Construct Public Key Encryption Scheme Using Ergodic Matrices over GF(2)*

Pei Shi-Hui, Zhao Yong-Zhe**, and Zhao Hong-Wei

College of Computer Science and Technology,
Jilin University, Changchun, Jilin, 130012, PRC
{peish, yongzhe, zhaohw}@jlu.edu.cn

Abstract. This paper proposes a new public key encryption scheme. It is based on the difficulty of deducing x and y from A and $B = x \cdot A \cdot y$ in a specific monoid $(m, \cdot)$ which is noncommutative. So we select and do research work on the certain monoid which is formed by all the $n \times n$ matrices over finite field F_2 under multiplication. By the cryptographic properties of an "ergodic matrix", we propose a hard problem based on the ergodic matrices over F_2, and use it construct a public key encryption scheme.

1 Introduction

Public key cryptography is used in e-commerce systems for authentication (electronic signatures) and secure communication (encryption). The security of using current public key cryptography centres on the difficulty of solving certain classes of problems [1]. The RSA scheme relies on the difficulty of factoring large integers, while the difficulty of solving discrete logarithms provide the basis for ElGamal and Elliptic Curves [2]. Given that the security of these public key schemes relies on such a small number of problems that are currently considered hard, research on new schemes that are based on other classes of problems is worthwhile.

This paper provides a scheme of constructing a one-way(trapdoor)function, its basic thoughts are as follows:

Let $M_{n\times n}^{F_2}$ be the set of all $n \times n$ matrices over F_2, then $(M_{n\times n}^{F_2}, +, \times)$ is a 1-*ring*, here $+$ and $\times$ are addition and multiplication of the matrices over F_2, respectively. We arbitrarily select two nonsingular matrices Q_1, $Q_2 \in M_{n\times n}^{F_2}$, then:

1. $(M_{n\times n}^{F_2}, \times)$ is a monoid, its identity is $I_{n\times n}$.
2. $(\langle Q_1\rangle, \times)$ and $(\langle Q_2\rangle, \times)$ are abelian groups, their identities are $I_{n\times n}$, too.

* This work supported by the National Research Foundation for the Doctoral Program of Higher Education of China under Grant No. 20050183032, and the Jilin Province Education Office Science Foundation Project of China under Grant No.2004150 and No. 2005180.

** Corresponding author.

J.-Y. Cai, S.B. Cooper, and H. Zhu (Eds.): TAMC 2007, LNCS 4484, pp. 181–188, 2007.

3. for m_1,$m_2 \in M^{F_2}_{n\times n}$, generally we have: $m_1 \times m_2 \neq m_2 \times m_1$, i.e. the operation $\times$ is noncommutative in $M^{F_2}_{n\times n}$.

Let $K = \langle Q_1 \rangle \times \langle Q_2 \rangle$, then we can construct a function $f : M^{F_2}_{n\times n} \times K \longrightarrow M^{F_2}_{n\times n}$, $f(m,(k_1,k_2)) = k_1 \times m \times k_2$; then f satisfies:

1. knowing $x \in M^{F_2}_{n\times n}$ and $k \in K$, it's easy to compute $y = f(x,k)$.
2. when $|\langle Q_1 \rangle|$ and $|\langle Q_2 \rangle|$ are big enough, knowing $x, y \in M^{F_2}_{n\times n}$, it's may be hard to deduce $k \in K$ such that $y = f(x,k)$.
3. form $k = (k_1,k_2) \in K$, it's easy to compute $k^{-1} = (k_1^{-1}, k_2^{-1}) \in K$, and for any $x \in M^{F_2}_{n\times n}$, we always have: $f(f(x,k),k^{-1}) = x$.

If 2 is true then by 1 and 2 we know that f has one-way property; by 3, we can take k as the "trapdoor" of the one-way function f, hence we get a one-way trapdoor function.

For $\forall m \in M^{F_2}_{n\times n}$, we know that $Q_1 \times m$ does corresponding linear transformation to every column of m, while $m \times Q_2$ does corresponding linear transformation to every row of m; So, $Q_1 \times m \times Q_2$ may "disarrange" every element of m. This process can be repeated many times, i.e. $Q_1^x m Q_2^y (1 \leq x \leq |\langle Q_1 \rangle|, 1 \leq y \leq |\langle Q_2 \rangle|)$, to get a complex transformation of m. To increase the quality of encryption(transformation), the selection of Q_1,Q_2 should make the generating set $\langle Q_1 \rangle$ and $\langle Q_2 \rangle$ as big as possible. And the result, of which Q_1 multiplying a column vector on the left and Q_2 multiplying a row vector on the right, should not be convergent. For this purpose, we put forward the concept of ergodic matrix.

2 Ergodic Matrices over Finite Field F_2

Let F_2^n be the set of all n-dimensional column vectors over finite field F_2.

Definition 1. *Let $Q \in M^{F_2}_{n\times n}$, if for any nonzero n-dimensional column vector $v \in F_2^n \backslash \{0\}, Qv, Q^2v, \ldots, Q^{2^n-1}v$ just exhaust $F_2^n \backslash \{0\}$, then Q is called an "ergodic matrix" over F_2.* $(0 = [0\ 0 \cdots 0]^T)$

For example, select the following matrix $Q \in M^{F_2}_{2\times 2}$:

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\textit{then}\ \ Q^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} Q^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

We verify weather Q is an ergodic matrix.

Let $v_1 = [0,1]^T$, $v_2 = [1,0]^T$, $v_3 = [1,1]^T$, then $F_2^2 \backslash \{0\} = \{v_1, v_2, v_3\}$.

To multiply v_1 by Q^1, Q^2, Q^3 respectively, we have:

$$Q^1 v_1 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = v_2$$
$$Q^2 v_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} = v_3$$
$$Q^3 v_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = v_1$$

Their result just exhaust $F_2^2 \backslash \{0\}$. For v_2 and v_3 the conclusion is the same. By Definition 1 Q is an ergodic matrix.

Theorem 1. *$Q \in M_{n\times n}^{F_2}$ is an ergodic matrix iff Q's period, under the multiplication, is $(2^n - 1)$.*

Proof. If $Q \in M_{n\times n}^{F_2}$ is an ergodic matrix, then for $\forall v \in F_2^n \backslash \{0\}$, it must be $Q^{2^n-1} v = v$. Let v respectively be $[1\ 0 \cdots 0]^T, [0\ 1\ 0 \cdots 0]^T, \ldots, [0 \cdots 0\ 1]^T$, then $Q^{2^n-1} = I_{n\times n}$, *i.e.* Q is nonsingular and Q's period divides $(2^n - 1)$ exactly; by Definition 1, Q's period must be $(2^n - 1)$.

If the period of $Q \in M_{n\times n}^{F_2}$ under multiplication is $(2^n - 1)$, then $\langle Q \rangle = \{Q, Q^2, \ldots, Q^{2^n-1} = I_{n\times n}\}$. By Cayley-Hamilton's theorem [3], we have:

$$F_2[Q] = \{p(Q)|p(t) \in F_2[t]\} = \{p(Q)|p(t) \in F_2[t] \wedge deg\ p \leq n-1\}$$

i.e. $|F_2[Q]| \leq 2^n$; Obviously $\langle Q \rangle \subseteq F_2[Q] \backslash \{0_{n\times n}\}$, so that:

$$F_2[Q] = \{0_{n\times n}, Q, Q^2, \ldots, Q^{2^n-1} = I_{n\times n}\}$$

Arbitrarily selecting $v \in F_2^n \backslash \{0\}$ and $Q^s, Q^t \in \langle Q \rangle$, if $Q^s v = Q^t v$, then$(Q^s - Q^t)v = 0$. Because $(Q^s - Q^t) \in F_2[Q]$ and $v \neq 0$, we have $(Q^s - Q^t) = 0_{n\times n}$, i.e. $Q^s = Q^t$. So, $Qv, Q^2 v, \ldots, Q^{2^n-1} v$ just exhaust $F_2^n \backslash \{0\}$, Q is an ergodic matrix. □

By Cayley-Hamilton's theorem, and finite field theory [4], it's easy to get the following lemmas:

Lemma 1. *If $m \in M_{n\times n}^{F_2}$ is nonsingular, then m's period is equal to or less than $(2^n - 1)$.*

Lemma 2. *If $Q \in M_{n\times n}^{F_2}$ is an ergodic matrix, then $(F_2[Q], +, \times)$ is a finite field with 2^n elements.*

Lemma 3. *If $Q \in M_{n\times n}^{F_2}$ is an ergodic matrix, then Q^T must also be an ergodic matrix.*

Lemma 4. *If $Q \in M_{n\times n}^{F_2}$ is an ergodic matrix, then for $\forall v \in F_2^n \backslash \{0\}$, $v^T Q, \ldots, v^T Q^{2^n-1}$ just exhaust $\{v^T | v \in F_2^n\} \backslash \{0^T\}$.*

Lemma 5. *If $Q \in M_{n\times n}^{F_2}$ is an ergodic matrix, then for $\forall a \in F_2$, $aQ \in F_2[Q]$.*

Lemma 6. *If $Q \in M_{n\times n}^{F_2}$ is an ergodic matrix, then there are just $\varphi(2^n - 1)$ ergodic matrices in $\langle Q\rangle$ and we call them being "equivalent" each other. here $\varphi(x)$ is Euler's totient function.*

From above, we know that the ergodic matrices over $M_{n\times n}^{F_2}$ has a maximal generating set, and the result of multiplying a nonzero column vector on the left or multiplying a nonzero row vector on the right by the ergodic matrix is thoroughly divergent; thus it can be used to construct one-way(trapdoor) function.

3 New Public Key Encryption System

3.1 Hard Problem

Problem 1. Let $Q_1,\ Q_2 \in M_{n\times n}^{F_2}$ be ergodic matrices, knowing that $A, B \in M_{n\times n}^{F_2}$, find $Q_1^x \in \langle Q_1\rangle$, $Q_2^y \in \langle Q_2\rangle$ such that $B = Q_1^x A Q_2^y$.

Suppose Eve knows A, B and their relation $B = Q_1^x A Q_2^y$, for deducing Q_1^x and Q_2^y, he may take attacks mainly by [5,6,7]:

1. Brute force attack
   For every $Q_1^s \in \langle Q_1\rangle$, and $Q_2^t \in \langle Q_2\rangle$, Eve computes $B' = Q_1^s A Q_2^t$ until $B' = B$, hence he gets $Q_1^x = Q_1^s$, $Q_2^y = Q_2^t$.
2. Simultaneous equations attack
   Eve elaborately selects $a_1, a_2, \ldots, a_m \in \langle Q_1\rangle$ and $b_1, b_2, \ldots, b_m \in \langle Q_2\rangle$, constructing the simultaneous equations as follows:

$$\begin{cases} B_1 = Q_1^x A_1 Q_2^y \\ B_2 = Q_1^x A_2 Q_2^y \ (Here\ A_k = a_k A b_k\ B_k = a_k B b_k\ are\ know) \\ \vdots \qquad \vdots \\ B_m = Q_1^x A_m Q_2^y \end{cases}$$

Thus Eve may possibly deduce Q_1^x and Q_2^y.

But all of these attacks are not polynomial time algorithm. We assume through this paper the Problem 1 are intractable, which means there is no polynomial time algorithm to solve it with non-negligible probability.

3.2 Public Key Encryption Scheme

Inspired by [8,9,10], We propose a new public key encryption scheme as follow:

- Key Generation.
  The key generation algorithm select two ergodc matrices $Q_1,\ Q_2 \in M_{n\times n}^{F_2}$ and a matrix $m \in M_{n\times n}^{F_2}$. It then chooses $s, t \in [0, 2^{n-1}]$, and sets $sk = (s, t)$, $pk = (Q_1, Q_2, m, Q_1^s m Q_2^t)$.

- Encryption.
  On input message matrix X, public key $pk = (Q_1, Q_2, m, Q_1^s m Q_2^t)$, choose $k, l \in [0, 2^{n-1}]$, computer $Z = X + Q_1^k Q_1^s m Q_2^t Q_2^l$, and output the ciphertext $Y = (Z, Q_1^k m Q_2^l)$.
- Decryption.
  On input $sk = (s, t)$, ciphertext $Y = (Z, C)$, output the plaintext $X = Z - Q_1^s C Q_2^t = Z - Q_1^s Q_1^k m Q_2^l Q_2^t = Z - Q_1^k Q_1^s m Q_2^t Q_2^l$.

The security for the public key encryption scheme based on ergodic matrices is defined through the following attack game:

1. The adversary queries a key generation oracle, the key generation oracle computes a key pair (pk, sk) and responds with pk.
2. The challenger gives the adversary a challenge matrix $c \in M_{n\times n}^{F_2}$.
3. The adversary makes a sequence of queries to a decryption oracle. Each query is an arbitrary ciphertext matrix (not include c); the oracle responds with corresponding plaintext.
4. At the end of the game, the adversary output a matrix a.

The advantage of an adversary is: $Adv = Pr[a = Decryption(c, sk)]$.

Definition 2. *A public key encryption scheme is said to be secure if no probabilistic polynomial time adversary has a non-negligible advantage in the above game.*

Theorem 2. *The security of the public key encryption scheme based on ergodic matrices is equivalent to the Problem 1.*

3.3 Example

(1) Key generation: Select two ergodic matrices $Q_1, Q_2 \in M_{23\times 23}^{F_2}$:

$$Q_1 = \begin{bmatrix}
0&0&1&0&0&1&1&1&0&0&0&1&0&0&0&1&1&1&0&1&0&1&1\\
1&1&1&0&0&1&1&1&1&0&1&1&1&1&0&0&1&0&0&1&1&1&0\\
1&0&0&1&0&1&0&0&1&1&0&1&0&1&0&1&1&1&0&0&0&0&1\\
0&1&0&1&1&1&1&0&0&0&0&1&0&0&0&1&0&1&0&1&0&1&1\\
1&0&0&1&1&0&0&1&0&0&0&0&0&1&1&0&1&1&0&1&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&1&0&1&1\\
1&1&0&1&1&1&0&1&1&0&0&1&0&0&1&0&1&0&0&0&0&1&0\\
1&1&1&0&0&1&1&1&1&0&1&1&1&1&0&0&0&0&1&1&1&1&1\\
1&1&1&0&0&0&0&1&1&1&1&0&1&1&0&1&1&0&1&0&0&0&0\\
1&1&1&0&1&1&1&0&0&0&0&0&0&0&0&1&0&0&1&1&1&1&0\\
1&1&0&1&1&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&1&0\\
0&1&0&0&1&1&0&0&1&0&1&0&0&0&0&0&0&0&0&1&0&1&1\\
1&0&0&1&0&0&1&0&1&1&1&1&1&0&1&0&1&1&0&1&1&1&1\\
1&1&0&0&1&0&1&1&0&1&1&0&1&0&0&1&1&1&0&0&1&1&1\\
1&0&0&0&1&0&1&0&1&0&0&0&0&1&0&1&0&0&1&1&1&1&1\\
1&0&0&0&0&1&0&0&0&0&0&0&1&0&1&1&0&1&1&0&0&0&1\\
1&1&0&0&1&0&0&1&1&1&0&0&0&1&0&1&1&1&1&0&1&1&0\\
0&0&0&0&1&1&0&1&0&0&0&1&0&1&1&0&0&0&1&1&0&1&0\\
1&1&0&1&0&1&1&1&1&1&1&0&0&0&1&0&0&0&1&0&0&0&0\\
1&0&1&1&0&0&1&1&1&0&1&1&1&1&0&1&0&1&0&1&0&0&1\\
1&0&1&0&0&1&1&1&1&1&0&1&1&1&0&0&0&1&0&1&0&1&1\\
1&0&0&0&1&0&0&1&0&0&1&1&0&1&1&0&1&1&0&1&0&0&0\\
1&1&0&1&0&0&0&1&0&1&0&0&1&1&1&1&1&0&0&0&0&1&1
\end{bmatrix}$$

$$Q_2 = \begin{bmatrix}
1&1&0&1&0&0&0&1&0&0&1&0&1&0&0&1&0&0&1&1&0&0&1\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&1&0&1&0&0&1&1&0\\
1&1&1&1&0&0&0&1&1&0&0&1&0&1&1&1&0&1&1&0&0&0&0\\
1&0&0&0&0&0&1&1&1&0&0&0&1&0&1&0&0&1&0&1&1&1&1\\
1&0&0&1&1&1&1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1&0\\
0&1&1&1&1&0&0&1&0&1&0&0&0&1&1&0&1&0&1&1&0&0&0\\
1&1&1&0&1&0&0&1&0&0&0&0&0&1&1&1&1&1&0&1&0&0&0\\
1&0&1&1&1&0&1&0&0&0&0&1&1&1&0&1&1&1&0&0&0&0&0\\
1&1&0&1&1&1&0&1&0&0&0&1&1&1&1&1&1&0&0&0&1&1&0\\
1&1&0&1&0&0&1&1&1&0&1&1&1&1&0&1&0&1&1&1&1&1&1\\
1&0&1&1&0&0&0&0&1&1&1&0&1&0&1&1&0&0&1&1&0&1&0\\
0&0&0&1&1&0&1&1&0&0&0&0&1&0&0&1&1&0&0&0&1&1&1\\
0&1&1&1&1&1&1&1&1&1&0&1&0&1&1&0&0&1&0&0&1&0&1\\
1&0&1&1&0&0&1&1&1&0&0&1&0&0&1&1&0&1&0&1&1&0&1\\
1&1&0&0&0&0&0&0&1&0&0&0&1&0&1&1&1&0&1&0&0&1&0\\
1&0&0&1&1&0&0&0&1&1&1&0&1&0&1&1&1&0&0&1&1&1&1\\
1&1&1&0&1&1&1&1&0&1&1&1&0&1&0&0&0&1&1&0&1&1&0\\
0&0&0&1&1&1&0&0&1&0&1&1&0&0&0&0&1&0&1&1&1&1&0\\
0&0&1&0&0&1&0&1&0&1&1&1&0&0&0&1&0&1&1&1&0&1&0\\
0&1&1&0&0&0&1&1&1&0&0&1&1&0&1&1&0&0&0&1&1&0&1\\
1&0&0&1&0&1&1&1&1&1&1&0&0&1&0&0&1&0&0&1&1&1&1\\
1&0&1&1&0&1&1&1&0&0&0&0&0&1&0&1&0&0&0&0&1&0&0\\
0&0&1&0&1&1&0&1&0&1&1&0&0&0&1&0&0&1&0&0&0&0&1
\end{bmatrix}$$

the ergodic matrices Q_1 and Q_2 can be generated using following algorithm:

1. select a random matrix $m \in M_{n\times n}^{F_2}$;
2. if $Rank(m) < n$, goto 1;
3. if $m^{2^n-1} \neq I_{n\times n}$, goto 1;
4. m is a ergodic matrix.

Moveover, we need select a matrices $m \in M_{23\times 23}^{F_2}$ randomly:

$$m = \begin{bmatrix}
0&0&1&0&1&1&0&0&0&0&0&0&1&1&0&0&0&1&0&1&0&1&0\\
1&0&0&1&0&1&1&1&1&0&0&0&1&1&0&0&1&1&0&1&0&1&1\\
1&1&1&0&0&0&1&1&1&0&1&1&0&1&0&1&1&1&0&0&0&1&1\\
0&0&0&1&1&1&1&1&0&0&1&0&1&0&0&0&0&1&0&0&0&1&1\\
1&1&1&0&1&0&0&1&0&0&1&1&1&1&0&1&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&1&1&0&0&1&1&0&0&0&0&0&1&0&0&1&0&1&0&1&1\\
0&1&1&1&1&1&1&1&1&0&1&0&1&0&0&0&0&1&0&1&0&1&1\\
0&1&1&1&1&0&0&1&0&0&1&1&0&0&1&1&0&1&0&1&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&1&1&0&0&1&1&0&1&0&0&0&1&0&1&0&0&0\\
0&1&1&0&0&0&1&0&1&0&0&0&0&1&0&1&0&1&0&0&0&0&1\\
0&0&1&1&0&1&1&0&0&0&0&0&1&1&1&0&1&1&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&1&1&0&0&1&1&0&1&1&0&0&1&0&1&0&0&1&0&1&0\\
1&1&0&1&0&1&1&1&0&0&0&0&0&1&0&0&1&0&0&0&0&1&1\\
0&1&1&0&0&1&0&1&0&0&1&0&1&1&1&0&1&0&0&0&0&0&0\\
0&1&0&1&1&0&0&0&1&0&1&1&1&1&0&0&1&0&0&1&0&0&1\\
1&1&0&1&0&0&0&1&1&0&1&0&1&0&1&1&1&1&0&0&0&0&1\\
0&1&0&1&0&1&0&0&0&0&1&1&0&1&1&1&0&0&0&1&0&1&1\\
1&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&1\\
1&0&1&0&1&1&0&0&1&0&1&0&0&1&1&1&1&1&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}$$

then select private key: $s = 1367235$ $t = 2480563$, and compute:

$$Q_1^{1367235} m Q_2^{2480563} = \begin{bmatrix}
1&0&0&1&1&0&1&1&0&1&1&1&1&1&1&1&1&1&1&0&1&0&1\\
0&0&0&1&0&1&1&0&1&0&0&0&0&0&0&1&0&0&0&1&1&1&1\\
1&1&1&1&1&1&1&1&0&1&0&0&0&1&1&1&1&0&0&1&1&0&0\\
1&1&0&1&1&1&1&1&0&0&1&0&1&0&1&1&1&0&1&1&1&1&0\\
1&0&0&1&0&1&1&0&0&0&1&0&0&1&0&1&0&1&1&0&0&1&1\\
1&1&1&1&0&1&1&1&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0\\
0&0&1&1&0&0&1&1&1&0&0&0&0&1&1&1&0&1&1&0&0&0&1\\
1&1&0&0&0&0&1&1&0&1&0&0&0&0&1&0&1&1&0&1&0&1&1\\
1&1&0&1&1&0&1&1&0&1&1&1&0&0&1&1&0&0&0&0&1&0&1\\
0&1&1&0&1&0&1&0&0&1&0&1&0&0&0&1&1&1&0&0&1&1&0\\
1&0&1&1&0&0&1&0&0&0&1&0&0&0&1&1&1&1&0&0&0&1&1\\
0&1&1&0&1&1&1&1&1&0&1&1&1&0&1&1&1&0&1&0&1&0&0\\
1&1&0&0&1&0&0&1&0&0&0&1&1&0&0&1&0&0&1&0&0&1&1\\
1&0&0&0&0&1&0&1&0&1&0&0&0&1&0&1&1&0&1&0&0&1&1\\
0&0&1&1&1&0&1&1&0&0&1&1&1&1&1&0&0&0&0&0&0&1&1\\
0&0&1&0&0&0&1&0&0&0&1&1&1&1&1&1&0&1&1&0&1&1&1\\
1&1&1&1&1&1&0&1&1&1&0&0&0&1&1&0&1&0&0&1&1&1&0\\
1&1&0&1&0&0&1&1&1&0&0&1&1&0&0&1&1&0&0&1&0&1&1\\
0&0&0&1&1&0&0&0&1&0&0&1&0&1&0&1&0&1&0&1&0&1&0\\
0&1&0&0&0&1&1&0&1&0&0&1&1&1&1&0&1&1&1&1&1&0&1\\
1&1&0&0&0&1&0&0&0&0&1&1&0&1&0&0&1&0&0&0&1&1&1\\
1&0&0&0&0&1&0&1&0&0&1&0&0&1&0&0&0&1&1&0&1&0&0\\
0&1&1&1&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&1&0&0
\end{bmatrix}$$

so the public key is $pk = (Q_1, Q_2, m, Q_1^s m Q_2^t)$.

(2)In the process of Encryption, select two random integers: $k = 4321506$, $l = 3493641$.

because $Q_1^k Q_1^s m Q_2^t Q_2^l = Q_1^s Q_1^k m Q_2^l Q_2^t$, i.e.
$Q_1^{4321506} Q_1^{1367235} m Q_2^{2480563} Q_2^{3483641} = Q_1^{1367235} Q_1^{4321506} m Q_2^{3483641} Q_2^{2480563}$,
the result is:

$$\begin{bmatrix}
1&1&1&1&0&0&0&1&0&0&1&1&1&1&1&0&1&0&1&0&0&1&1\\
0&0&1&0&0&1&0&0&0&1&0&0&1&1&0&0&1&0&1&0&0&0&0\\
1&0&1&0&1&1&1&1&0&1&1&0&0&1&0&0&0&0&0&1&1&1&0\\
0&1&0&1&0&0&1&1&1&1&0&0&0&1&0&0&1&1&0&1&0&1&0\\
0&1&0&0&1&0&0&0&1&1&1&1&1&1&0&0&1&0&1&0&0&0&0\\
1&0&1&0&0&0&0&1&0&0&1&1&1&1&1&1&1&0&0&0&1&1&0\\
0&1&1&1&1&0&0&0&0&1&1&1&0&1&1&1&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&1&1&0&1&0&0&1&1&0&1\\
1&0&0&1&1&0&1&1&1&1&0&0&1&0&1&0&1&1&1&0&1&1&0\\
0&1&0&1&0&1&0&1&1&0&0&0&0&0&1&1&0&1&1&1&0&1&0\\
1&1&1&0&0&0&1&1&0&0&0&0&1&0&1&0&0&1&0&0&0&1&0\\
1&1&1&1&0&0&0&0&1&0&0&0&1&1&0&0&1&1&0&1&0&0&0\\
1&0&0&1&1&0&1&0&0&1&1&0&0&0&0&0&1&1&0&0&1&1&0\\
1&1&0&0&1&1&0&0&1&0&0&0&0&0&1&0&0&1&0&0&1&0&0\\
0&1&0&0&0&0&1&0&1&0&0&1&0&1&1&1&0&0&0&0&0&0&0\\
1&0&0&0&1&1&0&0&1&0&0&1&1&0&0&0&0&1&1&1&0&0&1\\
1&1&1&0&1&0&0&1&0&1&1&1&0&0&0&1&0&0&0&0&1&1&0\\
1&1&0&0&1&0&0&1&1&1&0&1&1&1&0&1&0&0&0&0&0&1&1\\
0&1&1&0&0&0&1&0&0&1&0&0&0&0&0&0&0&1&1&1&1&1&1\\
0&1&0&0&1&1&0&1&0&0&0&1&0&1&1&1&1&1&1&0&1&0&1\\
1&0&1&0&0&1&0&0&0&0&1&0&1&1&0&1&0&1&1&0&0&1&1\\
1&0&0&0&1&0&1&0&0&1&1&0&1&0&0&1&1&0&1&1&1&1&0\\
1&1&0&1&1&0&0&1&0&1&0&0&0&0&1&1&0&1&1&0&0&1&0
\end{bmatrix}$$

It is easy to verify the process of encryption and decryption.

4 Conclusions

The ergodic matrices over $M_{n\times n}^{F_2}$ has a maximal generating set, and the result of multiplying a nonzero column vector on the left or multiplying a nonzero row vector on the right by the ergodic matrix is thoroughly divergent; thus it can be used to construct one-way(trapdoor) function. In this paper, we propose a new hard problem based on the ergodic matrices over F_2, by which, we implement a public key encryption scheme. Different from the previous approaches, we adopt matrix to represent plaintext, which can encrypt more information once a time.

We plan to give the theoretical proof on the hard problem based on the ergodic matrices over F_2. Additional research is also required to compare the security and performance with other public key encryption schemes such as RSA and Elliptic Curves.

References

1. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone: Handbook of Applied Cryptography, New York: CRC Press,1997.
2. Bruce Schneier: Applied Cryptography: protocols, algorithms, and source code in C, USA, John Wiley & Sons, Inc. 1996.
3. F.R. Gantmacher: The Theory of Matrices, Vol.2, New York:Chelsea, 1974
4. R. Lidl, H. Niederreiter: Introduction to Finite Fields and Their Applications, Cambridge: Univ. Press, 1994.
5. Y. Zhao, L. Wang L, W. Zhang: Information-Exchange Using the Ergodic Matrices in GF(2), Proc. 2th International Conference on Applied Cryptography and Network Security (ACNS 2004). ICISA PRESS, 2004: 388-397.
6. Y. Zhao, S. Huang, Z. Jiang: Ergodic matrices over GF(2k) and their properties, Mini-Micro Systems, 2005, 26(12): 35-39.
7. Y. Sun, Y. Zhao, Y. Yang, R. Li: Scheme to construct one-way(trapdoor)functions based on ergodic matrice, Journal of Jilin University, 2006, 24(5):554-560.
8. T. ElGamal: A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory, 31(4):469-472, 1985.
9. M. Gerard, M. Chris, R. Joachim: A public key cryptosystem based on actions by semigroups, IEEE International Symposium on Information Theory-Proceedings, 2002, p.266-289
10. R. Arash, H. Anwar: A new construction of Massey-Omura parallel multiplier over GF(2^m), IEEE Transactions on Computers, v51(5), 2002:511-520.