Key Exchange by Chebyshev Polynomials modulo 2^w

Ken Umeno
National Institute of Information and Communications Technology and ChaosWare, Inc.
4-2-1 Nukui Kitamachi Koganei Tokyo 184-8795 Japan
E-mail: umeno@nict.go.jp

Abstract

We show that Chebyshev polynomials of odd degree are permutable permutation polynomials modulo 2^w. We use this fact to construct a new key exchange algorithm.

Keywords: Chebyshev polynomials, Diffie-Hellman key exchange algorithm, Permutation polynomials, Public Key Cryptosystems

1 Introduction

A Chebyshev polynomial $T_d(x)$ of degree d is given by the multiplication formula $\cos(dx) = T_d(\cos(x))$. Chebyshev polynomials have been used for many engineering applications such as functional approximations, digital filter design, and e.t.c. These applications extensively use the fact that Chebyshev polynomials are permutable polynomials $T_p \circ T_q = T_q \circ T_p$ by definition and they have orthogonal properties. Examples of Chebyshev polynomials are given by

$$T_0(x) = 1, T_1(x) = x, T_2(x) = 2x^2 - 1, T_3(x) = 3x - 4x^3, \cdots. \tag{1}$$

In this paper, we prove that a Chebyshev polynomial $T_p(x)$ modulo 2^w is a permutation polynomial if and only if p is odd. Thus, odd degree Chebyshev polynomial modulo 2^w can be used for cryptgraphic applications efficiently implemented by modern computers and modern digital signal processing chips.

2 Chebyshev Polynomials modulo 2^w.

A polynomial $T(x)$ is said to be a permutation polynomials over a finite ring R if T permutes the elements of R. Many cryptographic algorithms such as RSA cryptosystems and RC6 block cipher essentially use permutation polynomials[1]. In this section we prove that Chebyshev polynomials of odd degree are also permutation polynomials module 2^w.

First, we prove the case of $T_1(x)$.

Lemma 2.1 *The first order Chebyshev polynomial $T_1(x) = x$ is a permutation polynomial modulo $n = 2^w$, where w is an integer greater than or equal to 2.*

Proof: Trivial, since $T_1(x) = x$ is an identity mapping modulo 2^w. ▮

Recently, Rivest proved the following theorem.

Theorem 1 (Rivest, 1999) *Let $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ be a polynomial with integral coefficients. Then $P(x)$ is a permutation polynomial modulo $n = 2^w, w \geq 2$, if and only if a_1 is odd, $(a_2 + a_4 + a_6 + \cdots)$ is even, and $(a_3 + a_5 + a_7 + \cdots)$ is even.*

By using this theorem 1, we can prove the following lemmas.

Lemma 2.2 *A Chebyshev polynomial of an even number degree is not a permutation polynomial modulo $n = 2^w$, where $w \geq 2$.*

Proof: A Chebyshev polynomial of the p-th degree is given by the fomula:

$$T_p(x) = \sum_{s=0}^{[p/2]} (-1)^s \binom{p}{2s} (1 - x^2)^s x^{p-2s}. \tag{2}$$

Thus, if p is even, then $T_p(x)$ has no terms of odd degree. This means that T_p is not a permutation polynomial modulo $n = 2^w, w \geq 2$ by using the necessary and sufficient condition in Theorem 1. ▮

Lemma 2.3 *Let p be an odd integer satisfying $p \geq 1$. If $T_p(x)$is a permutation polynomial modulo $n = 2^w, w \geq 2$, then $T_{p+2}(x)$ is also a permutation polynomial modulo $n = 2^w, w \geq 2$.*

Proof: Let $T_p(x) = a_0 + a_1 x + \cdots + a_p x^p$ and $T_{p+2}(x) = b_0 + b_1 x + \cdots + b_{p+2} x^{p+2}$. Suppose that $T_p(x)$ is a permutation polynomial modulo $n = 2^w, w \geq 2$. This means that a_1 is odd, $(a_2 + a_4 + a_6 + \cdots + a_p)$ is even, and $(a_3 + a_5 + a_7 + \cdots + a_{p-1})$ is even by Theorem 1.

It is well-known that Chebyshev polynomials have the following recursion relation

$$T_{p+2}(x) = 2xT_{p+1}(x) - T_p(x). \tag{3}$$

Since $xT_{p+1}(x)$ are composed of terms with even number coefficients , b_1 is odd, $(b_2 + b_4 + b_6 + \cdots + b_{p+2})$ is even, and $(b_3 + b_5 + b_7 + \cdots + b_{p+1})$ is even. Thus, we conclude that $T_{p+2}(x)$ is also a permutation polynomial modulo $n = 2^w, w \geq 2$ by Theorem 1. ▮

By using Lemma 2.1 and Lemma 2.3, we have the following lemma:

Lemma 2.4 *Let p be an odd integer satisfying $p \geq 1$. Then, $T_p(x)$ is a permutation polynomial modulo $n = 2^w, w \geq 2$.*

Finally, we obtain the theorem with combination of lemma 2.2 and 2.4.

Theorem 2 *A Chebyshev polynomial $T_p(x)$ is a permutation polynomial modulo $n = 2^w, w \geq 2$, if and only if p is odd.*

If $x \in \boldsymbol{Z}_{2^w}$ iterates as

$$x' = T_p(x) \mod 2^w, \tag{4}$$

this iteneracy will be periodic with some periodicity.

3 Key Exchange Algorithm

Chebyshev polynomials have the following commutativity [2].

$$T_l \circ T_m(x) = T_m \circ T_l(x) = T_{ml}(x), \tag{5}$$

which means that Chebyshev polynomials are permutable modulo 2^w. Let say that

$$S_p(x) \equiv T_p(x) \bmod 2^w. \tag{6}$$

We have the commutativity relation modulo 2^w as follows.

$$S_l \circ S_m(x) \equiv S_m \circ S_l(x) \equiv S_{ml}(x) \tag{7}$$

where $x \in \boldsymbol{Z}_{2^w}$.

Thus, we can construct new key exchange algorithms based on such permutable permutation polynomials modulo 2^w by using Chebyshev polynomials in the similar way of Diffe-Hellman algorithm [3]. Note that a dynamical system generated by Chebyshev polynomials are known to be ergodic (thus, chaotic). This shows a possibility of constructing new public key algorithm based on chaotic mapping over a finite field as well as the patented new public key encryption algorithm [4] based on exactly solvable chaos mapping [5].

We propose a new key exchange algorithm based on Chebyshev polynomials over a finite field. This all works because of the commutativity of Chebyshev polynomials over a finite field and the proven fact that Chebyshev polynomials are permutation polynomials modulo 2^w if and only if the degree is odd. This class of key exchange algorithm is an interesting class for further study because of mathematical structure in permutable permutation of Chebyshev polynomials. Such kind of key exchange algorithm based on permutable permutation polynomials module 2^w has a strong potential to be implemented very efficiently as compared with the Diffie-Hellman and the RSA Key exchanges.

References

[1] R. L. Rivest,"Permutation Polynomials Modulo 2^w",in *Finite Fields and their Applications* **vol.7** (2001) pp.287-292.

[2] J. F. Ritt,"Permutable rational functions",*Trans. Amer. Math. Soc.* **25** (1923) pp.399-448.

[3] W. Diffie and M. E. Hellman, "New directions in cryptography",*IEEE Trans. Inform. Theory* **22** (1976) pp.654-654.

[4] K. Umeno, Japanese Patent No. 3455483 granted on July 25, 2003.

[5] K. Umeno, "Method of constructing exactly solvable chaos",*Physical Review***E 55** (1997) pp.5280-5284.