A Novel Public Key Cryptosystem Based on Ergodic Matrices over $GF(2)$

Zhengjun Jing$^{1,2}$, Guoping Jiang$^1$, Chunsheng Gu$^2$

$^1$ College of Computer, Nanjing university of Posts and Telecommunications
Nanjing,China,210003
$^2$ School of Computer Engineering, Jiangsu Teachers University of Technology
Changzhuo,China,213001

jzjing@jstu.edu.cn,jianggp@njupt.edu.cn,Guchensheng@gmail.com

Abstract. A new ELGamal-type public key cryptosystem is proposed in this paper, which is based on matrix discrete logarithm. The security of this scheme is equal to the difficulty of polynomial discrete logarithm problem over finite field in the standard mode. Since plaintext is represented by matrix and its ciphertext expand is almost 1, the proposed scheme can encrypt more information one time.

Keywords: Ergodic Matrix; Public Key Encryption; Isomorphic over Finite Field; Polynomial Discrete Logarithm.

1 Introduction

In recently, cryptographic functions based on ergodic matrix have attracted considerable interest. Monico[1] analyzed semi-group actions in public key encryption using ergodic matrix. Pei and Zhao considered the methods to find ergodic matrix over finite field and constructed a new fast public key encryption algorithm [2] as well as Shamir’s three pass protocol. Unfortunately, through there are many good properties about ergodic matrix, some of them have been proved to not be secure [3]. In this note, we attempt to present an alternative for the current schemes, which based on the ergodic matrices over finite field.

1.1 Overview of Ergodic Matrix over $F_2$

Let $F_2^n$ be the set of all n-dimensional column vectors over finite field. The definition of ergodic matrix is as follow:
**Definition 1** [4]: Let $Q \in M_{n \times n}^{F_2}$, if for any nonzero $n$-dimensional column vector $v \in F_2^n \setminus \{0\}$, $Qv, Q^2v, \ldots, Q^{2^n-1}v$ just exhaust $F_2^n \setminus \{0\}$, then $Q$ is called an ergodic matrix over $F_2$, where $(0 = [0,0,\cdots,0]^T)$.

**Definition 2**: Let $Q \in M_{n \times n}^{F_2}$, if $<Q> = \{Q^i, i \in \mathbb{Z}\}$, then $Q$ is a generator and $<Q>$ is generating set of $Q$ over $F_2$.

The properties described above will be used in the new scheme. For the more details about ergodic matrix, the reader is referred to [4].

### 2 Relevant Theorems about New Scheme

According to the fundamental properties of ergodic matrix and polynomial finite field, a theorem about ergodic matrix could be resulted after further studying, proof of which will be described in the extended edition.

**Theorem 1**: $A \in M_{n \times n}^{F_2}$ is an ergodic matrix if and only if its characteristic polynomial $\phi(\lambda) = |\lambda I - A|$ is irreducible polynomial of degree $n$ over $F_2$.

**Lemma 1**: If $\phi(\lambda)$ is an irreducible polynomial over $F_2$, then the friend matrix $B \in M_{n \times n}^{F_2}$ induced by $\phi(\lambda)$ is an ergodic matrix, and the finite field $F_2[B]$ is isomorphic to finite field $F_2[\lambda] \mod \phi(\lambda)$.

### 3 A new Public Key Encryption Scheme over

We construct a new ELGamal-type public key encryption scheme as follow.

(a) Key generation

The key generation algorithm randomly chooses an irreducible polynomial $f(x)$ with degree $n$ over $F_2$ and a positive integer $a$ which satisfies $a < 2^n - 1$. It then compute $g(x) \equiv x^a \mod f(x)$ where $x$ is just a variable symbol, and set $pk = \{f(x), g(x)\}$ and $sk = \{a\}$.

(b) Encryption

On input a message matrix $Q \in M_{n \times n}^{F_2}$ and $pk = \{f(x), g(x)\}$, chooses $b \in [0,2^n - 1]$ at random and then takes some steps as follow.

**Step 1**: Computing $c_1(x)$ and $h(x)$, respectively.

\[ c_1(x) \equiv x^b \equiv a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \mod f(x) \quad (1) \]

\[ h(x) = (g(x))^b \equiv x^{ab} \equiv a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \mod f(x) \quad (2) \]
Step 2: Given $B$ is a friend matrix induced by $f(x)$, according to Lemma 1, we can get the following equation.

$$H = h(B) = \sum_{i=0}^{n-1} a'_i B^i$$  \hspace{1cm} (3)

Step 3: $C_2 = H + Q$, and output the ciphertext $C = (c_1, C_2)$.

Here, $c_1(x)$ is a unary polynomial of degree $n$, so its coefficients can be represented by a $n$-dimensional vector. At the same time, $C_2$ is an $n$-order matrix in which each entity is belonged to the finite field $F_2$.

(c) Decryption

On input ciphertext $C = (c_1, C_2)$ and $sk = \{a\}$, the message can be recovered exactly through the following steps.

Firstly, we construct the polynomial $c_1(x)$ by the vector $c_1$, and then we compute the polynomial. $h'(x) = c_1'(x) = (x^h)^a = \sum_{i=0}^{n-1} a'_i x^i \mod f(x)$.  \hspace{1cm} (4)

It is easy to identify that this polynomial is equal to $h(x)$ of the step 1 of encryption. So the step 2 of decryption is to get the same matrix $H$ as the step 2 in encryption. Finally, the ciphertext can be decrypted on step 3, such that $Q = C_2 - H$.

4 Conclusion

The ergodic matrix has some good properties which can be used to design cryptographic primitives. The new ELGamal-type public key cryptosystem over $GF(2)$ proposed in this paper just utilizes the irreducibility of characteristic polynomial of ergodic matrix, the security of which is equivalent to the difficulty of discrete logarithm problem.

References

2. S. Pei, Y. Zhao, and H. Zhao: Construct public key encryption scheme using ergodic matrices over $GF(2)$.: In 4th annual conference on theory and application of models of computation (TAMC07), pp.181--188, Springer-Verlag, Berlin Heidelberg (2007)