linear combinations of $x_1, \dots, x_n$.
2. One computes $E_1 = A \cdot B$ and $E_2 = A \cdot C$. The central map $\mathcal{F}$ of the scheme consists of the m components of E_1 and E_2.
$$F(x_1, .., x_n) = ((E_1)_{1,1}, ..., (E_1)_{s,s}, (E_2)_{1,1}, ..., (E_2)_{s,s}).$$
3. Randomly chosen invertible linear maps $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$.
4. The *public key* : $\bar{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^m$
5. The *private key* : B , C , $\mathcal{L}_1$ and $\mathcal{L}_2$.

Encryption

To encrypt a message $\mathbf{d} \in \mathbb{F}^n$, one simply computes $\mathbf{c} = \bar{\mathcal{F}}(\mathbf{d}) \in \mathbb{F}^m$.

Decryption

1. Compute $\mathbf{x} = \mathcal{L}_2^{-1}(\mathbf{c})$. The elements of the vector $\mathbf{x} \in \mathbb{F}^m$ are written into matrices $\bar{E}_1$ and $\bar{E}_2$ as follows.

$$\bar{E}_1 = \begin{pmatrix} x_1 & \cdots & x_s \\ \vdots & & \vdots \\ x_{(s-1)\cdot s+1} & \cdots & x_n \end{pmatrix}, \quad \bar{E}_2 = \begin{pmatrix} x_{n+1} & \cdots & x_{n+s} \\ \vdots & & \vdots \\ x_{n+(s-1)\cdot s+1} & \cdots & x_m \end{pmatrix}.$$

Decryption

2. In the second step one has to find a vector $\mathbf{y} = (y_1, \ldots, y_n)$ such that $\mathcal{F}(\mathbf{y}) = \mathbf{x}$. To do this, one has to distinguish four cases.
Case I.

- If $\bar{E}_1$ is invertible, one considers the equation $B \cdot \bar{E}_1^{-1} \cdot \bar{E}_2 - C = 0$. Therefore one gets n linear equations in the n variables $y_1, \ldots, y_n$.

Decryption

2. In the second step one has to find a vector $\mathbf{y} = (y_1, \ldots, y_n)$ such that $\mathcal{F}(\mathbf{y}) = \mathbf{x}$. To do this, one has to distinguish four cases.
Case I.

- If $\bar{E}_1$ is invertible, one considers the equation $B \cdot \bar{E}_1^{-1} \cdot \bar{E}_2 - C = 0$. Therefore one gets n linear equations in the n variables $y_1, \ldots, y_n$.
- This is due to the fact:

$$B(AB)^{-1}AC = C.$$

Decryption

Case II.

- If $\bar{E}_1$ is not invertible, but $\bar{E}_2$ is invertible, one considers the equation $C \cdot \bar{E}_2^{-1} \cdot \bar{E}_1 - B = 0$. One gets n linear equations in the n variables.

Decryption

Case II.

- If $\bar{E}_1$ is not invertible, but $\bar{E}_2$ is invertible, one considers the equation $C \cdot \bar{E}_2^{-1} \cdot \bar{E}_1 - B = 0$. One gets n linear equations in the n variables.
- This is due to the fact:

$$C(AC)^{-1}AB = B.$$

Decryption

Case III.

- If none of $\bar{E}_1$ and $\bar{E}_2$ is invertible, but $\bar{A} = A(\mathbf{y})$ is invertible, one considers the relations $\bar{A}^{-1} \cdot \bar{E}_1 - B = 0$ and $\bar{A}^{-1} \cdot \bar{E}_2 - C = 0$. One interprets the elements of $\bar{A}^{-1}$ as new variables $w_1, \ldots, w_n$ and therefore gets m linear equations in the m variables $w_1, \ldots, w_n, y_1, \ldots, y_n$.

Decryption

Case III.

- If none of $\bar{E}_1$ and $\bar{E}_2$ is invertible, but $\bar{A} = A(\mathbf{y})$ is invertible, one considers the relations $\bar{A}^{-1} \cdot \bar{E}_1 - B = 0$ and $\bar{A}^{-1} \cdot \bar{E}_2 - C = 0$. One interprets the elements of $\bar{A}^{-1}$ as new variables $w_1, \ldots, w_n$ and therefore gets m linear equations in the m variables $w_1, \ldots, w_n, y_1, \ldots, y_n$.
- This will give us a large set of linear equations and we will plug it into the original equations to find a solution.

Decryption

Case IV.

- If none of $\bar{E}_1$, $\bar{E}_2$ and $\bar{A}$ is invertible, there occurs a decryption error.

Decryption

Case IV.

- If none of $\bar{E}_1$, $\bar{E}_2$ and $\bar{A}$ is invertible, there occurs a decryption error.
- In this case, we can not decrypt.

Decryption

3. Finally, one computes the plaintext by $\mathbf{d} = \mathcal{L}_1^{-1}(y_1, \ldots, y_n)$.

Decryption failure rate

The probability of $r \times r$ matrix A of rank less than r is

$$1 - (1 - \frac{1}{q^r})(1 - \frac{1}{q^{r-1}}) \cdots (1 - \frac{1}{q}) \approx \frac{1}{q}.$$

Therefore the probability of decryption failure is about

$$\approx \frac{1}{q}.$$

We need to choose relatively large q.

Security analysis: algebraic attack

Two major attacks

- algebraic attack – attack using best polynomial solving algorithms.

Security analysis: algebraic attack

Two major attacks

- algebraic attack – attack using best polynomial solving algorithms.
- MinRank attack.

Security analysis: algebraic attack

Two major attacks

- We use computer experiments to test the case of of decryption using public key with the case of solving a set of random set of quadratic polynomials with n variables and $m = 2n$ equations.

Security analysis: algebraic attack

Two major attacks

- We use computer experiments to test the case of of decryption using public key with the case of solving a set of random set of quadratic polynomials with n variables and $m = 2n$ equations.
- There is not much difference in terms of both time and memory consumption.

Security analysis: algebraic attack

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.

Practical parameter sets

Claimed security level	parameters $\mathbb{F}$, s	input size (bit)	output size (bit)	public key size (kB)	private key size (kB)	decryption error
2^{80}	GF(2^{32}), 8	2,048	4,096	1,099	115	2^{-32}

Table : Proposed Parameters for the basic ABC encryption scheme

Security analysis: MinRank attack

Two major attacks

- The MinRank of our system is 2s.

$$x_1x_2 + x_3x_4 + \ldots + x_{2s-1}x_{2s}$$

is of rank $2s$.

Security analysis: MinRank attack

Two major attacks

- The MinRank of our system is 2s.

$$x_1 x_2 + x_3 x_4 + \ldots + x_{2s-1} x_{2s}$$

  is of rank $2s$.

- The complexity for MinRank for our case is: $O(q^{4r} m^3)$.

Security analysis: MinRank attack

Two major attacks

- The MinRank of our system is 2s.

$$x_1 x_2 + x_3 x_4 + \ldots + x_{2s-1} x_{2s}$$

  is of rank $2s$.
- The complexity for MinRank for our case is: $O(q^{4r} m^3)$.
- Our parameters: $q = 2^{32}$, $r = 16$ and $m = 128$.

Outline

The motivation

- The main goal is to reduce the encryption failure

The motivation

- The main goal is to reduce the encryption failure
- To make the system more efficient.

- We will remove L_1.

$$\bar{F} = L_2 \circ F$$

.

Make one or two variables to be dummy variables.

- What is the problem?
- The attack– set $x_1, ...x_s$ be be zero. Then next row.

The parameters

- $\mathbb{F}$ the finite field with q elements.

The parameters

- $\mathbb{F}$ the finite field with q elements.
- m, n, s, r, u, v the positive integer.

The parameters

- $\mathbb{F}$ the finite field with q elements.
- m, n, s, r, u, v the positive integer.
- n the number of variables.

The parameters

- $\mathbb{F}$ the finite field with q elements.
- m, n, s, r, u, v the positive integer.
- n the number of variables.
- $m = su + sv$ the number of equations.

The parameters

- $\mathbb{F}$ the finite field with q elements.
- m, n, s, r, u, v the positive integer.
- n the number of variables.
- $m = su + sv$ the number of equations.
- $\mathbb{F}[x_1, \ldots, x_n]$ the multivariate polynomial ring.

Key Generation

1. Define

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \dots & x_{sr} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1u} \\ b_{21} & b_{22} & \dots & b_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & \dots & b_{ru} \end{pmatrix}, C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1v} \\ c_{21} & c_{22} & \dots & c_{2v} \\ \vdots & \vdots & \ddots & \vdots \\ c_{r1} & c_{r2} & \dots & c_{rv} \end{pmatrix}.$$

The elements a_{ij} ,b_{ij} and c_{ij} are randomly chosen linear combinations of $x_1, \dots, x_n$. A is size $s \times r$, B is size $r \times u$ and C is of size $r \times v$.

Key Generation

1. Define

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \dots & x_{sr} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1u} \\ b_{21} & b_{22} & \dots & b_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & \dots & b_{ru} \end{pmatrix}, C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1v} \\ c_{21} & c_{22} & \dots & c_{2v} \\ \vdots & \vdots & \ddots & \vdots \\ c_{r1} & c_{r2} & \dots & c_{rv} \end{pmatrix}.$$

   The elements a_{ij} ,b_{ij} and c_{ij} are randomly chosen linear combinations of $x_1, \dots, x_n$. A is size $s \times r$, B is size $r \times u$ and C is of size $r \times v$.

2. Define $E_1 = A \cdot B$, $E_2 = A \cdot C$. The central map $\mathcal{F}$ consists of the $m = s \cdot (u + v)$ components of the matrices E_1 $(s \times u)$ and E_2 $(s \times v)$.

Key Generation

1. Define

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \dots & x_{sr} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1u} \\ b_{21} & b_{22} & \dots & b_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & \dots & b_{ru} \end{pmatrix}, C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1v} \\ c_{21} & c_{22} & \dots & c_{2v} \\ \vdots & \vdots & \ddots & \vdots \\ c_{r1} & c_{r2} & \dots & c_{rv} \end{pmatrix}.$$

   The elements a_{ij} ,b_{ij} and c_{ij} are randomly chosen linear combinations of $x_1, \dots, x_n$. A is size $s \times r$, B is size $r \times u$ and C is of size $r \times v$.

2. Define $E_1 = A \cdot B$, $E_2 = A \cdot C$. The central map $\mathcal{F}$ consists of the $m = s \cdot (u + v)$ components of the matrices E_1 $(s \times u)$ and E_2 $(s \times v)$.

3. Randomly chosen invertible linear maps $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$.

Key Generation

1. Define

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \dots & x_{sr} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1u} \\ b_{21} & b_{22} & \dots & b_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & \dots & b_{ru} \end{pmatrix}, C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1v} \\ c_{21} & c_{22} & \dots & c_{2v} \\ \vdots & \vdots & \ddots & \vdots \\ c_{r1} & c_{r2} & \dots & c_{rv} \end{pmatrix}.$$

   The elements a_{ij} ,b_{ij} and c_{ij} are randomly chosen linear combinations of $x_1, \dots, x_n$. A is size $s \times r$, B is size $r \times u$ and C is of size $r \times v$.

2. Define $E_1 = A \cdot B$, $E_2 = A \cdot C$. The central map $\mathcal{F}$ consists of the $m = s \cdot (u + v)$ components of the matrices E_1 $(s \times u)$ and E_2 $(s \times v)$.

3. Randomly chosen invertible linear maps $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$.

4. The *public key* : $\bar{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^m$

Key Generation

1. Define

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \dots & x_{sr} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1u} \\ b_{21} & b_{22} & \dots & b_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & \dots & b_{ru} \end{pmatrix}, C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1v} \\ c_{21} & c_{22} & \dots & c_{2v} \\ \vdots & \vdots & \ddots & \vdots \\ c_{r1} & c_{r2} & \dots & c_{rv} \end{pmatrix}.$$

   The elements a_{ij} ,b_{ij} and c_{ij} are randomly chosen linear combinations of $x_1, \dots, x_n$. A is size $s \times r$, B is size $r \times u$ and C is of size $r \times v$.
2. Define $E_1 = A \cdot B$, $E_2 = A \cdot C$. The central map $\mathcal{F}$ consists of the $m = s \cdot (u + v)$ components of the matrices E_1 $(s \times u)$ and E_2 $(s \times v)$.
3. Randomly chosen invertible linear maps $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$.
4. The *public key* : $\bar{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^m$
5. The *private key* : A, B , C , $\mathcal{L}_1$ and $\mathcal{L}_2$.

Encryption

To encrypt a message $\mathbf{d} \in \mathbb{F}^n$, one simply computes $\mathbf{c} = \bar{\mathcal{F}}(\mathbf{d}) \in \mathbb{F}^m$.

Decryption

- Step 1. Compute $\mathbf{y} = (y_1, y_2, \ldots, y_m) = \mathcal{L}_2^{-1}(\mathbf{c})$.
- Step 2. Set

$$\bar{E}_1 = \begin{pmatrix} y_1 & y_2 & \cdots & y_u \\ y_{u+1} & y_{u+2} & \cdots & y_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ y_{(s-1)u+1} & y_{(s-1)u+2} & \cdots & y_{su} \end{pmatrix};$$

$$\bar{E}_2 = \begin{pmatrix} y_{su+1} & y_{su+2} & \cdots & y_{su+v} \\ y_{su+v+1} & y_{su+v+2} & \cdots & y_{su+2v} \\ \vdots & \vdots & \ddots & \vdots \\ y_{su+(s-1)v+1} & y_{su+(s-1)v+2} & \cdots & y_{su+sv} \end{pmatrix}.$$

WE need to find the solution for this set of equation by inverting F.

Decryption

To find a vector $\bar{\mathbf{x}} = (\bar{x_1}, \ldots, \bar{x_n})$ such that $\mathcal{F}(\bar{\mathbf{x}}) = \mathbf{y}$, we do the following:

- If the rank of A is r, then there exits a $r \times s$ matrix W such that $WA = I$, where I is a $r \times r$ identity matrix.

Decryption

To find a vector $\bar{\mathbf{x}} = (\bar{x_1}, \ldots, \bar{x_n})$ such that $\mathcal{F}(\bar{\mathbf{x}}) = \mathbf{y}$, we do the following:

- If the rank of A is r, then there exits a $r \times s$ matrix W such that $WA = I$, where I is a $r \times r$ identity matrix.
- Since $E_1 = AB, E_2 = AC$, therefore $WE_1 = WAB, WE_2 = WAC$, that is $WE_1 = B, WE_2 = C$, We interpret the elements of W as the new variables and we end up with $r(u + v)$ linear equations in $sr + n$ unknowns.

Decryption

To find a vector $\bar{\mathbf{x}} = (\bar{x_1}, \ldots, \bar{x_n})$ such that $\mathcal{F}(\bar{\mathbf{x}}) = \mathbf{y}$, we do the following:

- If the rank of A is r, then there exits a $r \times s$ matrix W such that $WA = I$, where I is a $r \times r$ identity matrix.
- Since $E_1 = AB, E_2 = AC$, therefore $WE_1 = WAB, WE_2 = WAC$, that is $WE_1 = B, WE_2 = C$, We interpret the elements of W as the new variables and we end up with $r(u + v)$ linear equations in $sr + n$ unknowns.
- Then we eliminate the sr elements of W in these equations. We gain many linear equations with the variables $\bar{x_1}, ..., \bar{x_n}$.

Decryption

- The dimension of the solution space of the linear equations with the variables $\bar{x_1}, ..., \bar{x_n}$ is in general very small.

Decryption

- The dimension of the solution space of the linear equations with the variables $\bar{x_1}, ..., \bar{x_n}$ is in general very small.
- Solving this system by Gaussian elimination enables us to eliminate most of the unknowns, say Z of them.

Decryption

- The dimension of the solution space of the linear equations with the variables $\bar{x_1}, ..., \bar{x_n}$ 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.

Decryption

- The dimension of the solution space of the linear equations with the variables $\bar{x_1}, ..., \bar{x_n}$ 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.

Decryption

Step 3. Finally, one computes the plaintext by $\mathbf{d} = \mathcal{L}_1^{-1}(\bar{x_1}, \ldots, \bar{x_n})$.

Decryption Failure

For the improvement ABC scheme, if the rank of A is less than r, decryption will be failure. The probability of $s \times r$ matrix A of rank less than r is

$$1 - (1 - \frac{1}{q^s})(1 - \frac{1}{q^{s-1}}) \cdots (1 - \frac{1}{q^{s-r+1}}) \approx \frac{1}{q^{s-r+1}}.$$

Therefore the probability of decryption failure is about

$$\frac{1}{q^{s-r+1}}.$$

Security analysis: MinRank

The MinRank complexity stay the same as in the previous case, where the MinRank is now again $2r$.

Security analysis: Algebraic attack

- The situation of algebraic attack changed if we choose $s > r$, in particular if s is much bigger than r, because $m = s(u + v)$.

Security analysis: Algebraic attack

- The situation of algebraic attack changed if we choose $s > r$, in particular if s is much bigger than r, because $m = s(u + v)$.
- We considered the public keys of instances of the improved ABC scheme over GF(2^{16}) and GF(2^{32}) whose parameters fulfilled the relations
  - $(r, s, u, v, m, n) = (r, r + 1, r, r, 2 \cdot r \cdot (r + 1), r \cdot (r + 1))$ for $\mathbb{F} = \mathrm{GF}(2^{32})$ and
  - $(r, s, u, v, m, n) = (r, r + 2, r + 2, r + 2, 2 \cdot (r + 2)^2, (r + 2)^2)$ for $\mathbb{F} = \mathrm{GF}(2^{16})$.

Algebraic attack

	field	$GF(2^{32})$			$GF(2^{16})$	
	(r,s,u,v)	(3,4,3,3)	(4,5,4,4)	(5,6,5,5)	(2,4,4,4)	(3,5,5,5)
	(m, n)	(24,12)	(40,20)	(60,30)	(32,16)	(50,25)
ABC	time(s)	0.63	2,133		0.23	146.9
	d_{reg}	4	5	6	3	4
	(MB)	17.0	621	ooM[3]	17.8	241
RS	time (s)	1.4	4,151	-	32.9	29,202
	d_{reg}	4	5	6	5	6
	(MB)	18.2	1,157	-	76.7	23,181

[3] ooM = out of memory

Table : Running time of the direct attack against our improved ABC sc

- As the table shows, the public systems of our improved schemes can be solved faster than random systems (especially for the case of GF(2^{16})).

- As the table shows, the public systems of our improved schemes can be solved faster than random systems (especially for the case of GF(2^{16})).
- We therefore made an extrapolation to estimate the complexity of solving the public systems of the improved ABC scheme for larger parameters. By doing so, we obtained the following formulas

$$(\mathrm{GF}(2^{32}), r, r+1, r, r, 2r \cdot (r+1), r \cdot (r+1)) \approx 11.5 \cdot r + 5.5$$

$$(\mathrm{GF}(2^{16}), r, r+2, r+2, r+2, 2 \cdot (r+2)^2, (r+2)^2) \approx 8 \cdot r + 13.5.$$

Choosing parameters

- We choose the parameters of our scheme in such a way that the probability of a decryption failure occurring is less than 2^{-40}.
  - $s - r = 1$ for $\mathbb{F} = \mathrm{GF}(2^{32})$ and
  - $s - r = 2$ for $\mathbb{F} = \mathrm{GF}(2^{16})$.

Choosing parameters

- We choose the parameters of our scheme in such a way that the probability of a decryption failure occurring is less than 2^{-40}.
  - $s - r = 1$ for $\mathbb{F} = \mathrm{GF}(2^{32})$ and
  - $s - r = 2$ for $\mathbb{F} = \mathrm{GF}(2^{16})$.
- For security reasons that $m \leq 2n$. With this equation and $u = v$, the condition

$$(n - r \cdot (2 \cdot u - s)) \cdot (n - r \cdot (2 \cdot u - s) + 1) \leq 2 \cdot m \qquad (1)$$

  needed for the efficiency of the decryption process yields
  - $u \geq r$ for $\mathbb{F} = \mathrm{GF}(2^{32})$ and
  - $u \geq r + 3$ for $\mathbb{F} = \mathrm{GF}(2^{16})$.

Choosing parameters

- We choose the parameters of our scheme in such a way that the probability of a decryption failure occurring is less than 2^{-40}.
  - $s - r = 1$ for $\mathbb{F} = \mathrm{GF}(2^{32})$ and
  - $s - r = 2$ for $\mathbb{F} = \mathrm{GF}(2^{16})$.
- For security reasons that $m \leq 2n$. With this equation and $u = v$, the condition

$$(n - r \cdot (2 \cdot u - s)) \cdot (n - r \cdot (2 \cdot u - s) + 1) \leq 2 \cdot m \qquad (1)$$

  needed for the efficiency of the decryption process yields
  - $u \geq r$ for $\mathbb{F} = \mathrm{GF}(2^{32})$ and
  - $u \geq r + 3$ for $\mathbb{F} = \mathrm{GF}(2^{16})$.
- We obtain the two parameter sets
  - $(r, s, u, v, m, n) = (r, r + 1, r, r, 2r(r + 1), r(r + 1))$ for $\mathbb{F} = \mathrm{GF}(2^{32})$ and
  - $(r, s, u, v, m, n) = (r, r + 2, r + 2, r + 2, 2(r + 2)^2, (r + 2)^2)$ for $\mathbb{F} = \mathrm{GF}(2^{16})$.

Practical parameter sets

Claimed security level	parameters $\mathbb{F}$, (r, s, u, v, n)	input size (bit)	output size (bit)	public key size (kB)	private key size (kB)	decryption error
2^{80}	$GF(2^{32})$, $(7, 8, 7, 7, 56)$	1,792	3,584	674	83	2^{-64}
	$GF(2^{16})$, $(8, 10, 10, 10, 100)$	1,600	3,200	1,934	129	2^{-48}
2^{90}	$GF(2^{32})$, $(8, 9, 8, 8, 72)$	2,304	4,608	1,478	136	2^{-64}
	$GF(2^{16})$, $(9, 11, 11, 11, 121)$	1,936	3,872	3,489	190	2^{-48}
2^{100}	$GF(2^{32})$, $(9, 10, 9, 9, 90)$	2,880	5,760	2,880	216	2^{-64}
	$GF(2^{16})$, $(10, 12, 12, 12, 144)$	2,304	4,608	5,873	270	2^{-48}

Table : Proposed Parameters for the improved ABC encryption scheme

Efficiency of ABC scheme

- A comparation 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 $GF(2^{80})$ 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 $GF(2^{80})$.
- For the ABC scheme with $q = 2^{32}, n = 64, m = 128$, 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 $GF(2^{32})$.

Conclusion

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

- can resist to all known attacks.

Conclusion

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

- can resist to all known attacks.
- all the quadratic forms associate with the central map are not of low rank but related to some variable integer n.

Conclusion

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

- can resist to all known attacks.
- 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