ISSN: 2395-6607, Vol. 1, No. 1 March 2015, pp. 54–57

APPLICATION OF FUNCTION FIELDS IN A PUBLIC KEY CRYPTOSYSTEM

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

[1]Assistant Professor, Department of Mathematics, St. Thomas' College, Thrissur, India

[2]Associate Professor, Department of Mathematics, St. Joseph's College, Irinjalakuda, India

Abstract—*The function field has an important role in cryptography. One of the classical problems in mathematics is the Discrete Logarithm Problem (DLP).The difficulty and complexity for solving DLP is used in most of the cryptosystems. In this paper we design a public key system based on the ring of polynomials over the field F_p is developed. The security of the system is based on the difficulty of finding discrete logarithms over the function field F_{p^n} with suitable prime p and sufficiently large n.*

The presented system has all features of ordinary public key cryptosystem.

Keywords: *Discrete Logarithm Problem, Function Field, Polynomials Over Finite Fields, Primitive Polynomial, Public Key Cryptosystem*

INTRODUCTION

For the construction of a public key cryptosystem, we need a finite extension field F_{p^n} overF_p. In our paper [1] we design a public key cryptosystem based on discrete logarithm problem over the field F_2. Here, for increasing the complexity and difficulty for solving DLP, we made a proper additional modification in the system. 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][2]. 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) [3], ElGamal cryptosystem and Diffie-Hellman key exchange system. The security of the new cryptosystem is based on DLP [4][5]. The main feature of the new system is that its public key encryption is computationally equivalent to ElGamal public key encryption.

PUBLIC KEY CRYPTOSYSTEM

In this system we take a finite field $\frac{F_p[x]}{(f(x))}, where\ f(x)$ is a primitive polynomial of degree n will be considered as the base polynomial of the system [6] [7]. Let α be a root of $f(x)$, k be any random number less than $p^n - 1$where $(k, p^n - 1) = 1$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 algorithm [8] 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

Let M be the message to be encrypted. Then the values,

$$x^M \equiv T(x) mod\, f(x) \quad (1)$$

and

$$x^M \equiv T_k(x) mod f_k(x) \quad (2)$$

are calculated.

It is easy to show that

$$T_k(x) \equiv (T(x^{k^{-1}}))^k \, mod\, f_k(x) \quad (3)$$

or

$$T(x) \equiv (T_k(x^k))^{k^{-1}} mod f(x) \quad (4)$$

Where, $k^{-1}k \equiv 1 \bmod (p^n - 1)$

The encrypted message will then be a pair:

$$\{M \oplus T(x), T_k(x^k)\} \quad (5)$$

or

$$\{M \oplus T_k(x), T(x^{k^{-1}})\} \quad (6)$$

Decryption

Decryption is based on the fact that only the "owner" of the system knows k or $k^{-1}$and having $T_k(x)$ or $T(x)$can calculate either $(T_k(x^k))^{k^{-1}}$ or $(T(x^{k^{-1}}))^k$ and can get *M* by XOR-ing the respective results with the first part of the encrypted message.

EXAMPLE

Here p=2 and we take the finite field $\frac{F_2[x]}{(f(x))}$, where $f(x) = x^3 + x^2 + 1$ 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.

Let M = $(101)_2$ = 5 is the message to be encrypted. Then compute the values $x^5 \equiv (x + 1) mod (x^3 + x^2 + 1)$ 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 $3^{-1} = 5\ (mod 7)$.

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

$$\{M(x) \oplus T(x), T_3(x^3)\} = \{x^3 + x, x^6 + x^3 + 1\} \quad (7)$$

or

$$\{M(x) \oplus T_3(x), T(x^5)\} = \{x^3 + x^2 + x, x^5 + 1\} \quad (8)$$

The encrypted message is a pair as represented in (7) or (8).

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 XOR-ing the respective results with the first part of the encrypted message.

EXAMPLE

Here p=2 and we take the finite field $\frac{F_2[x]}{(f(x))}$, where $f(x) = x^8 + x^6 + 1$ be the base polynomial of the system and we will denote by α a root of $f(x)$. Let k = 4 and let $f_4(x) = x^4 + x^3 + 1$ be the primitive polynomial with the root α^4. Let k = 4 be the secret parameter of the system and polynomials $f(x)$ and $f_4(x)$ be public polynomials of the system.

Let M = $(11111)_2$ = 31 is the message to be encrypted. Then compute the values $x^{31} \equiv x\, mod(x^8 + x^6 + 1)$ and $x^{31} \equiv x\, mod(x^4 + x^3 + 1)$. Here, $T(x) = x$ and $T_4(x) = x$.

Then,

$x \equiv (x^{64})^4 mod(x^4 + x^3 + 1)$ Or

$x \equiv (x^4)^{64} mod(x^8 + x^6 + 1)$, where $4^{-1} = 64\ (mod 255)$.

Let the message M that needs to be encrypted be represented as a polynomial $M(x) = x^4 + x^3 + x^2 + x + 1$. Then compute,

$$\{M(x) \oplus T(x), T_4(x^4)\} = \{(x^4 + x^3 + x^2 + x + 1) \oplus x, x^4\} \quad (9)$$

or

$$\{M(x) \oplus T_4(x), T(x^{64})\} = \{(x^4 + x^3 + x^2 + x + 1) \oplus x,\ x^{64}\} \quad (10)$$

The encrypted message is a pair as represented in (9) or (10).

Decryption is based on the fact that only the owner of the system knows the secret number 4 or 64 and having $T_4(x) = x$ or $T(x) = x$ he can calculate either $(T_4(x^4))^{64}$ or $(T(x^{64}))^4$ and get M by XOR-ing the respective results with the first part of the encrypted message.

SECURITY OF THE SYSTEM

The security of the system is based on the discrete logarithm problem (DLP) over the function field F_{p^n}. 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 $f_k(x)$ [8]. For a polynomial $f_k(x)$ its root as a polynomial $g(\alpha)$ can be found using the algorithm presented in [8]. 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..

IMPLEMENTATION ASPECTS OF THE SYSTEM

An encryption operation of this system according to the formulae (5) or (6) is just XOR-ing. The encryption or decryption process of this system has the same complexity as for the ElGamal type encryption or decryption. 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. Here the encryption is faster than the encryption in [1].

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_{p^n}. In this system the selection of the prime number p and the exponent n has an important role. All public key operations of the presented system can be implemented virtually with the same complexity compared with existing systems. The concept used in this system may useful in the construction of digital signature and the process of hashing.

REFERENCES

Lilly P.L, Saju M.I., A method of designing a public-key cryptosystem based on discrete logarithm problem, *IRJPA-4(11),* 2014, 628-630.

Diffie W., Helman M.E., New Directions in Cryptography, *IEEE Transactions on information theory*, *Vol. IT-22*, Nov.1976, 644-654.

Digital Signature Standard, *Federal Information Processing Standards Publication 186*, May 1994.

Odlyzko A., *Discrete logarithms: The past and the Future; Designs, Codes and Cryptography, (2000),* 129-145.

McCurley K., The discrete logarithm problem, *Proceedings of Symposia in Applies Mathematica*, *Vol.42*, 1990, 49-74.

Lidl, Niederreiter (1997), *Finite Fields (2nd ed.),* Cambridge University, Press.

Neal Koblitz, *Algebraic Aspects of Cryptography*, Springer.

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.