The SimpleMatrix Encryption scheme

Jintai Ding, Albrecht Petzoldt, Lih-Chung Wang

DIMACS Workshop on The Mathematics of Post-Quantum Cryptography

Rutgers University, New Jersey, USA
15.01.2015

Outline

Multivariate Cryptography

$$p^{(1)}(x_1,\dots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_ix_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)}$$

$$p^{(2)}(x_1,\dots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_ix_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)}$$

$$\vdots$$

$$p^{(m)}(x_1,\dots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)}\cdot x_ix_j \quad + \quad \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)}$$

The security of multivariate schemes is based on the

Problem MQ: Given m multivariate quadratic polynomials $p^{(1)}(\mathbf{x}),\dots,p^{(m)}(\mathbf{x})$, find a vector $\bar{\mathbf{x}} = (\bar{x}_1,\dots,\bar{x}_n)$ such that $p^{(1)}(\bar{\mathbf{x}}) = \dots = p^{(m)}(\bar{\mathbf{x}}) = 0$.

Multivariate Cryptography (2)

Advantages

- Resistant against attacks with quantum computers
- Very fast
- Modest computational requirements
  $\Rightarrow$ can be implemented on low cost devices

Multivariate Cryptography (3)

Drawbacks

- Relatively young field of research
  $\Rightarrow$ Security is not so well understood
- No explicit parameter choices to meet given security levels known
- Large size of the public and private keys
- Many practical signature schemes (UOV, Rainbow, HFEv-, ...), but hardly any efficient and secure encryption schemes

Multivariate Cryptography (4)

Construction

- Easily invertible quadratic map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$
- Two invertible affine (or linear) maps $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- *Public key*: $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ supposed to look like a random system
- *Private key*: $\mathcal{S}$, $\mathcal{F}$, $\mathcal{T}$ allows to invert the public key

Multivariate Cryptography (5)

Encryption Schemes

$$\begin{tikzcd}
\mathbf{d} \in \mathbb{F}^n \arrow[r, "\mathcal{P}"] & \mathbf{c} \in \mathbb{F}^m \arrow[d, "\mathcal{S}^{-1}"] \\
\mathbf{y} \in \mathbb{F}^n \arrow[u, "\mathcal{T}^{-1}"] & \mathbf{z} \in \mathbb{F}^m \arrow[l, "\mathcal{F}^{-1}"']
\end{tikzcd}$$

Encryption: Given: message $\mathbf{d} \in \mathbb{F}^n$.
Compute $\mathbf{c} = \mathcal{P}(\mathbf{d}) \in \mathbb{F}^m$.

Decryption: Given $\mathbf{c} \in \mathbb{F}^m$.
Compute recursively $\mathbf{z} = \mathcal{S}^{-1}(\mathbf{c})$, $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{z})$ and $\mathbf{d} = \mathcal{T}^{-1}(\mathbf{y})$.

Key Generation

- Three $s \times s$ matrices A, B and C

$$A = \begin{pmatrix} x_1 & \dots & x_s \\ \vdots & & \vdots \\ x_{(s-1)\cdot s+1} & \dots & x_n \end{pmatrix}, B = \begin{pmatrix} b_1 & \dots & b_s \\ \vdots & & \vdots \\ b_{(s-1)\cdot s+1} & \dots & b_n \end{pmatrix}, C = \begin{pmatrix} c_1 & \dots & c_s \\ \vdots & & \vdots \\ c_{(s-1)\cdot s+1} & \dots & c_n \end{pmatrix}$$

- $b_1, \dots, b_n$ and $c_1, \dots, c_n$: randomly chosen linear combinations of $x_1, \dots, x_n$.
- $E_1 = A \cdot B$, $E_2 = A \cdot C$.
- central map $\mathcal{F}$: m components of E_1 and E_2.
- *Public key* : $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^m$
- *Private key* : B , C , $\mathcal{S}$ and $\mathcal{T}$.

Encryption

Given: message $\mathbf{d} \in \mathbb{F}^n$.

Compute $\mathbf{c} = \mathcal{P}(\mathbf{d}) \in \mathbb{F}^m$.

Decryption

Given: ciphertext $\mathbf{c} \in \mathbb{F}^m$.

Step 1. Compute $\mathbf{z} = \mathcal{S}^{-1}(\mathbf{c})$ and define

$$\bar{E}_1 = \begin{pmatrix} z_1 & \dots & z_s \\ \vdots & & \vdots \\ z_{(s-1)\cdot s+1} & \dots & z_n \end{pmatrix}, \quad \bar{E}_2 = \begin{pmatrix} z_{n+1} & \dots & z_{n+s} \\ \vdots & & \vdots \\ z_{n+(s-1)\cdot s+1} & \dots & z_m \end{pmatrix}.$$

Decryption (cont.)

Step 2. Find a vector $\mathbf{y} = (y_1, \ldots, y_n)$ such that $\mathcal{F}(\mathbf{y}) = \mathbf{z}$.
Assume $\bar{A} = A(\mathbf{y})$ to be invertible

- Consider the relations $\bar{A}^{-1} \cdot \bar{E}_1 - B = 0$ and $\bar{A}^{-1} \cdot \bar{E}_2 - C = 0$.
- Interpret the elements of $\bar{A}^{-1}$ as new variables $w_1, \ldots, w_n \Rightarrow$ m linear equations in the m variables $w_1, \ldots, w_n, y_1, \ldots, y_n$.

Step 3. Compute the plaintext by $\mathbf{d} = \mathcal{T}^{-1}(y_1, \ldots, y_n)$.

The linear systems in step 2 of the decryption process often have multiple solutions. In this case one has to test which of the possible plaintexts corresponds to the given ciphertext.

Decryption failure rate

If the matrix $\bar{A}$ from step 2 of the encryption process is not invertible, there occurs a decryption failure.

$$\mathrm{pr}(\bar{A} \text{ not invertible}) = 1 - (1 - \frac{1}{q^s})(1 - \frac{1}{q^{s-1}}) \cdots (1 - \frac{1}{q}) \approx \frac{1}{q}.$$

$$\Rightarrow \mathrm{pr}(\text{decryption failure}) \approx \frac{1}{q}$$

Improvements

1. Decreasing the probability of decryption failures
   $\Rightarrow$ Rectangular Simple Matrix
2. Increasing the security of the scheme further
   $\Rightarrow$ Cubic Simple Matrix
3. Reducing the blow up factor between plain and ciphertext size
   $\Rightarrow$ Triangular Simple Matrix (work in progress)

Decreasing the probability of decryption failures $\Rightarrow$ Rectangular Simple Matrix

Parameters:

- finite field $\mathbb{F}$ with q elements
- integers n, r, s, u with $r \leq s$
- set $m = 2 \cdot su$

Key Generation

- Three rectangular matrices A, B and C of the form

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1s} \\ a_{21} & a_{22} & \dots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rs} \end{pmatrix}, \; B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1u} \\ b_{21} & b_{22} & \dots & b_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ b_{s1} & b_{s2} & \dots & b_{su} \end{pmatrix}, \; C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1u} \\ c_{21} & c_{22} & \dots & c_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ c_{s1} & c_{s2} & \dots & c_{su} \end{pmatrix}.$$

  The elements a_{ij}, b_{ij} and c_{ij} are randomly chosen linear combinations of $x_1, \dots, x_n$.
- $E_1 = A \cdot B$, $E_2 = A \cdot C$
- central map $\mathcal{F}$: m components of E_1 and E_2.
- Choose randomly two invertible linear maps $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$.
- *Public key* : $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^m$
- *Private key* : A, B , C , $\mathcal{S}$ and $\mathcal{T}$.

Encryption

Given: message $\mathbf{d} \in \mathbb{F}^n$.

Compute $\mathbf{c} = \mathcal{P}(\mathbf{d}) \in \mathbb{F}^m$.

Decryption

Given: ciphertext $\mathbf{c} \in \mathbb{F}^m$.

Step 1. Compute $\mathbf{z} = (z_1, z_2, \ldots, z_m) = \mathcal{S}^{-1}(\mathbf{c})$ and set

$$\bar{E}_1 = \begin{pmatrix} z_1 & z_2 & \cdots & z_u \\ z_{u+1} & z_{u+2} & \cdots & z_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ z_{(s-1)u+1} & z_{(s-1)u+2} & \cdots & z_{su} \end{pmatrix} \in \mathbb{F}^{s \times u};$$

$$\bar{E}_2 = \begin{pmatrix} z_{su+1} & z_{su+2} & \cdots & z_{(s+1)\cdot u} \\ z_{(s+1)\cdot u} & z_{(s+1)\cdot u+2} & \cdots & z_{(s+3)\cdot u} \\ \vdots & \vdots & \ddots & \vdots \\ z_{(2s-1)\cdot u+1} & z_{(2s-1)\cdot u+2} & \cdots & z_{2su} \end{pmatrix} \in \mathbb{F}^{s \times u}.$$

Decryption (cont.)

Step 2. Find $\mathbf{y} \in \mathbb{F}^n$ such that $\mathcal{F}(\mathbf{y}) = \mathbf{z}$. Set $\bar{A} = A(\mathbf{y})$.
$\mathrm{Rank}(\bar{A}) = r \Rightarrow\ \exists W \in \mathbb{F}^{r \times s}$ with $W \cdot \bar{A} = I$.
Consider the relations $W \cdot \bar{E}_1 = B$ and $W \cdot \bar{E}_2 = C$.
Interpret the elements of W as new variables $w_1, \ldots w_{rs}$.
$\Rightarrow$ $2ru$ linear equations in $sr + n$ unknowns.
$\Rightarrow$ Eliminate the elements of W from the system
$\Rightarrow$ $r \cdot (2u - s)$ linear equations in the variables $y_1, y_2, ..., y_n$
$\Rightarrow$ Substitute these equations into $\mathcal{F}$
$\Rightarrow$ Quadratic system of m equations in a very small number of variables.
$\Rightarrow$ System can be solved by Relinearization

Decryption (cont.)

Step 3. Compute the plaintext by $\mathbf{d} = \mathcal{T}^{-1}(\mathbf{y})$.

Probability of decryption failures

Decryption failure occurs $\Leftrightarrow$ $\mathrm{Rank}(\bar{A}) < r$

$$Pr(\mathrm{Rank}(\bar{A}) < r) = 1-(1-\frac{1}{q^s})(1-\frac{1}{q^{s-1}})\cdots(1-\frac{1}{q^{s-r+1}}) \approx \frac{1}{q^{s-r+1}},$$

$\Rightarrow$ By choosing r and s in an appropriate way it is possible to decrease the probability of decryption failures to a negligible value.

Reducing the probability of decryption failures

Other methods

- use a public bijective map $\mathcal{Q}$ over the ring $\mathbb{Z}/q\mathbb{Z}$
  encrypt messages $\mathbf{d}$ and $\mathcal{Q}(\mathbf{d})$
  $\Rightarrow \mathrm{Pr}(\text{decr. fails}) \approx \frac{1}{q^2}$
- use messages $\mathbf{d}$ of length $n-1$ plus extra variable $x \in \mathbb{F}$
  encrypt messages $x_1||\mathbf{d}$ and $x_2||\mathbf{d}$
  $\Rightarrow \mathrm{Pr}(\text{decr. fails}) \approx \frac{1}{q^2}$

Increasing the security $\Rightarrow$ Cubic Simple Matrix

Parameters:

- finite field $\mathbb{F}$ with q elements
- integer s
- set $n = s^2$ and $m = 2 \cdot n$

Key Generation

- Three $s \times s$ matrices A, B and C

$$A = \begin{pmatrix} a_1 & \dots & a_s \\ \vdots & & \vdots \\ a_{(s-1)\cdot s+1} & \dots & a_n \end{pmatrix}, B = \begin{pmatrix} b_1 & \dots & b_s \\ \vdots & & \vdots \\ b_{(s-1)\cdot s+1} & \dots & b_n \end{pmatrix}, C = \begin{pmatrix} c_1 & \dots & c_s \\ \vdots & & \vdots \\ c_{(s-1)\cdot s+1} & \dots & c_n \end{pmatrix}$$

- $a_1, \dots, a_n$: random quadratic polynomials in $x_1, \dots, x_n$
- $b_1, \dots, b_n$ and $c_1, \dots, c_n$: randomly chosen linear combinations of $x_1, \dots, x_n$.
- $E_1 = A \cdot B$, $E_2 = A \cdot C$.
- central map $\mathcal{F}$: m components of E_1 and E_2.
- *Public key* : $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}^n \rightarrow \mathbb{F}^m$
- *Private key* : A, B , C , $\mathcal{S}$ and $\mathcal{T}$.

En- and Decryption

just as for the original scheme.

Security

Rank attacks

- MinRank Problem: Given m $n \times n$ matrices $Q_1, \ldots, Q_m$, find a linear combination

$$\tilde{Q} = \sum_{i=1}^{m} \lambda_i \cdot Q_i$$

of minimal rank s.

- The MinRank attack can be used to recover the central map from the public key.
- In our scheme, the polynomials of A are random polynomials of degree 2
  $\Rightarrow$ Rank is close to n $\Rightarrow$ Rank attacks are not applicable

Security (cont.)

Direct attacks

Denote

- I_A: ideal generated by the polynomials in A
- I_E: ideal generated by the polynomials in E_1 and E_2

$E_1 = A \cdot B,\ E_2 = A \cdot C \Rightarrow I_E \subset I_A$

$\Rightarrow$ every nontrivial syzygy between the elements of I_E should be a nontrivial syzygy between the elements of I_A

$\Rightarrow$ solving the public system directly should be at least as hard as solving the system A

Reducing the blow up factor between plain and ciphertext size $\Rightarrow$ Triangular Simple Matrix (work in progress)

Basic idea: Use structured quadratic polynomials in the matrix A

Benefits

- blow up factor between plain and ciphertext size is minimized
- $\mathcal{P}$ is a nearly determined system
  $\Rightarrow$ direct attacks become more complicated
  $\Rightarrow$ possibility to decrease parameters and therefore key sizes?

Problems to be solved

- $\mathcal{F}$ is not bijective
  $\Rightarrow$ restrict to messages from a subspace of $\mathbb{F}^m$
- Security against Rank attacks

Parameters and Key Sizes

80 bit security

scheme	plaintext size (bit)	ciphertext size (bit)	public key size (kB)	private key size (kB)	probability of decryption failures
SimpleMatrix(GF(2^8),8,64,128)	512	1,024	280.1	28.7	2^{-8}
RSM(GF(2^8),8,11,12,128,264)	1,008	2,112	2,062	84.0	2^{-32}
cubicSM(GF(2^8),7,49,98)	392	784	2,115	72.7	2^{-8}
TSM(GF(2^8),5,48,50)	384	400	1,077	17.2	2^{-8}

Parameters and Key Sizes (cont.)

100 bit security

scheme	plaintext size (bit)	ciphertext size (bit)	public key size (kB)	private key size (kB)	probability of decryption failures
SimpleMatrix(GF(2^8),10,100,200)	800	1,600	1,030	70.0	2^{-8}
RSM(GF(2^8),10,13,14,180,364)	1,408	2,912	5,537	160.0	2^{-32}
cubicSM(GF(2^8),8,64,128)	512	1,024	5,988	154.0	2^{-8}
TSM(GF(2^8),6,70,72)	560	576	4,552	45.0	2^{-8}

Conclusion

The Simple Matrix Encryption Scheme

+ resists all known attacks
+ has a very fast decryption process
- decryption failures occur with non-negligible probability
- large public key size

Improvements

- Decrease the probability of decryption failures
- Improve the security of the scheme further
- Reduce the blow up factor between plain and ciphertext size

Future Work

Future work includes

- behavior of direct attacks against cubic Simple Matrix
- security issues of the triangular schemes
- analysis of different methods to decrease the probability of decryption failures
- cyclic version of the scheme $\Rightarrow$ reduce key sizes
- white-box implementation of the scheme
  $\Rightarrow$ eliminate decryption failures completely

THANK YOU

Questions?