On some properties of Chebyshev polynomial sequences modulo $2^k$

Daisaburo Yoshioka$^1a)$ and Yuta Dainobu

$^1$Department of Information and Computer Sciences, Sojo University
4-22-1 Ikeda, Nishi-ku, Kumamoto 860-0082, Japan

$^a$yoshioka@cis.sojo-u.ac.jp

Received September 18, 2014; Revised January 28, 2015; Published July 1, 2015

Abstract: In this paper, we give a characterization of permutation polynomials modulo $2^k$: the period of sequences generated by iterating such polynomials is a power of two. Chebyshev polynomials are examples of such polynomials. Based on these findings, we also evaluate the factual key space of a recently proposed key exchange protocol based on Chebyshev polynomials modulo $2^k$.

Key Words: Chebyshev polynomials, permutation polynomials, period

1. Introduction

Chebyshev polynomials have been used for many engineering applications such as functional approximation, digital filter design, and so on. Chebyshev polynomials are also famous examples of one-dimensional chaotic systems which generate random behavior and unpredictable trajectories in spite of being deterministic. Due to these properties, Chebyshev polynomials have become a good candidate for their use particularly in the field of pseudorandom number generation [1] and cryptography [2].

Since these applications are composed of digital architecture, Chebyshev polynomials should be defined on a finite phase space. So far, Chebyshev polynomials over a finite field or a finite ring have been proposed [3–5]. Particularly, applications based on Chebyshev polynomials modulo $2^k$ have a potential to be implemented very efficiently in modern computers. We think in the study of such applications, a central problem is the calculation and classification of the periodic sequences composed by Chebyshev polynomials over finite sets (called Chebyshev polynomial sequence in the following discussion). So far, the periodicity of Chebyshev polynomials over finite sets and its effect on security of cryptosystems based on Chebyshev polynomials had been studied [6–9]. The main contribution of this paper is that we give a characterization of permutation polynomials modulo $2^k$: the period of sequences generated by iterating such polynomials is a power of two [10]. Based on the finding, we clarify some properties of Chebyshev polynomial sequences modulo $2^k$.

This is the outline of the paper. In Section 2 we briefly introduce Chebyshev polynomials. In Sect.3, we characterize permutation polynomials which generate periodic sequences with length of a power of two. By that means, we derive some properties of Chebyshev polynomial sequences modulo $2^k$. The factual key space of the key exchange protocol proposed in [4] is also analyzed. Finally the report concludes with the summary in Section 4.
2. Chebyshev polynomials

In this section, we briefly give the definition and properties of Chebyshev polynomials [11].

**Definition 1** Let \( n \geq 0 \) be an integer. Chebyshev polynomial \( T_n(x) \) is a polynomial in \( x \) of degree \( n \), defined by the relation

\[
T_n(x) = \cos n\theta \quad \text{when} \quad x = \cos \theta. \tag{1}
\]

It has been known that \( \cos n\theta \) is a polynomial of degree \( n \) in \( \cos \theta \), that is,

\[
\cos 0\theta = 1, \quad \cos 1\theta = \cos \theta, \quad \cos 2\theta = 2\cos^2 \theta - 1, \quad \cos 3\theta = 4\cos^3 \theta - 3\cos \theta, \ldots
\]

We may immediately deduce from Eq.(1) that the first few Chebyshev polynomials are obtained as the following list

\[
\begin{align*}
T_0(x) &= 1, \\
T_1(x) &= x, \\
T_2(x) &= 2x^2 - 1, \\
T_3(x) &= 4x^3 - 3x, \\
T_4(x) &= 8x^4 - 8x^2 + 1, \\
T_5(x) &= 16x^5 - 20x^3 + 5x.
\end{align*}
\]

By combining the trigonometric identity

\[
\cos n\theta + \cos(n - 2)\theta = 2 \cos \theta \cos(n - 1)\theta
\]

with Definition 1, we obtain the fundamental recurrence relation

\[
T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x), \quad n = 2, 3, \ldots. \tag{2}
\]

Eq.(2) recursively generates all the polynomials \( \{T_n(x)\}_{n=0}^{\infty} \) very efficiently. Figure 1 shows examples of the first few Chebyshev polynomials \( T_n(x) \) in the domain \( x \in [-1, 1] \). Chebyshev polynomial restricted in \([-1, 1]\) is a well-known chaotic map for all \( n \geq 2 \).

One of the most important properties of Chebyshev polynomials is the semi-group property, that is, the compositions of Chebyshev polynomials are also Chebyshev polynomials. In particular,

\[
T_n \left( T_m(x) \right) = T_{m \cdot n}(x), \tag{3}
\]

which can be deduced from Eq.(1). Chebyshev polynomials are commute under composition:

\[
T_n(T_m) = T_m(T_n). \tag{4}
\]

This commutative property allows the construction of a public-key cryptosystem [2, 4].

2.1 Chebyshev polynomials modulo \( 2^k \)

Let \( \mathbb{Z} \) be the set of all integers. For a positive integer \( k \), we consider Chebyshev polynomials over the residue ring \( R = \mathbb{Z}/2^k\mathbb{Z} \) as

\[
y = T_n(x) \mod 2^k. \tag{5}
\]

Chebyshev polynomials over \( R \) commute under composition and have the semi-group property [3], that is,

\[
T_n \left( T_m(x) \right) \equiv T_m \left( T_n(x) \right) \equiv T_{m \cdot n}(x) \mod 2^k. \tag{6}
\]

A polynomial \( P(x) \) is said to be a **permutation polynomial over** \( R \) if \( P(x) \) permutes the elements of \( R \). Many cryptographic algorithms such as RSA cryptosystems and RC6 block cipher essentially use permutation polynomials [12]. Umeno showed the following.
Fig. 1. Examples of the first few Chebyshev polynomials $T_n(x)$ for $n = 2, 3$ and 4.

Lemma 1 (Umeno [4]) A Chebyshev polynomial $T_n(x)$ is a permutation polynomial modulo $2^k$, $k \geq 2$, if and only if $n$ is odd.

Thus, we assume that $n$ is odd hereafter.

The $i$th iterate of $T_n$ is denoted by $T_i^n$: $$T_0^n(x) = x$$ and $$T_i^n(x) = T_n(T_{i-1}^n(x)),$$ for $i = 1, 2, \ldots$. (7)

We can generate an integer periodic sequence $\{T_i^n(x)\}_{i=0}^{N-1}$ by iterating Eq. (5) from an initial value $x$, where the period length $N$ is defined as the least positive number such that $T_N^n(x) \equiv x \mod 2^k$.

We now present examples. The periodic sequences $\{T_i^3(x)\}_{i=0}^{N-1}$ with $x = 2$ and $\{T_5(x)\}_{i=0}^{N-1}$ with $x = 5$ for several values of $k$ are shown in Tables I and II, respectively. Next we generate all of periodic sequences and investigate their periods. Determining periodic sequences is straightforward. We start from an initial value $x_0 \in \{0, 1, \ldots, 2^k-1\}$ and form the sequence as $x_0, T_n(x_0), T_2^n(x_0), \ldots, T_{N-1}^n(x_0)$ until $T_N^n(x_0) \equiv x_0 \mod 2^k$. We then start over with an element not included in the sequences found so far. We continue forming sequences until we exhaust all the elements in the set $\{0, 1, \ldots, 2^k-1\}$. In this process, we count the number of occurrences of $N$. The period distributions for several values of $n$ are summarized in Tables III, IV and V, where $k=15, 16$ and $17$, respectively. For example, it is shown from Table III that the number of sequences with the period $N = 4096$ is two for $n = 3, 5, 11$ and $13$ when $k = 15$.

From these results, we can find two interesting properties of the sequences $\{T_i^n(x) \mod 2^k\}_{i=0}^{N-1}$: (1) there is an integer $s \geq 0$ such that $N = 2^s$, and (2) the period of $\{T_i^n(x) \mod 2^k\}$ is twice as long as that of $\{T_i^n(x) \mod 2^{k-1}\}$. In [6], the answer of the above mentioned (1) is stated by applying the structure of the group of reduced residue classes of the ring $R$. The periodic property of Chebyshev polynomial sequences modulo $2^k$ is partially solved in [9]. In the next section, we also derive the answers of (1) and (2) by classifying permutation polynomials over $R$.

3. Analysis of the period of sequences generated by integer polynomials modulo $2^k$

In this section, we give a characterization of permutation polynomials over $R$ which generate sequences with the period $N = 2^s$. An integer polynomial is a polynomial of the form

$$F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

(8)

\[\text{This experimental result had been also reported in [5].}\]
Table I. Examples of the periodic sequences of \( \{ T_i (x) \}_{i=0}^{N-1} \) mod \( 2^k \), where \( n = 3 \) and \( x = 2 \).

| \( k \) | \( \{ T_i (2) \}_{i=0}^{N-1} \) | \( N \) |
|---|---|---|
| 3 | 2 \( \rightarrow 10 \) | 1 |
| 4 | 2 \( \rightarrow 26 \rightarrow 18 \rightarrow 10 \) | 2 |
| 5 | 2 \( \rightarrow 26 \rightarrow 18 \rightarrow 42 \rightarrow 34 \rightarrow 58 \rightarrow 50 \rightarrow 10 \) | 4 |
| 6 | 2 \( \rightarrow 26 \rightarrow 18 \rightarrow 42 \rightarrow 34 \rightarrow 58 \rightarrow 50 \rightarrow 10 \) | 8 |

Table II. Examples of the periodic sequences of \( \{ T_i (x) \}_{i=0}^{N-1} \) mod \( 2^k \), where \( n = 5 \) and \( x = 5 \).

| \( k \) | \( \{ T_i (5) \}_{i=0}^{N-1} \) | \( N \) |
|---|---|---|
| 3, 4, 5 | 5 \( \rightarrow 37 \) | 1 |
| 6 | 5 \( \rightarrow 37 \rightarrow 69 \rightarrow 101 \) | 2 |
| 7 | 5 \( \rightarrow 37 \rightarrow 69 \rightarrow 229 \rightarrow 133 \rightarrow 37 \rightarrow 197 \rightarrow 101 \) | 4 |
| 8 | 5 \( \rightarrow 165 \rightarrow 69 \rightarrow 229 \rightarrow 133 \rightarrow 37 \rightarrow 197 \rightarrow 101 \) | 8 |

Table III. Examples of the period distribution for several values of \( n \), where \( k = 15 \).

| \( N \) | \( n = 3 \) | \( n = 5 \) | \( n = 7 \) | \( n = 9 \) | \( n = 11 \) | \( n = 13 \) |
|---|---|---|---|---|---|---|
| 1 | 20 | 20 | 40 | 40 | 20 | 20 |
| 2 | 10 | 10 | 20 | 20 | 10 | 10 |
| 4 | 10 | 10 | 20 | 20 | 10 | 10 |
| 8 | 10 | 10 | 20 | 20 | 10 | 10 |
| 16 | 10 | 10 | 20 | 20 | 10 | 10 |
| 32 | 10 | 10 | 20 | 20 | 10 | 10 |
| 64 | 10 | 10 | 20 | 20 | 10 | 10 |
| 128 | 10 | 10 | 20 | 20 | 10 | 10 |
| 256 | 10 | 10 | 20 | 20 | 10 | 10 |
| 512 | 10 | 10 | 20 | 20 | 10 | 10 |
| 1024 | 10 | 10 | 4 | 4 | 10 | 10 |
| 2048 | 2 | 2 | 4 | 4 | 2 | 2 |
| 4096 | 2 | 2 | 0 | 0 | 2 | 2 |

having coefficients \( a_i \) that are all integers. The set of integer polynomials is denoted \( \mathbb{Z}[x] \). Rivest proved the following [12].

**Lemma 2 (Rivest [12])** An integer polynomial \( F(x) \) is a permutation polynomial modulo \( 2^k \), \( k \geq 2 \), if and only if \( a_1 \) is odd, \( (a_2 + a_4 + \cdots) \) is even, and \( (a_3 + a_5 + \cdots) \) is even.

We define the subset of \( \mathbb{Z}[x] \) such that
\[
\mathcal{C} = \{ F \in \mathbb{Z}[x] : \forall i \geq 2, a_i \equiv 0 \mod 4 \land a_1 \equiv 1 \mod 4 \land a_0 = 0 \}. \tag{9}
\]

**Lemma 3** An integer polynomial \( F \in \mathcal{C} \) has the semi-group property: For \( F, G \in \mathcal{C} \)
\[
F \circ G \in \mathcal{C}. \tag{10}
\]

**Proof:** Let \( F(x) = \sum_{i=1}^{n} a_i x^i \) and \( G(x) = \sum_{i=1}^{m} b_i x^i \), where \( a_i, b_i \in \mathbb{Z} \). We obtain
\[
F(G(x)) = \sum_{i=2}^{n} a_i G(x)^i + a_1 \sum_{i=2}^{m} b_i x^i + a_1 b_1 x. \tag{11}
\]

Since for \( i \geq 2, a_i, b_i \equiv 0 \mod 4 \), \( (F(G))_i \equiv 0 \mod 4 \) for \( i \geq 2 \), where \( (F(G))_i \) denotes the coefficient of \( x^i \) in \( F \circ G \). Since \( a_1 b_1 \equiv 1 \mod 4 \), \( (F(G))_1 \equiv 1 \mod 4 \). This completes the proof. \( \square \)
Table IV. Examples of the period distribution for several values of \( n \), where \( k = 16 \).

| \( N \) | \( n = 3 \) | \( n = 5 \) | \( n = 7 \) | \( n = 9 \) | \( n = 11 \) | \( n = 13 \) |
|-------|--------|--------|--------|--------|--------|--------|
| 1     | 20     | 20     | 40     | 40     | 20     | 20     |
| 2     | 10     | 10     | 20     | 20     | 10     | 10     |
| 4     | 10     | 10     | 20     | 20     | 10     | 10     |
| 8     | 10     | 10     | 20     | 20     | 10     | 10     |
| 16    | 10     | 10     | 20     | 20     | 10     | 10     |
| 32    | 10     | 10     | 20     | 20     | 10     | 10     |
| 64    | 10     | 10     | 20     | 20     | 10     | 10     |
| 128   | 10     | 10     | 20     | 20     | 10     | 10     |
| 256   | 10     | 10     | 20     | 20     | 10     | 10     |
| 512   | 10     | 10     | 20     | 20     | 10     | 10     |
| 1024  | 10     | 10     | 20     | 20     | 10     | 10     |
| 2048  | 10     | 10     | 4      | 4      | 10     | 10     |
| 4096  | 2      | 2      | 4      | 4      | 2      | 2      |
| 8192  | 2      | 2      | 0      | 0      | 2      | 2      |

Table V. Examples of the period distribution for several values of \( n \), where \( k = 17 \).

| \( N \) | \( n = 3 \) | \( n = 5 \) | \( n = 7 \) | \( n = 9 \) | \( n = 11 \) | \( n = 13 \) |
|-------|--------|--------|--------|--------|--------|--------|
| 1     | 20     | 20     | 40     | 40     | 20     | 20     |
| 2     | 10     | 10     | 20     | 20     | 10     | 10     |
| 4     | 10     | 10     | 20     | 20     | 10     | 10     |
| 8     | 10     | 10     | 20     | 20     | 10     | 10     |
| 16    | 10     | 10     | 20     | 20     | 10     | 10     |
| 32    | 10     | 10     | 20     | 20     | 10     | 10     |
| 64    | 10     | 10     | 20     | 20     | 10     | 10     |
| 128   | 10     | 10     | 20     | 20     | 10     | 10     |
| 256   | 10     | 10     | 20     | 20     | 10     | 10     |
| 512   | 10     | 10     | 20     | 20     | 10     | 10     |
| 1024  | 10     | 10     | 20     | 20     | 10     | 10     |
| 2048  | 10     | 10     | 4      | 4      | 10     | 10     |
| 4096  | 10     | 10     | 4      | 4      | 2      | 2      |
| 8192  | 2      | 2      | 0      | 0      | 2      | 2      |
| 16384 | 2      | 2      | 0      | 0      | 2      | 2      |

When \( k = 1 \) and 2, \( F \in C \) is an identity mapping modulo \( 2^k \), that is, \( F(x) \equiv x \mod 2^k \). First, we can prove that if there is an integer \( w \geq 2 \) such that

\[
F(X) \equiv X \mod 2^w,
F(X) \not\equiv X \mod 2^{w+1},
\]

then \( F(X) \equiv X + 2^w \mod 2^{w+1} \). According to Eq.(12), there exists an odd number \( 2v + 1 \) \((v \geq 0)\) such that \( F(X) = (2v + 1) \cdot 2^w + X \), which means \( F(X) \equiv X + 2^w \mod 2^{w+1} \).

Let \( F^i \) be the \( i \)th iterate of \( F \), where \( F^0(x) = x \) and \( F^i(x) = F(F^{i-1}(x)) \) for \( i \geq 1 \). We have the following lemma.

**Lemma 4** Assume that \( X \) and \( w \) satisfy the relation of Eq.(12), then,

\[
F^2(X) \equiv X \mod 2^{w+1},
\]

\[
F^2(X) \equiv X + 2^{w+1} \mod 2^{w+2}.
\]

**Proof:** Substituting \( F(X) = (2v + 1) \cdot 2^w + X \) into Eq.(8), we have...
Lemma 4, we have
\begin{equation}
F^2(X) = (2v + 1) \cdot 2^w + X,
\end{equation}
Substituting $F(X) = \sum_{i=1}^{n} a_i X^i = (2v + 1) \cdot 2^w + X$ and $a_1 = 4u + 1 \ (u \geq 0)$ into Eq.(15), we get $F^2(X) \equiv X \mod 2^w+1$ and $F^2(X) \equiv X + 2^w+1 \mod 2^{w+2}$.

**Theorem 1** Assume that $X$ and $w$ satisfy the relation of Eq.(12). For $m \geq 0$,
\begin{align}
F^{2m}(X) &\equiv X \mod 2^{w+m}, \\
F^{2m}(X) &\equiv X + 2^{w+m} \mod 2^{w+m+1}.
\end{align}
Proof: We prove the above theorem by mathematical induction. By the assumption of Eq.(12) and Lemma 4, Eq.(16) is satisfied for $m = 0$ and $m = 1$. Suppose that Eq.(16) is satisfied for $m = i$, that is,
\begin{align}
F^{2^i}(X) &\equiv X \mod 2^{w+i}, \\
F^{2^i}(X) &\equiv X + 2^{w+i} \mod 2^{w+i+1}.
\end{align}
From the semi-group property of polynomials in $C$, $G = F^{2^i}$ is also an element of $C$. Therefore, using Lemma 4, we have
\begin{align}
G^2(X) &\equiv X \mod 2^{w+i+1}, \\
G^2(X) &\equiv X + 2^{w+i+1} \mod 2^{w+i+2},
\end{align}
which means Eq.(16) is also satisfied for $m = i+1$ since $G^2 = F^{2^{i+1}}$. From the discussions above, Eq.(16) is satisfied for arbitrary $m \geq 0$ under the assumption of Eq.(12), which completes the proof.

**Theorem 2** Assume that $X$ and $w$ satisfy the relation of Eq.(12). For $m \geq 1$,
\begin{equation}
\{F^j(X) \mod 2^{w+m} : j = 0, 1, \ldots, 2^m - 1\} = \{X + 2^w \cdot j \mod 2^{w+m} : j = 0, 1, \ldots, 2^m - 1\}.
\end{equation}
Proof: We show the above theorem by using induction. The case of $m = 1$ is trivial. Assume Eq.(19) is satisfied for $m = i$. Then, there is an integer $\ell_j$ for $0 \leq \ell_j \leq 2^i - 1$ such that
\begin{equation}
F^j(X) \equiv X + 2^w \cdot \ell_j \mod 2^{w+i}.
\end{equation}
It follows $F^j(X) = p \cdot 2^{w+i} + 2^w \cdot \ell_j + X$ for an integer $p$. Then, we get
\begin{equation}
F^j(X) \equiv X + 2^w \cdot \ell_j + 2^{w+i} c_j \mod 2^{w+i+1},
\end{equation}
where $c_j = 0$ for even $p$ and $c_j = 1$, otherwise. In view of Theorem 1, we have
\begin{equation}
F^{j+2^i}(X) \equiv X + 2^w \cdot \ell_j + 2^{w+i}(1 - c_j) \mod 2^{w+i+1}.
\end{equation}
Let $A = \{X + 2^w j \mod 2^{w+i+1} : 0 \leq j < 2^i\}$ and $B = \{X + 2^w j \mod 2^{w+i+1} : 2^i \leq j < 2^{i+1}\}$. We have
These 16 values are elements of the set $X$ mod $2^{w+1}$ as the integer coefficients of $F(X)$ satisfy Eq.(26) if and only if $i = j$. Therefore, the least value of $N$ satisfying $F^N(X) \equiv X$ mod $2^{w+m}$ is $2^m$, which completes the proof.

Determining periods of sequences is a fundamental problem for engineering applications such as pseudo random number and cryptography. Using Theorem 3, we do not need to form a sequence as $X, F(X), F^2(X), \ldots, F^{N-1}(X)$ until $F^N(X) \equiv X$ mod $2^k$, which requires at most $2^k$ operations. We just try to find the value of $w$ satisfying Eq.(12) from $w = 2$ to $k$. After finding $w$, the period of sequence $\{F^i(X) \mod 2^k\}_{i \geq 0}$ is derived as $2^{k-w}$ for any $k$. Theorems 2 and 3 also tell us that the least significant $w$ bits of $F^i(X)$ mod $2^{w+m}$ are unchanged for each $i = 0, 1, \ldots, 2^m-1$, which means $b_{i+1} = b_i$ for $\ell = 0, 1, \ldots, w-1$, where $b_i \in \{0, 1\}$ is determined such that $F^i(X) \mod 2^k = (b_{i-1} b_{i-2} \cdots b_0)$. If we use the sequence $X, F(X), F^2(X), \ldots$ as a pseudo random number, it should be noticed that the least significant $w$ bits of the sequence do not have any randomness. Moreover, all possible $2^{k-w}$ bit combinations appear in the most significant $k-w$ bits of $F^i(X)$ mod $2^{w+m}$. These properties are also important to analyze the security of cryptosystems based on Chebyshev polynomials as discussed in the following subsection.

Example 1 Assume $F(x) = 4x^2 + x$. For any $x$, $F(x) \equiv x \mod 2^k$ when $k = 1$ or $k = 2$. Since $F(1) \equiv 5 \mod 2^3$, the value of $w$ satisfying Eq.(12) is two when $X = 1$. Therefore, the sequence $X = 1, F(1), F^2(1), \ldots$ has the period $N = 2^{k-2}$. Specifically, when $k = 6$, the generated sequence having the period $N = 16$ is

$$1 \rightarrow 5 \rightarrow 41 \rightarrow 45 \rightarrow 17 \rightarrow 21 \rightarrow 57 \rightarrow 61 \rightarrow 33 \rightarrow 37 \rightarrow 9 \rightarrow 13 \rightarrow 49 \rightarrow 53 \rightarrow 25 \rightarrow 29 \rightarrow 1.$$ 

These 16 values are elements of the set $\{1 + 4 \cdot i \mid i = 0, 1, \ldots, 15\}$. One can see that the least significant $w = 2$ bits of the sequence are always $(01)_2$ and all possible 4 bit patterns appear in the most significant 4 bits in the sequence.

3.1 Some properties of Chebyshev polynomial sequences modulo $2^k$

The integer coefficients of $T_n(x)$ are given explicitly by the following formula $[11]$:

$$T_n(x) = \sum_{j=0}^{\lfloor n/2 \rfloor} (-1)^j \frac{n}{n-j} n-j C_j 2^{n-2j-1} x^{n-2j}. \quad (25)$$

One can see from Eqs.(9) and (25) that $C$ contains $T_n(x)$ of odd degree $n$.

Lemma 5 For an odd $n$, the map of Eq.(5) is an identity mapping when $k = 3$, that is,

$$T_n(x) \equiv x \mod 2^3. \quad (26)$$

Proof: We prove this by mathematical induction. We set $n = 2i + 1$ ($i \geq 0$). For $i = 0$, this is trivial since $T_1(x) = x$. It is also easy to confirm that $T_3(x) = 4x^3 - 3x \equiv x \mod 2^3$ for $i = 1$. Suppose Eq.(26) is satisfied for $i = j$. Using Eqs.(2) and (25), we have

$$T_{2j+3}(x) \equiv (-1)^j 2x + (-1)^{j-1} 4j^2 x^3 - x \mod 2^3. \quad (27)$$

We get $T_{2j+3}(x) \equiv x \mod 2^3$ for even $j$ and $T_{2j+3}(x) \equiv 4x^3 - 3x \mod 2^3$ for odd $j$. This means Eq.(26) is also satisfied for $i = j + 1$. Thus, the proof is completed. \qed

449
Lemma 6  For an odd \( n \) and \( w = 4 \), when \( x \) is odd, then
\[
T_n(x) \equiv x \mod 2^4.
\]

The proof is similar to that in Lemma 6, and is omitted.

In conjunction with Lemmas 5, 6 and Theorem 3, it can be said that the period of Chebyshev polynomial sequences modulo \( 2^k \) is at most \( 2^{k-3} \) for an even \( x \) and \( 2^{k-4} \) for an odd \( x \). When \( n \equiv 3 \) or \( 5 \mod 8 \), there are four even \( X \)'s such that \( T_n(X) \neq X \mod 2^4 \) and \( T_n(T_n(X)) \equiv X \mod 2^4 \). This is verified as the following. Let \( X = 2p \) for \( p = 0, 1, \ldots, 7 \) and \( n = 8i + 2j + 1 \) for \( i = 0, 1, \ldots, j = 0, 1, 2, 3 \). Using Eq.(25), we have
\[
T_n(2p) \equiv (-1)^{4i+j}(8i + 2j + 1) \cdot 2p \mod 2^4.
\]

By substituting \( j = 0 \) or \( j = 3 \), we get \( T_n(2p) \equiv 2p \mod 2^4 \). When \( j = 1 \) or \( j = 2 \), we get \( T_n(2p) \equiv 10p \mod 2^4 \). Therefore, \( T_n(2p) \equiv 2p \mod 2^4 \) for even \( p \). For odd \( p \), \( T_n(2p) \equiv 2p + 8 \mod 2^4 \) and \( T_n(2p + 8) \equiv 2p \mod 2^4 \). From the discussions above, when \( n \equiv 3 \) or \( 5 \mod 8 \), the sequence \( \{ T_n(X) \}_{i=0}^{N-1} \) has the maximum period \( N = 2^{k-3} \), where \( X = 2, 6, 8 \) or 10. This is also confirmed by Tables III, IV and V.

Now, we present the key exchange protocol proposed in [4]. Suppose Alice and Bob want to share a secret key from \( 0 \sim 2^k - 1 \). First, Alice and Bob select a random number \( X \). Next, Alice generates an odd integer \( s \) and computes \( T_s(X) \), then sends \( T_s(X) \) to Bob. Bob also generates an odd integer \( r \) and computes \( T_r(X) \), then sends \( T_r(X) \) to Alice. Third, Alice and Bob can get their secret key \( K \) by computing \( K \equiv T_s(T_r(X)) \equiv T_s(T_r(X)) \equiv T_s(T_r(X)) \mod 2^k \) because of the commutative property of Chebyshev polynomials modulo \( 2^k \). It has been already shown that the cryptosystems based on Chebyshev polynomials modulo \( 2^k \) is decided in at most polynomial time in the case that the parameter \( X \) is even number [7]. Using an odd number \( X \) such that \( X^2 - 1 = 4^v \times p \) for an integer \( p \) and a large integer \( v(\leq \frac{k}{2}) \) is a necessary condition in the cryptosystem. We also give another necessary condition on \( X \) by suggesting a simple attack on the key exchange protocol based on Chebyshev polynomials. The following corollary is important for this attack.

Corollary 1  Assume \( X \) and \( w \) satisfies the relation of Eq.(12). Let \( n \) be an odd number and \( \{X_i\}_{i=0}^{N-1} \) be a Chebyshev polynomial sequence with the period \( N = 2^k-w \), where \( X_i = T_n(X) \mod 2^k \). Let \( B_i = (b_{i-2} \ldots b_2 b_0 b_1) \) for \( b_i \in \{0, 1\} \) be a binary expansion of \( X_i \). For \( j = 1, \ldots, k-w \),
\[
b_{w+j-1} = \begin{cases} 
  b_{w-j-1} & i \equiv \ell \mod 2^j, \\
  b_{w-j-1} & i \not\equiv \ell \mod 2^j \text{ and } i \equiv \ell \mod 2^{j-1}
\end{cases}
\]

(28)

We use \( \tau \) to denote the binary complement of \( a \), i.e., \( \overline{0} = 1 \) and \( \overline{1} = 0 \).

Proof: Taking every \( 2^{j-1} \) and \( 2^{j-1} \)th element of \( \{X_i\}_{i=0}^{N-1} \), we obtain the sequences \( \{X_{m,2^j}\}_{m=0}^{N/2^{j-1}} \) and \( \{X_{r,2^{j-1}}\}_{r=0}^{N/2^{j-1}-1} \). Since \( T_n^{2^j} = T_n^{2^{j-1}} \) and \( T_n^{2^{j-1}} = T_n^{2^{j-2}} \), \( X \) has the period of \( N/2^j = 2^{k-w-j} \) in \( T_n^{2^j} \mod 2^k \) and the period of \( N/2^{j-1} = 2^{k-w-j+1} \) in \( T_n^{2^{j-1}} \mod 2^k \). In view of Theorem 2, the least significant \( w+j \) bits of \( X_{m,2^j} \) and \( w+j-1 \) bits of \( X_{r,2^{j-1}} \) in the sequence are unchanged for each \( m \) and \( r \). Note that the sequence \( \{X_{r,2^{j-1}}\} \) for even \( \ell \) is equivalent with \( \{X_{m,2^j}\} \). The \( w+j \)th bit of \( X_{r,2^{j-1}} \) for odd \( \ell \) should be different with the \( w+j \)th bit of \( X_{r,2^{j-1}} \) for even \( \ell \), which gives Eq.(28).

Remark 1  In view of Theorem 2, there is an integer \( i_j \) for \( i_j = 0, 1, \ldots, 2^{k-w} - 1 \) such that \( T_{i_j}^{2^j}(X) = X + 2^{w}i_j \mod 2^k \). Corollary 1 also tells us that whether the number \( i_j \) is even or not depends on \( j \) being even or not, which is to say that even and odd numbers \( i_j \) occur alternately in the sequence \( X, X + 2^w i_1, X + 2^w i_2, \ldots \). For instance, as shown in Table I, when \( k = 5 \), \( n = 3 \), \( X = 2 \) and \( w = 3 \), the Chebyshev polynomial sequence is written as \( 2 = 2 + 8 \times 0 \rightarrow 26 = 2 + 8 \times 3 \rightarrow 18 = 2 + 8 \times 2 \rightarrow 10 = 2 + 8 \times 1 \).

450
Suppose \( T_s(X) \equiv X \mod 2^w, T_s(X) \neq X \mod 2^{w+1} \) and \( T_r(X) \equiv X \mod 2^\hat{w}, T_r(X) \neq X \mod 2^{\hat{w}+1} \). Assume \( \hat{w} \geq w \). Let \( X = (b_{k-1}b_{k-2} \cdots b_0) \), \( T_s(X) = (b_{k-1}b_{k-2} \cdots b_0) \) and \( T_r(X) = (b_{k-1}b_{k-2} \cdots b_0) \), where \( b_i, b'_i, \in \{0, 1\} \). Since \( T_r(X) \) is an element in the set \( \{X + 2^\hat{w} \cdot i \mod 2^{\hat{w}} \mid 0 \leq i < 2^{\hat{w}} - 1\} \), the key \( K = T_s(T_r(X)) \) also exists in the set \( \{X + 2^w \cdot i \mod 2^w \mid 0 \leq i < 2^w - 1\} \). If Eve who is an eavesdropper derives the values of \( w \) and \( w' \), the exact key space is reduced from \( 2^k \) to \( 2^k - w' \). It is easy for Eve to determine the values of \( w \) and \( w' \) because \( b_w \neq b'_w \) and \( b_w \neq b'_w \) from Corollary 1. Moreover, when \( w = \hat{w} \), the key is given by \( K = T_s(T_r(X)) = X + 2^w \cdot i \mod 2^k \) for an even integer \( i \) as explained in Remark 1. It is confirmed by our numerical experiments that if \( s, r \equiv 3 \) or \( 5 \mod 8 \), \( w = \hat{w} \) for any \( X \). In this case, the key exists in the set \( \{X + 2^{w+1} \cdot i \mod 2^k \mid 0 \leq i < 2^{k-1} - 1\} \).

**Example 2** Here is an example with artificially small parameters. Let \( k = 16 \). Alice and Bob choose \( X = 6145 \) with \( X^2 - 1 = 4^6 \times 9219 \), where the condition given in [7] is fulfilled because the value of \( v = 6 \) is close to \( \frac{k}{2} \). Alice selects \( s = 3 \) with \( T_s(X) = 55297 \). Bob selects \( r = 21 \) with \( T_r(X) = 22529 \). Eve gets \( X = 6145 = 0x1801, T_s(X) = 55297 = 0xd801 \) and \( T_r(X) = 22529 = 0x5801 \), who easily derives the values of \( w = 14 \) and \( \hat{w} = 14 \) since \( b_{14} \neq b'_{14} \) and \( b_{14} \neq b'_{14} \). Thus, Eve knows that the key exists in the set \( \{X + 2^{15} \cdot i \mod 2^{16} \mid i = 0, 1, \ldots, 2^{16} - 1\} \). Indeed, the key \( K = T_s(T_r(X)) = 6145 \).

From the discussions above, it can be seen that the factual key space of the key exchange protocol depends on the parameter \( w \). Therefore, the period of Chebyshev polynomial sequence modulo \( 2^k \) should be considered when selecting \( X \). To make brute force attack infeasible, \( X \) should be carefully chosen such that \( w \) is small enough.

**4. Conclusion**

In this paper, we characterize permutation polynomials which generate periodic sequences with the period of a power of two. Chebyshev polynomials of odd degree are examples of such polynomials. Based on such findings, we devise a simple attack on the key exchange protocol based on Chebyshev polynomials. It is revealed by our security analysis that parameters generating short period Chebyshev polynomial sequences must be avoided in the key exchange protocol.

Another important problem is to characterize the period distribution of Chebyshev polynomial sequences. This topic is challenging and needed further research.

**Acknowledgments**

The authors would like to thank anonymous reviewers for their helpful comments that improve the quality of this paper.

This work was supported in part by the Grant-in-Aid (KAKENHI) for Young Scientific Research (B) under Grant Number 25820167 from the Japan Society for the Promotion of Science (JSPS).

**References**

[1] T. Kohda and A. Tsuneda, “Explicit evaluations of correlation functions of Chebyshev and bit sequences based on Perron-Frobenius operator,” IEICE Trans. Fundamentals, vol. E77-A, no. 11, pp. 1794–1800, 1994.

[2] L. Kocarev and Z. Tasev, “Public-key encryption based on Chebyshev maps,” Proc. of 2003 IEEE int’l Symp. Circuits and Systems, vol. 3, pp. 28–31, 2003.

[3] L. Kocarev, J. Makraduli, and P. Amato, “Public-key encryption based on Chebyshev polynomials,” Circuits Systems and Signal Processing, vol. 24, no. 5, pp. 497–517, 2005.

[4] K. Umeno, “Key exchange by Chebyshev polynomials modulo 2^w,” Proc. of INA-CISC, pp. 95–97, 2005.

[5] K. Umeno, “Information systems as complex systems,” Kyoritsu syuppan, pp. 181–250, 2007. (in Japanese)

[6] M. Ishii, “Periodicity of Chebyshev polynomials over the residue ring of Z/2^rZ and an electronic signature,” Trans. of The Japan Society for Industrial and Applied Mathematics, vol. 18, no. 2, pp. 257–265, 2008. (in Japanese)
[7] M. Ishii and A. Yoshimoto, “Applications for cryptography of the structure of the group of reduced residue classes of residue ring of $\mathbb{Z}/2^w\mathbb{Z}$,” Trans. of The Japan Society for Industrial and Applied Mathematics, vol. 19, no. 1, pp. 57–71, 2009. (in Japanese)

[8] X. Liao, F. Chen, and K. Wong, “On the security of public-key algorithms based on Chebyshev polynomials over the finite field $\mathbb{Z}_N$,” IEEE Trans. Computers, vol. 59, no. 10, pp. 1392–1401, 2010.

[9] A. Iwasaki and K. Umeno, “Periodical property of Chebyshev polynomials on the residue class rings modulo $2^w$,” IEICE Technical Report, CAS2014-67k, NLP2014-61, pp. 81–86, October 2014. (in Japanese)

[10] Y. Dainobu and D. Yoshioka, “Period of sequences generated by Chebyshev polynomials over the residue ring $\mathbb{Z}/2^w\mathbb{Z}$,” Proc. of the 31st Symposium on Cryptography and Information Security (SCIS), January 2014. (in Japanese)

[11] J.C. Mason and D.C. Handscomb, Chebyshev polynomials, Chapman& hall, CRC, 2002.

[12] R.L. Rivest, “Permutation polynomials modulo $2^w$,” Finite fields and their applications, vol. 7, pp. 287–292, 2001.