Key Distribution and Agreement Diffie – Hellman Over Polynomial Rings with Two Cyclomic Cossets

Le Danh Cuong[1], Nguyen Le Cuong[2], Nguyen Binh[1]*

[1]*Posts and Telecommunications Institute of Technology,* [2]*Electric Power University*

Received: June 27, 2017; Accepted: November 03, 2017

Abstract

In this paper, we introduce a D-H key distribution protocol over polynomial rings. These protocols use some polynomials with two cyclomic cosets in the center of the ring as part of the private keys. We give some examples over the polynomial rings Zp, where p is a prime number. We also give a security analysis of the proposed protocols and conclude that the only possible attack is by brute force. In this paper, D-H key distribution and agreement protocols are also described in PR with two cyclotomic cosets based on DLP. DLP over number rings is important problem in public-key cryptography.This DLP is studied in the case of polynomial rings with two cyclotomic coset.

Keywords: key distribution, authentication, discrete logarithm problem, polynomial rings, cyclotomic coset

1. Introduction

The ElGamal protocol [2] and all its variants are based on the Discrete Logarithm Problem (DLP) over a finite field Zp, here p is a large prime. The discrete logarithm problem (DLP) in a finite cyclic group G is an algorithmic question to find for any given pair of elements g,h∈G a number n∈N satisfying gn = h. This problem is extremely important due to its relation to cryptography. One of the most prominent and long withstanding protocols, the Diffie-Hellman key-exchange protocol, is based on the assumption that DLP is hard in certain groups. The Diffie-Hellman protocol proposed in [3] was the first practical solution to the key distribution problem, allowing two parties, never having met in advance or shared keying material, to establish a shared secret by exchanging messages over an open channel [4].

Since Diffie and Hellman [5] proposed the first key exchange algorithm, we can find an extensive bibliography on the problem of key exchange protocols in public key cryptography (see, for example, [6, 7, 8] and the references therein). Most of proposed algorithms are related to arithmetic operations on commutative algebraic structures and some efficient attacks based on the commutative property of these structures are well known.

It is believed that the increasing computing power of modern computers has made these techniques less secure (see, for example, [9, 10]). As a consequence of this, there exists an active field of research known as noncommutative algebraic cryptography, aiming to develop and analyze new cryptosystems and key exchange protocols based on noncommutative cryptographic platforms.

The main idea of this work is the design of some public key exchange protocols over polynomial rings with two cyclomic cosets, in particular over the ring of endomorphisms of Zp where p is a prime number. This last property is what makes this ring very interesting for cryptographic applications.

2. DLP problems over polynomial rings with two cyclotomic cosets.

2.1. PR with 2 cyclotomic cosets $\mathbb{Z}_2[x]/(x^n+1)$

Definition 1[1]: PRs with 2 cyclotomic cosets are PRs satisfying the following factoring:

$$x^n + 1 = (x + 1)\sum_{i=0}^{n-1} x^i \quad (1)$$

Here,$(x + 1)$and $\sum_{i=0}^{n-1} x^i$ are irreducible polynomials.

Example: n = 5, 11, 19, 29, 31,…

$x5 + 1 = (x+1)(x^4 + x^3 + x^2 + x + 1)$

Lemma 1: in PRs with 2 cyclotomic cosets we have following maximum decomposition

With $|A| = |\bar{A}| = 2^{n-1} - 1 = \max \text{ord } a(x), a(x) \in \mathbb{Z}_2[x]/(x^n + 1)$

A
$\bar{A}$
$e_0(x)$

* Corresponding author: Tel.: (+84) 913.546.234
Email: cuongnl@epu.edu.vn

A – cyclic multipicative group

$\overline{A}$ – symmetric cyclic multiplicative group of A.

$$A = \{a^i(x), i = 1,2, \dots, 2^{n-1} - 1\}$$

$$\overline{A} = \{\bar{a}^i(x), i = 1,2, \dots, 2^{n-1} - 1\}$$

Definition 2: Swallowing idempotent e0(x).

$e_0(x) = \sum_{i=0}^{n-1} x^i$ is called swallowing idempotent.

We have:

$$f(x).e_n(x) = \begin{cases} e_n(x) & \text{if } W(f(x)) \text{odd} \\ 0 & \text{if } W(f(x)) \text{even} \end{cases} \quad (2)$$

Definition 3: Polynomial $\bar{a}(x)$ is called symmetric polynomial of a(x), if $a(x) = \sum_{i \in I} a_i x^i$

Then $\bar{a}(x) = \sum_{j \in J} a_j x^j$ (3)

In which, $I \cap J = \phi$; $I \cup J = \mathbb{Z}n$.

On the other hand

$$\bar{a}(x) = e_n(x) + a(x)$$

2.2. Discrete logarithm problem (DLP) in PRs with 2 cyclotomic cosets

DLP in $\mathbb{Z}p$ is described in [1], in this part, we describe DLP in $\mathbb{Z}_2[x]/(x^n+1)$.

Problem instance: $\mathbb{Z}_2[x]/(x^n+1)$ – PR with two cyclotomic cosets, a(x) is a primitive element of CGP A with maximum order.

Objective: Find the unique integer k, $0 \le k \le 2n-1-1$ such that $a^k(x) \equiv b(x) \bmod (x^n + 1)$.

We will denote this integer K by $\log_{a(x)} b(x)$.

Remark:

If W(a(x)) is odd, the W (b(x)) odd.

If W (a(x)) is even, then W (b(x)) even.

Example: let $\mathbb{Z}_2[x]/(x^n + 1) = \mathbb{Z}_2[x]/(x^5 + 1)$

$$a(x) = 1 + x^2 + x^4$$

We have $7 = \log_{a(x)}(x + x^2 + x^4)$

DLP in PR with 2 cyclotomic cosets is hard if n is sufficient large.

Generally, DLP in PR with 2 cyclotomic cosets is easier than DLP in GF(p)

$$i = \log_{a(x)} a^i(x) = \log_{\bar{a}(x)} \bar{a}^i(x)$$

$K = \log_{x^j} x^i; K \in \{1,2, \dots, n-1\}$ Since $n | (2^{n-1} - 1)$

Easy problem: $\mathbb{Z}_2[x]/(x^n + 1)$ – PR with two cyclotomic cosets; p=2n-1 –1 is a Mersenne prime; $a(x) \in \mathbb{Z}_2^*[x]/(x^n + 1)$.

Compute ai(x) (according to the repeated square and multiply algorithm for exponentiation).

Hard problem: Compute i = loga(x)b(x).

3. D-H key distribution and agreement protocol over PRs with two cyclotomic cosets.

3.1. D-H key distribution and agreement protocol without authentication

Let $\mathbb{Z}_2[x]/(x^n + 1)$ – PR with 2 cyclotomic cosets

$a(x) \neq 0, a(x) \neq e_0(x), a(x) \in \mathbb{Z}_2[x]/(x^n + 1)$ is a primitive element of A.

A and B are agreement with common key K of private key cryptosystem according to the following protocol

Remark:

This protocol is secure provided DLP in $\mathbb{Z}_2[x]/(x^n + 1)$ is intractive. Both A and B are assured of key fresh new, since the session key depends on both random exponents i and j.

This protocol is not authentication and vulnerable to an active adversary who uses an intruder in the middle attack.

Table 1. D-H key distribution and agreement protocol without authentication

A	B
A chooses a random i ($0 < i < 2^{n-1} - 1$) and computes $a^i(x) \bmod (x^n + 1)$	B chooses a random j ($0 < j < 2^{n-1} - 1$) and computes $a^j(x) \bmod (x^n + 1)$
A computes $K(x) = [a^j(x)]^i \bmod (x^n + 1) = a^{i+j}(x) \bmod (x^n + 1)$	
	B computes $K(x) = [a^i(x)]^j \bmod (x^n + 1) = a^{i+j}(x) \bmod (x^n + 1)$

Table 2. D-H key pre-distribution in PR with two cyclotomic cosets

A	B
A chooses i = 7 and compute $(1+x^2+x^4)^7 \bmod (x^5+1) = x+x^2+x^4 = ID(A)$	B chooses j = 5 and compute $(1+x^2+x^4)^5 \bmod (x^5+1) = x+x+x^4 = ID(B)$
A receives ID(B) and computes $K(x) = [ID(B)]^7 \bmod (x^5+1) = (1+x+x^4)^7 \bmod (x^5+1) = 1+x+x^4$	
	B receives ID(A) and computes $K(x) = [ID(A)]^5 \bmod (x^5+1) = (1+x+x^4)^5 \bmod (x^5+1) = 1+x+x^4$

3.2. D-H key pre-distribution in PR with two cyclotomic cosets

For authentication we can use the following protocol:

$\mathbb{Z}_2[x]/(x^n+1)$ – PR with two cyclotomic cosets

A chooses a random i and computes

$$ID(A) = a^i(x) \bmod (x^n+1)$$

Also, B chooses a random j and computes

$$ID(B) = a^j(x) \bmod (x^n+1)$$

Values ID(A) and ID(B) are made public.

A computes

$$K(x) = [ID(B)]^i \bmod (x^n+1)$$

Also, B computes

$$K(x) = [ID(B)]^i \bmod (x^n+1)$$

Example: let $\mathbb{Z}_2[x]/(x^n+1) = \mathbb{Z}_2[x]/(x^5+1)$

$$a(x) = 1+x^2+x^4$$

Remark:

- This protocol is secure against a passive adversary if DLP in PR with two cyclotomic cosets is intractive.

- This is an authentication protocol with communication parties A and B.

- Similary, we can construct a D-H protocol with recipient authentication.

In this protocol, used key is defined in different communication sessions.

3.3. D-H Key Distribution with receipient authentication

Key generation

- A chooses a PR with two cyclotomic cosets $\mathbb{Z}_2[x]/(x^n+1)$ and a primitive element $a_A(x)$.

- A chooses a random iA ($0 \le i_A \le 2^{n-1}-1$) and computes

$$b_A(x) = a_A^{i_A}(x) \bmod (x^n+1)$$

A's public key $(\mathbb{Z}_2[x]/(x^n+1), a_A(x), b_A(x))$

Key distribution from B to A

- B chooses a random j_B ($0 \le j_B \le 2^{n-1}-1$) and computes

$$\gamma_B(x) = a_B^{j_B}(x) \bmod (x^n+1)$$

- B sends $\gamma_B(x)$ to A if $w(\gamma_B(x))$ is odd.

- If $w(\gamma_B(x))$ is even then $\gamma_B(x) := \overline{\gamma_B}(x)$.

Remark:

This protocol is used in ElGamal cryptosystem [2].

4. Conclusions

In this paper, we have shown how polynomial rings can be used in order to provide protocols for making D-H key distribution that allow a key exchange in a secure manner. Such protocols can be used in ElGama cryptosystems also provided secure solutions for DLP problems by constructing from two polynomial cosets. It is also clear how to describe the protocol to operate type of security.

References

[1]. Bac Dang Hoai.Cyclic and local cyclic codes over polynomial rings with two cyclotomic cosets. Doctor Thesis, PTIT, 2010.

[2]. T. ElGamal. “A public key cryptosystem and a signature scheme based on discrete logarithms”. IEEE Transactions on Information Theory, 31(4), 469-472 (1985).

[3]. R. Alvarez, L. Tortosa, J. Vicent and A. Zamora. “A non-abelian group based on block upper triangular matrices with cryptographic applications”. In M. Bras-Amoros and T. Hoholdt (editors), Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, volume 5527 of Lecture Notes in Computer Science, pages 117-126. Springer-Verlag, Berlin, 2009.

[4]. J.-J. Climent, P. R. Navarro and L. Tortosa. “Key exchange protocols over noncommutative rings”. The case End(Zp ×Zp2). In J. Vigo Aguiar (editor), Proceedings of the 11th International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2011), pages 357-364. 2011.

[5]. W. D. Diffie and M. E. Hellman. “New directions in cryptography”. IEEE Transactions on Information Theory, 22(6): 644{654 (1976).

[6]. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, Boca Raton, FL, 1996.

[7]. B. Schneier. Applied Cryptography. John Wiley & Sons, New York, NY, second edition, 1996.

[8]. D. R. Stinson. Cryptography. Theory and Practice. CRC Press, Boca Raton, FL, 1995.

[9]. D. Boneh and R. J. Lipton, “Quantum cryptanalysis of hidden linear functions”. In D. Coppersmith (editor), Advances in Cryptology, CRYPT0 '95, volume 963 of Lecture Notes in Computer Science, pages 424-437. Springer-Verlag, Berlin, 1995.

[10]. P. W. Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”. SIAM Journal on Computing, 26(5): 1484-1509 (1997).

[11]. Nguyen Trung Hieu, Nguyen Van Tung, Nguyen Binh, “A classification of Linear Codes based on Algebraic Structures and LCC”, Proceeding of ATC 2014