Construct a New ELGamal-type Public Key Cryptography over Finite Field

Zheng-jun Jing[1,2], Guo-ping Jiang[1] and Chun-sheng Gu[2]

[1] *College of Computer, Nanjing university of Posts and Telecommunications Nanjing, China*
[2] *School of Computer Engineering, Jiangsu Teachers University of Technology Changzhou, China*
jzjing@jstu.edu.cn,Jianggp@njupt.edu.cn,Guchunsehng@gamil.com

Abstract

A new ELGamal-type public key cryptosystem using ergodic matrix is proposed in this paper, which is based on isomorphism over finite field. The security of this scheme is equal to the intractability of polynomial discrete logarithm problem over finite field in the standard mode. At the same time, an optimization is described after the performance is analyzed in details. Since the ciphertext expand rate of new scheme is approximately 1, the proposed scheme can encrypt more information one time. Moreover, compared with the original ELGamal scheme, its security has been not reduced.

Keywords: *Public Key Encryption, Ergodic Matrix, Isomorphic over Finite Field, Polynomial Discrete logarithm.*

1. Introduction

We know that public key encryption has been a central notion in cryptography, and many of the exciting cryptographic applications in theory and practice are based on it, such as e-commerce and secure communication. 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 [2, 3] considered the methods to find ergodic matrix over finite field and constructed a new fast public key encryption algorithm as well as Shamir's three pass protocol [4]. Unfortunately, though there are many good properties about ergodic matrix, some of schemes have been proved to not be secure [5, 6].

In this paper, we attempt to present an alternative for the current schemes using ergodic matrix. We firstly review some definitions and properties about ergodic matrix. Then, a definition is introduced about the relation between the irreducibility of characteristic polynomial of ergodic matrix and polynomial finite field. According to it, a novel public key encryption scheme is presented over F_q, which secure is proved to be equivalent to the difficulty of polynomial discrete logarithm problem.

This paper is organized into five sections. Section 2 explains the relevant theorem about new scheme. Section 3, presents the proposed new scheme in detail, while section 4 make a special analysis about it. Section 5 concludes this paper.

1.1 Overview of Ergodic Matrix over F_p

Let F_p^n be the set of all n-dimensional column vectors over finite field F_p. The definition of ergodic matrix is as follow.

Definition 1[5]**:** Let $Q \in M_{n\times n}^{F_p}$, if for any nonzero n-dimensional column vector $v \in F_p^n \setminus \{0\}$, $Qv, Q^2v, \cdots Q^{p^n-1}v$ just exhaust $F_p^n \setminus \{0\}$, then Q is called an ergodic matrix over F_p, where $(0 = [0,0,\cdots 0]^T)$.

Theorem 1: $Q \in M_{n\times n}^{F_p}$ is an ergodic matrix if and only if the order of Q is $p^n - 1$ under multiplication of Q over F_p.

Theorem 2: If $Q \in M_{n\times n}^{F_p}$ is an ergodic matrix, then $(F_p(Q), +, \times)$ is a finite field with p^n elements, and $\{Q^0, Q^1, \cdots, Q^{n-1}\}$ is a basis of $F_p(Q)$.

The properties described above will be used in the new scheme. For the more details about ergodic matrix, the reader is referred to [7].

2. A Theorem About New Scheme

According to the fundamental properties of ergodic matrix and polynomial finite field, a theorem about ergodic matrix could be resulted.

Theorem 3: $A \in M_{n\times n}^{F_p}$ is an ergodic matrix if and only if its characteristic polynomial $\varphi(\lambda) = |\lambda I - A|$ is irreducible polynomial of degree n over F_p.

Proof: sufficiency. According to the Hemilton-Cayley theorem, we know that A is a root of $\varphi(\lambda)$, i.e. $\varphi(A) = 0$. Given $\varphi(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$ is a irreducible polynomial over F_p, according to the expanding field theorem [8], then $F_p(A)$ is a finite field with p^n members in which the set $\{A^0, A^1, \cdots, A^{n-1}\}$ is a base, and for any $v \in F_p(A)$ there is unique $a_0, a_1, \cdots a_{n-1} \in F_p$ such that $v = \sum_{i=0}^{n-1} a_i A^i$. So there is $A^{p^n-1} = I$ exactly. By Theorem 1, we know that $A \in M_{n\times n}^{F_p}$ is an ergodic matrix.

Necessity. Given $A \in M_{n\times n}^{F_p}$ is an ergodic matrix, then the order of A is $p^n - 1$. Without loss of generality, assume $\varphi(\lambda) = \tau(\lambda)\mu(\lambda)$ where both $\tau(\lambda)$ and $\mu(\lambda)$ are irreducible polynomial over F_p with $\deg(\tau(\lambda)) < n$ and $\deg(\mu(\lambda)) < n$. According to $\varphi(\lambda) = |\lambda I - A|$, we have $\varphi(A) = \tau(A)\mu(A) = 0$ by Hemilton-Cayley theorem. Hence, $\tau(A) = 0$ or $\mu(A) = 0$. Now, we assume $\tau(A) = 0$, then the process of sufficiency of poof shows that $F_p(A)$ is a finite field whose order is less than $p^n - 1$. Namely, the order of A is less than $p^n - 1$. This is a contradiction.

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

Proof: Given $\varphi(\lambda)=\lambda^n+c_{n-1}\lambda^{n-1}+\cdots+c_1\lambda+c_0$ is an irreducible polynomial over F_p with-$\deg(\varphi(\lambda))=n$, then the friend matrix B of $\varphi(\lambda)$ is $\begin{bmatrix}0&0&\cdots&0&-c_0\\1&0&\cdots&0&-c_1\\0&1&\ddots&\vdots&\vdots\\\vdots&\vdots&\ddots&0&-c_{n-2}\\0&\cdots&0&1&-c_{n-1}\end{bmatrix}$, where $c_i\in F_p$. According to the matrix theorem, we have that the characteristic polynomial of B is equal to $\varphi(\lambda)$, i.e. $|\lambda I-B|=\varphi(\lambda)$. By the theorem 3, we can not only get that $B\in M_{n\times n}^{F_p}$ is an ergodic matrix, but there is a finite field $F_p(B)$ with q^n members in which the set $\{B^0,B^1,\cdots,B^{n-1}\}$ is a base. It is also know that the set $\{1,\lambda,\cdots,\lambda^{n-1}\}$ is a base for the field $F_p[\lambda]\bmod\varphi(\lambda)$ by finite field theorem [8], therefore the two finite fields are isomorphic. In other words, the elements B^s of $F_p(B)$ is one-to-one corresponding to the remainder polynomial $g(\lambda)$ for the modulo $\varphi(\lambda)$, namely, $g(\lambda)=\lambda^s \bmod\varphi(\lambda)$ where - $0\le s<n$, i.e. $g(B)=B^s$.

3. A new Public Key Encryption Scheme over F_p

3.1. Public key encryption scheme

1. Key generation

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

2. Encryption

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

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

$$c_1(x)\equiv x^b\equiv a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \bmod f(x) \tag{1}$$

$$h(x)=(g(x))^b=x^{ab}\equiv a_{n-1}^{'}x^{n-1}+\cdots+a_1^{'}x+a_0^{'} \bmod f(x) \tag{2}$$

Step 2: Given B is a friend matrix induced by $f(x)$, according to Lemma 1, we can get the following equation.

$$H=h(B)=\sum_{i=0}^{n-1}a_i^{'}B^i \tag{3}$$

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

Here, $c_1(x)$ is polynomial of degree n over F_p, 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 F_p.Therefore, the encrypted space of new scheme is $(F_p^n,F_p^{n\times n})$.

3. Decryption

On input $C=(c_1,\mathrm{C}_2)$, $sk=\{a\}$, the message can be recovered exactly through the following steps.

Step 1 is to construct $c_1(x)$ from the c_1, and then we compute the polynomial $h'(x)$.

$$h'(x)=c_1^a(x)=(x^b)^a\equiv\sum_{i=0}^{n-1}a_i'x^i \bmod f(x) \tag{4}$$

Step 2 is to get the matrix H, that is $H=h'(B)=\sum_{i=0}^{n-1}a_i'B^i$. It is easy to identify that this polynomial $h'(x)$ is equal to $h(x)$ of the step 1 of encryption.

Step 3 is to recover the message Q through computing $Q=\mathrm{C}_2-H$.

3.2 Security

Through the process of encryption and decryption, it is easy to see that to find *sk* from *pk* is a polynomial discrete logarithm problem. Similarly, when adversary wants to get encryption key *b* from $c_1(x)$ and $f(x)$, he (or she) should have to solve the problem of polynomial discrete logarithm too. Therefore, the difficult to break the new scheme is not less than the difficult to solve the problem of polynomial discrete logarithm. According to [9], given $f(x)$ is an irreducible polynomial of degree n over F_p, then solving the polynomial discrete logarithm problem over the polynomial field $F_p[x] \bmod f(x)$ is equivalent to the problem of discrete logarithm over the finite field F_{p^n}. Therefore, we get a theorem about the security of new scheme.

Theorem 4: The difficulty of breaking new public key encryption scheme is not less than the difficult to solving the problem of discrete logarithm over the finite field F_{p^n}.

3.3 Example

Firstly, we select a positive integer private key $a=417352$ and an irreducible polynomial $f(x)$ of degree 9 over F_{251}, e.g. $f(x)=238+54x+137x^2+197x^3+154x^4+61x^5+212x^6+200x^7+114x^8+x^9$.

Then we compute $g(x)=x^{417352}\equiv 80+241x+68x^2+148x^3+157x^4+204x^5+157x^6+200x^7+64x^8 \bmod(f(x))$ and the friend matrix B induced by $f(x)$. Moreover, we need select a message matrix $Q\in M_{9\times 9}^{F_{251}}$ at random.

$$B=\begin{bmatrix}0&0&0&0&0&0&0&0&13\\1&0&0&0&0&0&0&0&197\\0&1&0&0&0&0&0&0&114\\0&0&1&0&0&0&0&0&54\\0&0&0&1&0&0&0&0&97\\0&0&0&0&1&0&0&0&190\\0&0&0&0&0&1&0&0&39\\0&0&0&0&0&0&1&0&51\\0&0&0&0&0&0&0&1&137\end{bmatrix},\quad Q=\begin{bmatrix}43&54&163&98&157&68&135&85&108\\138&104&18&47&12&2&114&198&219\\11&82&170&52&231&170&51&82&53\\247&204&173&209&15&234&91&126&34\\69&87&108&109&21&206&32&11&214\\121&32&50&47&11&54&199&247&83\\10&126&38&167&205&65&210&218&141\\240&65&231&233&234&40&1&31&8\\18&239&40&70&195&14&117&91&70\end{bmatrix}$$

In the progress of encryption, select a random positive integer $b = 513267$, then, compute $c_1(x), h(x)$ and H , respectively.

$$c_1(x) = x^b = x^{513267} \equiv 80 + 241x + 68x^2 + 148x^3 + 157x^4 + 204x^5 + 157x^6 + 200x^7 + 64x^8 \bmod(f(x))$$

$$h(x) = (g(x))^b \equiv 108 + 6x + 167x^2 + 225x^3 + 219x^4 + 51x^5 + 181x^6 + 58x^7 + 165x^8 \bmod f(x)$$

and $H = h(B) \equiv 108I + 6B + 167B^2 + 225B^3 + 219B^4 + 51B^5 + 181B^6 + 58B^7 + 165B^8 \pmod{251}$

Hence, the result of vector is $c_1^T = \begin{bmatrix} 80 & 241 & 68 & 148 & 157 & 204 & 157 & 200 & 64 \end{bmatrix}$, and the result of $C_2 = H + Q$ over F_{251} is:

$$C_2 = \begin{bmatrix} 43 & 191 & 108 & 146 & 145 & 72 & 176 & 218 & 36 \\ 144 & 230 & 229 & 5 & 245 & 12 & 218 & 92 & 207 \\ 178 & 73 & 84 & 124 & 161 & 245 & 73 & 78 & 30 \\ 163 & 245 & 90 & 110 & 153 & 142 & 66 & 44 & 175 \\ 43 & 195 & 202 & 249 & 180 & 7 & 188 & 13 & 174 \\ 172 & 232 & 223 & 244 & 188 & 177 & 20 & 223 & 56 \\ 191 & 86 & 73 & 233 & 115 & 3 & 145 & 217 & 152 \\ 47 & 127 & 149 & 186 & 195 & 236 & 235 & 63 & 100 \\ 183 & 61 & 63 & 127 & 176 & 133 & 50 & 182 & 19 \end{bmatrix}$$

It is easy to verify the process of decryption.

4. Performance Analysis and Optimization

In this section, we analyze the performance of the proposed encryption scheme and put forward an optimization.

1. Message expansion. The plaintext of new scheme proposed in the paper is an n-order matrix over F_p , so the bit size of message is $n^2 \log_2 p$. Since the ciphertext consists of a n dimensional vector and n order matrix, the size of ciphertext is $(n + n^2)\log_2 p$. Hence the message expansion is almost 1.

2. Complexity of time and space. Since encryption and decryption of the new public key encryption scheme proposed mainly involves the polynomial modulus computing and addition and multiplication of matrix over F_p , both of them have efficient algorithm to solve. Compared with the scheme described in [10], the new scheme just adds the operations of matrix. According to [6], for getting the matrix H , it should take almost $\Theta(n^4)$ time complexity and $\Theta(n^3)$ space complexity of byte in encryption and decryption, respectively.

3. Optimization. It can be found that the friend matrix B induced by $f(x)$ and the power of B^i is not changed during the encryption and decryption. Hence, some pre-processes can be done to promote the performance. That is to calculate and store each of the power of B^i before encryption and decryption. Of course, this method should spend some storing memories.

5. Conclusion

Though the previous design cryptographic schemes based on ergodic matrix is vulnerable to be attack by solving higher order leaner equation [2] [3], ergodic matrix over finite field has some good properties which can be used to design cryptographic primitives. The new ELGamal-type public key cryptosystem proposed in this paper just utilizes the irreducibility of characteristic polynomial of ergodic matrix. Since plaintext is represented by matrix and its ciphertext expand is almost 1, the novel scheme can encrypt more information one time. Moreover, compared with the original ELGamal scheme, its security has been not reduced.

Next, we will further study the choice of security parameters p and n to make the new scheme proposed more efficient without compromising the security, e.g. $p = 2$, that is over $GF(2)$.

References

[1] C. J. Monico, "Semi-rings and semi-group actions in public key cryptography", PhD. thesis, university of Notre Dame **(2002).**
[2] S. Pei, Y. Zhao and H. Zhao, "Public key cryptography based on ergodic matrices over finite field", Wuhan university journal of natural science **11(2006)** 1525-1528.
[3] S. Pei, Y. Zhao and H. Zhao, "Construct public key encryption scheme using ergodic matrices over GF(2)", Proceedings of 4th conference on theory and application of models of computation, **(2007)** May 22-25; Shanghai, China.
[4] Y. Z. Zhao, Z. H. Jiang and S. L Huang, "Implementation of Shamir's three pass protocol based on ergodic matrix over finite Field", Mini-Micro Systems **27 (2006)** 986-991.
[5] M. Rasslan and A. Youssef, "Cryptanalysis of a public key encryption scheme using ergodic matrices", IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences. **94 (2011)** 853-854.
[6] C. S. Gu, Z. M. Yu and Z. J. Jing, "Attack on shamir's three pass protocol of ergodic matrix over finite field", Journal of Chinese Computer Systems **32 (2011)** 1375-1378.
[7] Y. Zhao, S. Huang and Z. Jiang, "Ergodic matrix over and its properties", Mini-micro Systems **26 (2005)** 2135-2139.
[8] S. M. Shi, "The Introduction of Modern Algebra", Vol. 2. Higher Education Press, Beijing **(2006)**.
[9] A. Menezes, P. Van Oorschot and S.Vanstone, "Handbook of applied cryptography", CRC Press, New York **(1996)**.
[10] Q. P. Zhang, C. Y. Chen and L.S. Chen, "ElGamal cryptosystem and digital signature scheme based on polynomials over finite fields. Journal on Communications **26 (2005)** 69-72.

Authors

Jing Zhengjun is now working towards his Ph.D. degree in college of computer at Nanjing University of Posts and Telecommunications. His research interests include cryptographic applications and cloud computing security.

Jiang Guoping received his Ph.D. degree in automatic control theory and applications from Southeast University in 1997. Since 2003 he has been a professor in college of automation at Nanjing University of Posts and Telecommunications. His research interests include synchronization of chaotic systems and control, Complex network theory and its application.

Gu Chunsheng received his Ph.D. Degree from University of Science and Technology of China in 2005. Since 2008 he has been an associate professor in the School of Computer Engineering, Jiangsu Teachers University of Technology. His research interests are in the cryptanalysis and design of cryptography.