International Research Journal of Pure Algebra-4(11), 2014, 628-630
Available online through www.rjpa.info ISSN 2248–9037

A METHOD OF DESIGNING A PUBLIC-KEY CRYPTOSYSTEM BASED ON DISCRETE LOGARITHM PROBLEM

Lilly P.L.[1] and Saju M.I.*[2]

[1]Associate professor, Department of Mathematics, St. Joseph's College, Irinjalakuda, India.
[2]Assistant Professor, Department of Mathematics, St. Thomas' College, Thrissur. India.

(Received On: 10-11-14; Revised & Accepted On: 25-11-14)

ABSTRACT

In this paper we design a public key system based on the ring of polynomials over the field F_2 is developed. The security of the system is based on the difficulty of finding discrete logarithms over the function field F_{2^m} with sufficiently large m. The presented system has all features of ordinary public key cryptosystem.

Keywords: *Function Field, Polynomials over finite fields, public key cryptosystem, discrete logarithm problem.*

1. INTRODUCTION

A cryptosystem for message transmission means a map from units of ordinary text called plaintext message units to units of coded text called cipher text message units. The face of cryptography was radically altered when Diffie and Hellman invented an entirely new type of cryptography, called public key [Diffie and Hellman 1976][1]. At the heart of this concept is the idea of using a one-way function for encryption. The most common purposes for which public key cryptography has been applied are confidential message transmission, authentication, key exchange, coin flip, secret sharing and zero knowledge proof. There are public key cryptosystems and digital signature systems based on the discrete logarithm problem (DLP) such as Digital Signature Standard (DSS) [2], ElGamal cryptosystem and Diffie-Hellman key exchange system. The security of the new cryptosystem is based on DLP [6][4]. The main feature of the new system is that its public key encryption is computationally equivalent to EIGamal public key encryption, but signature verification is significantly faster than other analogous systems.

2. PUBLIC KEY CRYPTOSYSTEM

In this system we take a finite field $\frac{F_2[x]}{(f(x))}$, *where* $f(x)$ is a primitive polynomial of degree n will be considered as the base polynomial of the system [3][5]. Let α be a root of $f(x)$, k be any random number less than $2^n - 1$ where $(k, 2^n - 1) = 1$ and let $f_k(x)$ be a primitive polynomial with the root α^k. Let k be the secret parameter of the system and polynomials $f(x)$ and $f_k(x)$ *be public polynomials* of the system. Using the squaring-multiplying algorithm we can compute α^k, then we can express α^k as a polynomial $g(\alpha)$. However for a given $g(\alpha)$ to find k where $\alpha^k = g(\alpha)$ is a DLP.

Encryption: For a randomly generated N with n bits we have

$$x^N \equiv T(x) mod\ f(x) \tag{2.1}$$

and

$$x^N \equiv T_k(x) mod f_k(x). \tag{2.2}$$

It is easy to show that

$$T_k(x) \equiv (T(x^{k^{-1}}))^k\ mod\ f_k(x). \tag{2.3}$$

or

$$T(x) \equiv (T_k(x^k))^{k^{-1}} mod f(x) \tag{2.4}$$

where $k^{-1}k \equiv 1 \bmod (2^n - 1)$

Corresponding author:* **Saju M.I.*[2]
[2]Assistant Professor, Department of Mathematics, St. Thomas' College, Thrissur. India.

Suppose we want to encrypt the message *M*. We can express the message *M* as a polynomial $M(x)$ of degree n overF_2. The encryption process is the following:

$$\{M.\left(T(x)\right)^{-1},\ T_k(x^k)\} \tag{2.5}$$

or

$$\{M.\left(T_k(x)\right)^{-1},\ T\left(x^{k^{-1}}\right)\} \tag{2.6}$$

and the encrypted message is a pair as represented in (2.5) or (2.6).

Decryption: Using the secret key *k*, compute either $(T_k(x^k))^{k^{-1}}$ or $(T(x^{k^{-1}}))^k$ and can get M by multiplying the respective element with the first part of the encrypted message.

3. EXAMPLE

Let $f(x) = x^3 + x^2 + 1$ be the base polynomial of the system and we will denote by α a root of $f(x)$. Let k = 3 and let $f_3(x) = x^3 + x + 1$ be the primitive polynomial with the root α^3. Let k = 3 be the secret parameter of the system and polynomials $f(x)$ and $f_3(x)$ be public polynomials of the system.

Take N = $(101)_2$ = 5, we have,

$x^5 \equiv (x+1) mod(x^3 + x^2 + 1)$ and

$x^5 \equiv (x^2 + x + 1) mod(x^3 + x + 1)$. Here, $T(x) = x + 1$ and $T_3(x) = x^2 + x + 1$.

Then,

$x^2 + x + 1 \equiv (x^5 + 1)^3 mod(x^3 + x + 1)$ or

$x + 1 \equiv (x^6 + x^3 + 1)^5 mod(x^3 + x^2 + 1)$, where $3^{-1} = 5\ (mod 7)$.

Also, $T(x)^{-1} = x^2$ or $T_3(x)^{-1} = x^2 + 1$.

Let the message M that needs to be encrypted be represented as a polynomial $M(x) = x^3 + x + 1$. Then compute,

$$\{M(x).\left(T(x)\right)^{-1},\ T_3(x^3)\} = \{x^5 + x^3 + x^2, x^6 + x^3 + 1\} \tag{3.1}$$

Or

$$\{M(x).\left(T_3(x)\right)^{-1},\ T(x^5)\} = \{x^5 + x^2 + x + 1, x^5 + 1\} \tag{3.2}$$

The encrypted message is a pair as represented in (3.1) or (3.2).

Decryption is based on the fact that only the owner of the system knows the secret number 3 or 5 and having $T_3(x) = x^2 + x + 1$ or $T(x) = x + 1$ he can calculate either $(T_3(x^3))^5$ or $(T(x^5))^3$ and get M by multiplying the respective results with the first part of the encrypted message.

4. SECURITY OF THE SYSTEM

The security of the system is based on the discrete logarithm problem (DLP) over the function field F_{2^m}. Assuming that α is the root of the base primitive polynomial $f(x)$ and α^k is the root of the primitive polynomial $f_k(x)$.For a given α^k it is quite easy to construct its minimal polynomial $f_k(x)$ [7]. For a polynomial $f_k(x)$ its root as a polynomial $g(\alpha)$ can be found using the algorithm presented in [7]. The complexity of the algorithm is not more than O (t^3). However for a given $g(\alpha)$ to find $\alpha^k = g(\alpha)$is a DLP. The decryption process is difficult when we work in the field of size with prime extension to be equal at least to 2048 for example the field $F_{2^{2053}}$.

5. IMPLEMENTATION ASPECTS OF THE SYSTEM

The encryption process of this system has the same complexity as for the ElGamal type encryption. When comparing decryption operations we can conclude that the system presented here has about the same complexity compared with both RSA and ElGamal type decryption since both require one regular exponentiation.

6. CONCLUSION

In this paper a new public key system which is based on DLP is developed. The complexity of this system is based on the selection of the Function Field F_{2^m}. All public key operations of the presented system can be implemented virtually with the same complexity compared with existing systems.

REFERENCES

1. Diffie W., Helman M.E., New Directions in Cryptography, IEEE Transcations on information theory, Vol. IT-22, Nov.1976, 644-654.
2. Digital Signature Standard, Federal Information Processing Standards Publication 186, May 1994.
3. Lidl, Niederreiter (1997), Finite Fields (2^{nd} ed.), Cambridge University, Press.
4. McCurley K., The discrete logarithm problem, Proceedings of Symposia in Applies Mathematica, Vol.42, 1990, 49-74.
5. Neal Koblitz, Algebraic Aspects of Cryptography, Springer.
6. Odlyzko A., Discrete logarithms: The past and the Future; Designs, Codes and Cryptography, (2000), 129-145.
7. Taher ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE, Transactions on Information Theory, Vol. IT-31, n.4, 1985, 469-472, also in CRYPTO 84, 10-18, Springer-Verlag.

Source of Support: Nil, Conflict of interest: None Declared