Parameter Selection in Public Key Cryptosystem based on Chebyshev Polynomials over Finite Field

Zhihui Li[1,2], Yidong Cui[1], Yuehui Jin[1], Huimin Xu[2]
[1]Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education,
Beijing University of Posts and Telecommunications, Beijing, China
[2]School of Information and communication Engineering,
Beijing University of Posts and Telecommunications, Beijing, China
Email:{lizhihui8601@gmail.com}

***Abstract*— A recently proposed public key cryptosystem based on Chebyshev polynomials suggests a new approach to data encryption. But the security of the cryptosystem has not been investigated in depth, for lack of an appropriate analysis method. In this paper, a new representation of Chebyshev polynomial is introduced to study security issues of the cryptosystem. The properties of Chebyshev polynomial sequence are presented, and their impact on the cryptosystem are discussed. Finally some principles for parameter selection for the cryptosystem are proposed. The methodology used in this paper is supposed to offer a useful means for future researches on this topic.**

***Index Terms*— Chebyshev polynomial sequence, period, symmetry, cryptanalysis, security**

I. Introduction

Since Diffie and Hellman [1] presented the conception of public key encryption in 1976, various public key cryptosystems have been proposed. Those systems depend on certain difficult problems to protect data from being recovered by eavesdroppers. For example, the security of RSA cryptosystem [2] and that of Rabin cryptosystem [3] depend on the intractability of large integer factorization, and the security of Elgamal encryption algorithm [4] depends on the intractability of discrete logarithm problem. All the three cryptosystems employ the semigroup property [5]:

$$(X^p)^q = X^{pq} \pmod{n}$$

A necessary condition for these cryptosystems is that the exponentiation operation X^p must be a one-way function.

Taking advantage of the semigroup property of Chebyshev polynomials in real field, a public key cryptosystem was proposed [6], in the assumption that the computation of Chebyshev polynomial in real field is a one-way function. But it was soon found the private key can be quickly recovered from the public key, using trigonometric function substitution [5], [7]. In other words, the one-way condition is not satisfied in such cryptosystem. To resist this attack, some references recommended to encrypt the public key in transformation process [8], [9], but the security of such a cryptosystem depends on another totally different encryption algorithm, and the problem of Chebyshev polynomials itself had not been solved.

In another more feasible approach, the definition of Chebyshev polynomials was expanded from real field to finite field, while the similar encryption operation is performed [10]–[12]. To analyze the security of this cryptosystem, the sequence composed by Chebyshev polynomials over finite field(called **Chebyshev polynomial sequence** in the following discussions) needs to be investigated. Using matrix representation of Chebyshev polynomial, the period of Chebyshev polynomial sequence is proved to be factor of $p+1$ or $p-1$ [10]. Furthermore, reference [13] gave out the distribution density of these periods, after studying the generating polynomial of Chebyshev polynomial sequence. But as these two methods can not determine the minimal period of a certain sequence, after initial value x and prime p are given, they are unable to find a sequence with large period. Another analysis strategy is to convert the present problem to another equivalent one, while the latter has been intensively studied for a long time. For example, Lima et al. [14] presented a generalized cosine substitution for Chebyshev polynomials over finite field, and proved that recovering the corresponding plaintext from a given ciphertext involves discrete logarithm problem. In [10] the transformation is made by hyperbolic function substitution, and the same conclusion was drawn. While some kinds of discrete logarithm problems can be solved efficiently, it is necessary to construct a cryptosystem whose corresponding discrete logarithm problem is intractable. The substitution methods become inconvenient in that question. Besides, as these methods study the security of the cryptosystem based on either its corresponding Chebyshev polynomial sequence, or its corresponding discrete logarithm problem, none of them can explain the relationship between these two forms.

In this paper, a new representation of Chebyshev polynomials is introduced to study security problem in the cryptosystem. Using that representation some new

[1]Manuscript received June 10, 2011; accepted June 30, 2011.

doi:10.4304/jcm.6.5.400-408

properties of Chebyshev polynomial sequence are found, which can be used to reduce the time cost on exhaustive attack. By that representation the cryptanalysis of the encryption algorithm can also be converted to Generalized discrete logarithm problem(GDLP) on a cyclic group. The relationship between Chebyshev polynomial sequence and the group is also presented, then some efficient algorithms against the GDLP can be applied. To resist these attacks some principles for parameter selection are proposed. The methodology adopted in this paper is supposed to be useful in the future researches.

II. Cryptosystem based on Chebyshev polynomials over finite field

Let $n \in Z^+$ and $x \in {F_p}^*$, the Chebyshev polynomials over finite field are recursively defined as [12]:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \pmod p \quad (1)$$

with $n \geq 2$, and $T_0(x) = 1$, $T_1(x) = x$.

The Chebyshev polynomials over finite field have semigroup property, i.e. for arbitrary $r, s \in Z^+$ and $x \in {F_p}^*$, equation

$$T_s(T_r(x)) = T_{sr}(x) = T_{rs}(x) = T_r(T_s(x)) \pmod p \quad (2)$$

holds.

Taking advantage of the semigroup property, an Elgamal-like public key cryptosystem is constructed, whose processes can be described as follows:

(1) Key pair generation:
Randomly select integers $s \in Z^+$, and $x \in {F_p}^*$, where $s \neq 1, x \neq 1$, and compute

$$p_k = T_s(x) \pmod p$$

Then s is private key and (x, p_k) is public key.

(2) Message encryption
Assume Alice wants to send a message m to Bob. The encryption process is:
   (a) Alice randomly selects an integer $r \in Z_n$ and $r \neq 1$.
   (b) Alice uses Bob's public key to compute as follows:

$$k_1 = T_r(x) \pmod p$$
$$k_2 = T_r(p_k) \pmod p$$
$$c = m \cdot k_2 \pmod p$$

   (c) Alice sends $(c, k_1)$to Bob as the cipher.

(3) Message decryption
After receiving the cipher, Bob can decrypt it as follows:
   (a) Compute ${k_2}' = T_s(k_1) \pmod p$
   (b) Compute $m' = \frac{c}{{k_2}'} \pmod p$

since $m' = m$, Bob gets the right message.

The cryptosystem runs on a prime finite field, as p is requested to be a prime number. The RSA-like cryptosystem proposed in [10] and [11] does not work on the same kind of field, so its characteristics are different from the former. In present paper it is not discussed.

III. Properties of Chebyshev polynomial sequence

In the three processes of this cryptosystem, the most operations are done on Chebyshev polynomial sequence. Hence its properties have significant influence on the security of the cryptosystem, and need to be investigated in details. For this purpose, a new representation of Chebyshev polynomial is introduced by the following proposition.

Proposition 1: The Chebyshev polynomial can be represented with the following expression:

$$T_n(x) = \frac{(x + \sqrt{x^2-1})^n + (x - \sqrt{x^2-1})^n}{2} \pmod p \quad (3)$$

Proof: The Chebyshev polynomial can be rewritten as

$$T_n(x) = (\lambda_1 + \lambda_2)T_{n-1}(x) - \lambda_1\lambda_2 T_{n-2}(x) \pmod p$$

where $\lambda_1 + \lambda_2 = 2x \pmod p$, and $\lambda_1\lambda_2 = 1 \pmod p$, i.e.

$$\begin{cases} \lambda_1 = x + \sqrt{x^2-1} \pmod p \\ \lambda_2 = x - \sqrt{x^2-1} \pmod p \end{cases}$$

Notice $T_0(x) = \lambda_1\lambda_2 \pmod p$ and $T_1(x) = \frac{\lambda_1 + \lambda_2}{2} \pmod p$, then we can get the formula of general term of $T_n(x)$:

$$T_n(x) = \frac{\lambda_1^n + \lambda_2^n}{2} \pmod p$$

i.e.

$$T_n(x) = \frac{(x + \sqrt{x^2-1})^n + (x - \sqrt{x^2-1})^n}{2} \pmod p$$

■

Based on representation (3) the following important properties of Chebyshev polynomial sequence can be proved.

Property 1: The p-th element of Chebyshev polynomial sequence is x, i.e. $T_p(x) = x \pmod p$.

Proof: Using equation (3), the expression of $T_p(x)$ can be transformed as follows:

$$\begin{aligned}
&T_p(x)\\
=&\frac{(x+\sqrt{x^2-1})^p+(x-\sqrt{x^2-1})^p}{2}\\
=&\frac{\sum_{i=0}^{p}\binom{p}{i}x^i(\sqrt{x^2-1})^{p-i}+\sum_{i=0}^{p}\binom{p}{i}x^i(-\sqrt{x^2-1})^{p-i}}{2}\\
=&\frac{\sum_{k=0}^{(p-1)/2}\binom{p}{2k}x^{2k}(\sqrt{x^2-1})^{p-2k}}{2}\\
&+\frac{\sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}x^{2k+1}(\sqrt{x^2-1})^{p-(2k+1)}}{2}\\
&+\frac{\sum_{k=0}^{(p-1)/2}\binom{p}{2k}x^{2k}(-\sqrt{x^2-1})^{p-2k}}{2}\\
&+\frac{\sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}x^{2k+1}(-\sqrt{x^2-1})^{p-(2k+1)}}{2}\\
=&\frac{\sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}x^{2k+1}(\sqrt{x^2-1})^{p-(2k+1)}}{2}\\
&+\frac{\sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}x^{2k+1}(-\sqrt{x^2-1})^{p-(2k+1)}}{2}\\
=&\sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}x^{2k+1}(\sqrt{x^2-1})^{p-(2k+1)} \pmod p
\end{aligned}$$

When $0 \le k < \frac{p-1}{2}$, $\binom{p}{2k+1}$ is exactly divisible by p, in other words $\binom{p}{2k+1} = 0 \pmod p$. When $k = \frac{p-1}{2}$, $\binom{p}{2k+1} = 1$. Hence the expression of $T_p(x)$ can finally be simplified as

$$T_p(x) = x^p = x \pmod p$$

■

Property 2: If Chebyshev polynomial sequence has no period of $p+1$, it must have period of $p-1$.

Proof: First, Chebyshev polynomial sequence has period n if and only if $T_n(x) = 1 \pmod p$ and $T_{n+1}(x) = x \pmod p$. By the means applied in proof of Property 1, the expression of $T_{p+1}(x)$ can be simplified as:

$$T_{p+1}(x) = (x^2-1)^{\frac{p+1}{2}} + x^2 \pmod p \qquad (4)$$

or another form

$$T_{p+1}(x) = \sqrt{(x^2-1)^{p+1}} + x^2 \pmod p$$

It is easy to find both x^2-1 and $-(x^2-1)$ are square roots of $(x^2-1)^{p+1}$. As there are at most 2 different square roots for any element in a prime finite field, x^2-1 and $-(x^2-1)$ represent all possible square roots of $(x^2-1)^{p+1}$, including the case when $x = 1$. So all possible values of $T_{p+1}(x)$ can be represented as:

$$T_{p+1}(x) = \pm(x^2-1) + x^2 \pmod p$$

When $T_{p+1}(x) = 2x^2 - 1$, from Eq.1 it is known

$$T_{p-1}(x) = 1 \pmod p$$

When $T_{p-1}(x) = 1 \pmod p$ and $T_p(x) = x \pmod p$, $p-1$ is a period of Chebyshev polynomial sequence. For the same reason, when $T_{p+1}(x) = 1 \pmod p$, the value of $T_{p+2}(x)$ must be x, so $p+1$ is a period of that sequence. Therefore, either $p-1$ or $p+1$ must be a period of the sequence. ■

While $p+1$ or $p-1$ is one period of Chebyshev polynomial sequence, it is not necessarily the minimal period. In fact the minimal period may be less than $p+1$ or $p-1$. In order to distinguish them in the following discussions, we call period that equals to $p \pm 1$ as the **ordinary period**(denoted by T_{ord}), for that kind of period must exist in the sequence. Comparatively, **the minimal period**(denoted by T_{min}) can take more possible values. The relationship between these two periods is stated in Property 3.

Property 3: The minimal period of Chebyshev polynomial sequence is a factor of its ordinary period. i.e. $T_{min} | T_{ord}$.

Proof: When T_{min} is equal to 1 or T_{ord}, the proposition is true.

When $1 < T_{min} < T_{ord}$, assume T_{min} is not a factor of T_{ord}, then there must be two integers q and r, where $0 < r < T_{min}$, satisfying $T_{ord} = q \cdot T_{min} + r$. Because T_{min} is the minimal period of the sequence, it is true that $T_{n \cdot T_{min}}(x) = 1$ and $T_{n \cdot T_{min}+r}(x) \neq 1$, where n is an arbitrary nonnegative integer. Let $n = q$, we have $T_{q \cdot T_{min}+r}(x) \neq 1$, i.e. $T_{T_{ord}}(x) \neq 1$, which is contradictory to the fact that T_{ord} is a period of the sequence. Hence T_{min} must be a factor of T_{ord}. ■

Property 4: The elements of Chebyshev polynomial sequence distribute evenly symmetrically in a period. i.e. $T_{nd+i}(x) = T_{(n+1)d-i}$, where d is a period of the sequence, and i is an integer satisfying $0 \le i < d$.

Proof: According to Eq.1, when $T_{nd}(x) = 1$, the addition of $T_{nd+1}(x)$ and $T_{nd-1}(x)$ is

$$T_{nd+1}(x) + T_{nd-1}(x) = 2xT_{nd}(x) = 2x \pmod p \quad (5)$$

The multiplication of $T_{nd+1}(x)$ and $T_{nd-1}(x)$ can be calculated as follows:

$$\begin{aligned}
&T_{nd+1}(x) \cdot T_{nd-1}(x)\\
=&\frac{(x+\sqrt{x^2-1})^{nd+1}+(x-\sqrt{x^2-1})^{nd+1}}{2}\\
&\cdot\frac{(x+\sqrt{x^2-1})^{nd-1}+(x-\sqrt{x^2-1})^{nd-1}}{2}\\
=&\frac{(x+\sqrt{x^2-1})^{2nd}+(x-\sqrt{x^2-1})^2}{4}\\
&+\frac{(x+\sqrt{x^2-1})^2+(x-\sqrt{x^2-1})^{2nd}}{4}\\
=&\frac{T_{2nd}(x)+T_2(x)}{2}\\
=&\frac{T_2(T_{nd}(x))+T_2(x)}{2}\\
=&x^2 \pmod p
\end{aligned} \qquad (6)$$

From (5) and (6) the values of $T_{nd+1}(x)$ and $T_{nd-1}(x)$ can be determined:

$$T_{nd+1}(x) = T_{nd-1}(x) = x \pmod p$$

Then according to relation

$$T_{nd+2}(x) = 2xT_{nd+1}(x) - T_{nd}(x) \pmod p$$

and the reverse form

$$T_{nd-2}(x) = 2xT_{nd-1}(x) - T_{nd}(x) \pmod p$$

we have

$$T_{nd+2}(x) = T_{nd-2}(x) \pmod p$$

Thus the conclusion can be proved inductively. ■

From the proof it can be seen when $T_n(x) = 1 \pmod p$ the values of $T_{n-1}(x)$ and $T_{n+1}(x)$ must be x. So we can say that the sequence has period of n if and only if $T_n(x) = 1 \pmod p$.

Property 5: If there are two integers a, b satisfying $T_a(x) = T_b(x) \pmod p$, then $a = \pm b \pmod{T_{min}}$.

Proof: By the way used in proof of Property 4, the following simultaneous equations about $T_{a-1}(x)$ and $T_{a+1}(x)$ can be drawn:

$$\begin{cases} T_{a-1}(x) + T_{a+1}(x) = 2xT_a(x) \pmod p \\ T_{a-1}(x) \cdot T_{a+1}(x) = \dfrac{T_2(T_a(x)) + T_2(x)}{2} \pmod p \end{cases}$$

Suppose the solutions of that simultaneous equations are λ_1 and λ_2, then the values of $T_{a-1}(x)$ and $T_{a+1}(x)$ may be

$$\begin{cases} T_{a-1}(x) = \lambda_1 \pmod p \\ T_{a+1}(x) = \lambda_2 \pmod p \end{cases}$$

or

$$\begin{cases} T_{a-1}(x) = \lambda_2 \pmod p \\ T_{a+1}(x) = \lambda_1 \pmod p \end{cases}$$

For $T_b(x) = T_a(x) \pmod p$, $T_{b-1}(x)$ and $T_{b+1}(x)$ must take these two values as well. So we have

$$\begin{cases} T_{a-1}(x) = T_{b-1}(x) \pmod p \\ T_{a+1}(x) = T_{b+1}(x) \pmod p \end{cases}$$

or

$$\begin{cases} T_{a-1}(x) = T_{b+1}(x) \pmod p \\ T_{a+1}(x) = T_{b-1}(x) \pmod p \end{cases}$$

In the former case, it is easy to know $T_{a+i}(x) = T_{b+i} \pmod p$, where i is an arbitrary integer in F_p. Let $i = -b \pmod p$, then we have $T_{a-b}(x) = 1 \pmod p$, so $a-b$ is a period of the sequence, i.e. $a = b \pmod{T_{min}}$. Similarly, if the latter case is true, $a = -b \pmod{T_{min}}$. ■

Property 6: If T_{min} is even, the elements of Chebyshev polynomial sequence distribute oddly symmetrically in range of $\frac{nT_{min}}{2} \sim \frac{(n+1)T_{min}}{2}$, i.e. $T_{\frac{nT_{min}}{2}+i}(x) = -T_{\frac{(n+1)T_{min}}{2}-i}(x) \pmod p$, where i is an integer and $0 \le i < \frac{T_{min}}{2}$.

Proof: When T_{min} is even, we have

$$T_{min}(x) = 1 = 2T_{\frac{T_{min}}{2}}{}^2(x) - 1 \pmod p$$

As the minimal period of the sequence is T_{min}, the value of $T_{\frac{T_{min}}{2}}$ must be -1. Similar to the proof of Property 4, we have the following equations

$$T_{\frac{T_{min}}{2}+1}(x) + T_{\frac{T_{min}}{2}-1}(x) = -2x \pmod p \quad (7)$$

$$T_{\frac{T_{min}}{2}+1}(x) \cdot T_{\frac{T_{min}}{2}-1}(x) = x^2 \pmod p \quad (8)$$

From (7) and (8) the values of $T_{\frac{T_{min}}{2}+1}(x)$ and $T_{\frac{T_{min}}{2}-1}(x)$ can be drawn

$$T_{\frac{T_{min}}{2}+1}(x) = T_{\frac{T_{min}}{2}-1}(x) = -x \pmod p$$

Notice $T_{\frac{T_{min}}{2}-1}(x) = -T_1(x) \pmod p$ and $T_{\frac{T_{min}}{2}}(x) = -T_0(x) \pmod p$. Then according to recursive relation

$$T_2(x) = 2xT_1(x) - T_0(x) \pmod p$$

and the reverse form

$$T_{\frac{T_{min}}{2}-2}(x) = 2xT_{\frac{T_{min}}{2}-1}(x) - T_{\frac{T_{min}}{2}}(x) \pmod p$$

we have

$$T_2(x) = -T_{\frac{T_{min}}{2}-2}(x) \pmod p$$

By induction it is easy to known $T_i(x) = -T_{\frac{T_{min}}{2}-i}(x) \pmod p$. According to period property and even symmetry property of Chebyshev polynomial sequence, it can be proved $T_{\frac{nT_{min}}{2}+i}(x) = -T_{\frac{(n+1)T_{min}}{2}-i}(x) \pmod p$. ■

Property 7: If there are two integers a, b satisfying $T_a(x) = -T_b(x) \pmod p$, then T_{min} must be even, and $a = \frac{T_{min}}{2} \pm b \pmod{T_{min}}$.

Proof: First, we can prove that if there is an integer n satisfying $T_n(x) = -1 \pmod p$, then T_{min} must be even, and $n = \frac{T_{min}}{2} \pmod{T_{min}}$. Suppose T_{min} is odd. Since $T_n(x) = -1 \pmod p$, from $T_{2n}(x) = T_2(T_n(x)) = 2T_n^2(x) - 1 = 1 \pmod p$ we know $2n$ is a period of the sequence, so $T_{min} | 2n$. When T_{min} is odd, $T_{min} | n$. It means n is also a period of the sequence, which is contradictory with the known condition that $T_n(x) = -1 \pmod p$. So T_{min} must be even. Since $T_n(x) = -1 = T_{\frac{T_{min}}{2}}(x) \pmod p$, according to Property 5 $n = \pm\frac{T_{min}}{2} \pmod{T_{min}}$, so $n = \frac{T_{min}}{2} \pmod{T_{min}}$.

The remainder part of the proof is similar to that in Property 5, and is omitted. ■

Property 8: When n is even, $T_n(x) = T_n(-x) \pmod p$; otherwise when n is odd, $T_n(x) = -T_n(-x) \pmod p$.

Proof:

$$\begin{aligned} & T_n(-x) \\ =& \frac{[(-x) + \sqrt{(-x)^2 - 1}]^n + [(-x) - \sqrt{(-x)^2 - 1}]^n}{2} \\ =& \frac{[-(x - \sqrt{x^2 - 1})]^n + [-(x + \sqrt{x^2 - 1})]^n}{2} \pmod p \end{aligned}$$

When n is even

$$\begin{aligned} & T_n(-x) \\ =&\frac{(x-\sqrt{x^2-1})^n+(x+\sqrt{x^2-1})^n}{2} \\ =&T_n(x) \pmod p \end{aligned}$$

Otherwise, when n is odd

$$\begin{aligned} & T_n(-x) \\ =&\frac{-(x-\sqrt{x^2-1})^n-(x+\sqrt{x^2-1})^n}{2} \\ =&-T_n(x) \pmod p \end{aligned}$$

■

An example of Chebyshev polynomial sequences on F_{53} is shown in Fig 1. From the Figure it can be seen that the value of Chebyshev polynomial $T_{53}(x)$ equals to x, in all sequences. Corresponding to $x = 6$, 19, and 27, the period of Chebyshev polynomial sequence is 54, 13, and 6 respectively. Each of them is exactly divisible by the ordinary period of the sequence, either 52 or 54. The even symmetry distribution exists in every sequence, while the odd symmetry distribution can only be observed in sequence whose minimal period is even.

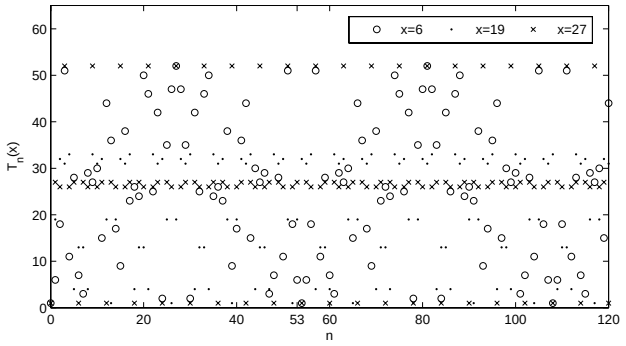

Figure 1. Chebyshev polynomial sequences

IV. Cryptanalysis of the Cryptosystem

In this section, some attack methods against this cryptosystem are analyzed. The properties of Chebyshev polynomial sequence presented in Section III can be used to reduce the time cost on these attacks. To make the cryptosystem secure some principles for parameter selection must be adopted.

A. Exhaustive search attack

To recover the private key from the public key, eavesdroppers can exhaustively search an integer s' in range of $0 \sim p$ until it satisfy $T_{s'}(x) = p_k$. Taking advantage of period property and even symmetry property of Chebyshev polynomial sequence, such a value will be found before $\frac{T_{min}}{2}$ is enumerated, so the factual search range is $0 \sim \frac{T_{min}}{2}$. Whether it is the right private key or not, it can be used to decrypt the cipher. When odd symmetry exists in that sequence, the expected time of such attack can be further reduced, by searching a key s' satisfying $T_{s'}(x) = \pm p_k$ in range of $0 \sim \frac{T_{min}}{4}$. If s' satisfies $T_{s'}(x) = p_k$ is found, it can be used to decrypt the cipher directly:

$$\begin{aligned} m' = \frac{c}{{k_2}'} &= \frac{m \cdot T_r(T_s(x))}{T_{s'}(T_r(x))} = \frac{m \cdot T_r(T_s(x))}{T_r(T_{s'}(x))} \\ &= \frac{m \cdot T_r(T_s(x))}{T_r(T_s(x))} = m \pmod p \end{aligned}$$

then m' is the right message. When s' satisfies $T_{s'}(x) = -p_k$, according to Property 6 the decryption result will be:

$$\begin{aligned} m' = \frac{c}{{k_2}'} &= \frac{m \cdot T_r(T_s(x))}{T_{s'}(T_r(x))} = \frac{m \cdot T_r(T_s(x))}{T_r(T_{s'}(x))} \\ &= \frac{m \cdot T_r(T_s(x))}{T_r(-T_s(x))} = \frac{m \cdot T_r(T_s(x))}{\pm T_r(T_s(x))} = \pm m \pmod p \end{aligned}$$

m' may be the right message, or the inverse element of m. The exact value of m is relevant with the value of r selected by the sender, but it can be easily decided by other means.

If the exact value of the minimal period is known, and s' satisfies $T_{s'}(x) = -p_k$, according to Property 7 an equivalent private key can be calculated as follows:

$$s = \frac{T_{min}}{2} - s' \pmod{T_{min}} \tag{9}$$

Therefore, a specific exhaustive attack method against the cryptosystem can be described as follows:

(1) Get the public key (x, p_k);
(2) Through exhaustive search, find an equivalent private key s', satisfying

$$T_{s'}(x) = \pm p_k \pmod p$$

(3) Get the cipher (c, k_1) from the sender;
(4) If $T_{s'}(x) = p_k \pmod p$, let $s = s'$; Else if $T_{s'}(x) = -p_k \pmod p$, and T_{min} is known, let $s = \frac{T_{min}}{2} - s' \pmod{T_{min}}$. Then use s to decrypt the cipher:

$$\begin{aligned} {k_2}' &= T_s(k_1) \pmod p \\ m' &= \frac{c}{{k_2}'} \pmod p \end{aligned}$$

m' is the right message.
(5) In other cases, use s' to decrypt the cipher:

$$\begin{aligned} {k_2}' &= T_{s'}(k_1) \pmod p \\ m' &= \frac{c}{{k_2}'} \pmod p \end{aligned}$$

and then pick up the right message from the set of $\{m', -m'\}$, by other means.

This method can also be used to find the equivalent value of parameter r that selected by sender in encryption process. If it was found, the message can also be got from the cipher. The necessary information for such attack is the public key p_k and the cipher (c, k_1). The complexity of this kind of attack is O(T_{min}). In order to make this attack impracticable, the minimal period of the Chebyshev polynomial sequence must be large enough.

B. Convert to GDLP

In [14] the trigonometry functions in finite fields are used to convert the computation of private key from public key to discrete logarithm problem. G. J. Fee and M. B. Monagan [10] give a more simple process for such a conversion, using hyperbolic function substitution. The corresponding discrete logarithm problem is treated in group ${F_p}^*$ or ${F_{p^2}}^*$, which means one must search private key among p or p^2 candidates. However, in some circumstances, one could search the private key in smaller space.

Proposition 2: The problem of finding private key from public key in the cryptosystem can be converted to a GDLP on a group G, whose order is T_{min}.

Proof: Assume $T_n(x) = y$. From Eq.3 it can be expressed as follows:

$$\frac{\lambda_1^n + \lambda_1^{-n}}{2} = y \pmod p$$

where $\lambda_1 = x + \sqrt{x^2-1}$. Solving the equation we can get

$$\begin{aligned} n &= \log_{\lambda_1} y \pm \sqrt{y^2-1} \\ &= \log_{x+\sqrt{x^2-1}} y \pm \sqrt{y^2-1} \pmod{T_{min}} \end{aligned} \quad (10)$$

If $x + \sqrt{x^2-1} \in F_p$, $y + \sqrt{y^2-1}$ must be in the same field, or else Eq.10 has no integer solution. In such case the problem can be converted to a GDLP on group G, where G is a subgroup of ${F_p}^*$. By the same reason, if $x + \sqrt{x^2-1}$ is not in F_p, the problem is a GDLP on G, where G is a subgroup of ${F_{p^2}}^*$.

As for the order of G, since T_{min} is a period of Chebyshev polynomial sequence, it is easy to know $(x + \sqrt{x^2-1})^{T_{min}} = 1$. Assume there is an positive integer r less than T_{min} satisfying $(x + \sqrt{x^2-1})^r = 1$, then according to Eq.3 $T_r(x) = 1$, which is opposite to the definition of T_{min}. So T_{min} is the minimal positive integer n satisfying $(x + \sqrt{x^2-1})^n = 1$, i.e. it is the order of group G. ■

According to that proposition, when the minimal period T_{min} is known, the private key can be searched in a group G with order of T_{min}, instead of ${F_p}^*$ or ${F_{p^2}}^*$. Various techniques have been presented to solve the GDLP, such as Baby-step giant-step algorithm [15], Pohlig-Hellman algorithm [16], Index-calculus algorithm [17], and so on. A brief survey about these techniques can be seen in [18]. When T_{min} is odd, from expression $T_n(x) = y$ two equivalent problems are acquired: $n = \log_{x+\sqrt{x^2-1}}(y + \sqrt{y^2-1})$, $n = \log_{x+\sqrt{x^2-1}}(y - \sqrt{y^2-1})$. If T_{min} is even, the equivalent private key can also be get by solving equation $T_n(x) = -y$, then another two equations $n = \log_{x+\sqrt{x^2-1}}(-y + \sqrt{y^2-1})$ and $n = \log_{x+\sqrt{x^2-1}}(-y - \sqrt{y^2-1})$ are added.

In some attack processes, when G is a subgroup of ${F_{p^2}}^*$, it may be required that all relevant values are represented with the same form. Suppose $y + \sqrt{y^2-1}$ is rewritten as the form of $a + b\sqrt{x^2-1}$. To determined a and b the following equation should be solved:

$$y + \sqrt{y^2-1} = a + b\sqrt{x^2-1} \pmod p$$

Since $\sqrt{x^2-1}$ is not in F_p, we have $a = y$ and $b = \sqrt{(y^2-1)(x^2-1)^{-1}}$. Hence the solution of that problem is equivalent to solve

$$n = \log_{x+\sqrt{x^2-1}}(a + b\sqrt{x^2-1})$$

C. Example

In this subsection, an example of Baby-step giant-step algorithm is given to illustrate the usage of period and symmetry properties of Chebyshev polynomial sequence in a cryptanalysis process. The Baby-step giant-step algorithm is describe as follows [15]:

Algorithm IV.1 Baby-step giant-step algorithm

Require: A generator α of a cyclic group G of order n, and an element $\beta \in G$

Ensure: The discrete logarithm $\log_\alpha \beta$

1. Set $m = \lceil n \rceil$.
2. Construct a table with entries $(j; \alpha^j)$ for $0 \le j < m$. Sort this table by second component.
3. Compute α^{-m} and set $\gamma \leftarrow \beta$.
4. For i from 0 to $m-1$ do the following:
   4.1 Check if γ is the second component of some entry in the table.
   4.2 If $\gamma = \alpha$ then return $n = im + j$.
   4.3 Set $\gamma \leftarrow \gamma \cdot \alpha^{-m}$.

If the algorithm is used directly, parameter m in step 1 should be set to $\lceil T_{min} \rceil$. Let $\alpha = x + \sqrt{x^2-1}$, and γ is either $y + \sqrt{y^2-1}$ or $y - \sqrt{y^2-1}$. The actual average running time of this algorithm is relevant with the choice of γ. If in fact $\log_\alpha \gamma < \frac{T_{min}}{2}$, it needs $\frac{5\sqrt{T_{min}}}{4}$ group multiplications on average. Otherwise if $\log_\alpha \gamma > \frac{T_{min}}{2}$, the average number of required group multiplications is $\frac{7\sqrt{T_{min}}}{4}$.

In our implementation, to even the running time both $y + \sqrt{y^2-1}$ and $y - \sqrt{y^2-1}$ will participate in the comparison process. In such case the smaller private key will be found firstly. Because it is just required to search the private key in range of $0 \sim \frac{T_{min}}{2}$, the parameter m can be set to $\sqrt{\frac{T_{min}}{2}}$, so the memory cost on the table constructed in Step 2 is saved. The average number of required group multiplications is $\sqrt{2T_{min}}$.

As an example, let $x = 5$, $p = 103$, and the value of Chebyshev polynomial $y = 91$. We want to get an integer n satisfying $T_n(x) = y$. First the question is converted to a GDLP in a group. The generator of the group is $x + \sqrt{x^2-1} = 5 + \sqrt{24}$, and its powers are $y \pm \sqrt{y^2-1} = 91 \pm \sqrt{(91^2-1)(5^2-1)^{-1}}\sqrt{5^2-1} = 91 \pm 97\sqrt{24}$. The minimal period is $T_{min} = 104$, which is the order of the group. Using Baby-step giant-step algorithm the logarithm $\log_{5+\sqrt{24}}(91 \pm 97\sqrt{24})$ is computed as follows:

1. Set $m \leftarrow \lceil \sqrt{\frac{104}{2}} \rceil = 8$.

2. Construct a table whose entries are (j, α^j) for $0 \leq j < 8$. For convenience denote the power α^j by the form of $a_j + b_j\sqrt{24}$. These entries are shown in Table I. Table II is resulted from Table I with the entries sorted by a_j.

TABLE I.
α^j

j	0	1	2	3	4	5	6	7
a_j	1	5	49	73	63	42	48	26
b_j	0	1	10	99	53	19	34	12

TABLE II.
α^j(SORTED)

j	0	1	7	5	6	2	4	3
a_j	1	5	26	42	48	49	63	73
b_j	0	1	12	19	34	10	53	99

3. Compute $\alpha^{-m} = (5 + \sqrt{24})^8 = 6 + 17\sqrt{24}$.

4. Compute $\gamma_1 = \beta_1 \cdot \alpha^{-mi}$ and $\gamma_2 = \beta_2 \cdot \alpha^{-mi}$, until one of them equals to anyone in Table II. This yields Table III and Table IV.

TABLE III.
$\gamma_1 = \beta_1\alpha^{-mi}$

i	0	1	2	3	4
a_i	91	55	54	78	58
b_i	97	69	10	51	87

TABLE IV.
$\gamma_2 = \beta_2\alpha^{-mi}$

i	0	1	2	3	4
a_i	91	7	96	12	48
b_i	6	38	38	6	34

In Table IV, $\beta\alpha^{-4m} = 48 + 34\sqrt{24}$ equals to the value with α^6 in Table II, so the private key $n = im + j = 4 \times 8 + 6 = 38 \pmod{104}$.

In fact, as T_{min} is even, odd symmetry can be used to find private key more quickly. In Step 4 $-\gamma_1$ and $-\gamma_2$ can be added to compare with elements in Table II. If $-\gamma_1 = \alpha^m i$ or $-\gamma_2 = \alpha^m i$, then the right private key can be calculated by relation (9). In this example it can be found $55 + 69\sqrt{24}$ of Table III is the opposite number of $48 + 34\sqrt{24}$ in Table II. So the value of n' is $mi + j = 8 \times 1 + 6 = 14 \pmod{104}$, then $n = \frac{T_{min}}{2} - n' = \frac{104}{2} - 14 = 38 \pmod{104}$.

V. PRINCIPLES OF PARAMETER SELECTION

As mentioned before, the security of the cryptosystem is relevant with its corresponding Chebyshev polynomial sequence, whose characteristic is in turn decided by parameters x and p. This section will further discuss the impact of these parameters on the security of the cryptosystem, and propose some principles for parameter selection.

A. Security in different fields

The cryptanalysis of the cryptosystem can be converted to solving GDLP in a group G, where G is either a subgroup of ${F_p}^*$, or a subgroup of ${F_{p^2}}^*$. In different circumstances, the complexity of these attack algorithms is shown in Table V.

The results come from reference [15], where T_{min} or $p - 1$ can be factorized as ${p_1}^{e_1}{p_2}^{e_2}...{p_r}^{e_r}$.The Index calculus method is implemented in form of number field sieve method. With Pohlig-Hellman algorithm the values of T_{min} and p_is are not the same under different circumstances, but the complexity is in the same level. The complexity of attack algorithms against Elgamal cryptosystem is also given as a reference.

Before further comparison, two states should be made. First, it is not a necessary condition that T_{min} equals to $p \pm 1$, but is the best case from view of security. For convenience of following discussion, suppose T_{min} take the maximum value, i.e. $T_{min} = p \pm 1$. Second, when G is subgroup of ${F_{p^2}}^*$, the basic multiplication arithmetic of the group is composed of 5 integer multiplications, which has direct influence on the time cost of cryptanalysis methods.

Therefore, when G is subgroup of ${F_p}^*$, both the complexity of and the time cost of cryptanalysis against that cryptosystem are no more than that of Elgamal cryptosystem, so it is of little value in practice. On the other hand, when G is subgroup of ${F_{p^2}}^*$, and exhaustive search attack, Baby-step Giant-step algorithm or Pohlig-Hellman algorithm is applied, even the complexity of cryptanalysis is in the same level, its time cost is greater than that against Elgamal cryptosystem. As for the Index calculus algorithm, the cryptanalysis algorithm must be performed in ${F_p}^*$ or ${F_{p^2}}^*$. Hence its complexity is more than that against Elgamal cryptosystem, which means the cryptosystem can resist against Index calculus algorithm more effectively. So the cryptosystem should work on ${F_{p^2}}^*$ to achieve the best security.

B. Prime

The complexity of exhaustive attack is $O(T_{min})$ and that of Baby-step giant-step attack is $O(\sqrt{T_{min}})$. To resist these attacks the minimal period T_{min} of the Chebyshev polynomial sequence must be large enough, which means prime p must be large enough.

The GDLP problem is on subgroup of ${F_{p^2}}^*$ if and only if The ordinary period of the Chebyshev polynomial sequence is $p + 1$, which can be deduced from the following proposition.

Proposition 3: The Chebyshev polynomial sequence has ordinary period $p-1$ if and only if $\sqrt{x^2 - 1}$ is in F_p; when $T_{min} > 2$, the Chebyshev polynomial sequence has ordinary period $p+1$ if and only if $\sqrt{x^2 - 1}$ is not in F_p.

Proof: If $\sqrt{x^2 - 1} = 0$, $T_{min} = 1$, $p - 1$ is an ordinary period of the sequence.

If $\sqrt{x^2 - 1} \in F_p$ and $\sqrt{x^2 - 1} \neq 0$, then $x^2 - 1$ is a

TABLE V.
COMPLEXITY OF DIFFERENT CRYPTANALYSIS METHODS

	Elgamal cryptosystem	This cryptosystem($G \in F_p{}^*$)	This cryptosystem($G \in F_{p^2}{}^*$)
exhaustive search	$O(p-1)$	$O(T_{min})$	$O(T_{min})$
Baby-step Giant-step algorithm	$O(\sqrt{p-1})$	$O(\sqrt{T_{min}})$	$O(\sqrt{T_{min}})$
Pohlig-Hellman algorithm	$O(\sum_{i=1}^{r} e_i(lg(p-1)+\sqrt{p_i}))$	$O(\sum_{i=1}^{r} e_i(lgT_{min}+\sqrt{p_i}))$	$O(\sum_{i=1}^{r} e_i(lgT_{min}+\sqrt{p_i}))$
Index calculus algorithm	$L_p(\frac{1}{3},c)$	$L_p(\frac{1}{3},c)$	$L_{p^2}(\frac{1}{3},c)$

quadratic residue modulo p, so the Legendre symbol [15]

$$\left(\frac{x^2-1}{p}\right) = (x^2-1)^{\frac{p-1}{2}} = 1 \pmod p$$

which means

$$\begin{aligned} T_{p+1}(x) &= (x^2-1)^{\frac{p+1}{2}} + x^2 \\ &= (x^2-1)^{\frac{p-1}{2}} \cdot (x^2-1) + x^2 \\ &= 2x^2 - 1 \pmod p \end{aligned}$$

so $T_{p-1}(x) = 1$, and $p-1$ is the ordinary period of the sequence. By the reverse deduction it can be proved that, if $p-1$ is the ordinary period of the sequence, $\sqrt{x^2-1}$ must be in F_p. The first half of this proposition is proved.

In the case of $T_{ord} = p+1$, when $T_{min} = 1$ or $T_{min} = 2$, $p-1$ is also the ordinary period of the sequence, $\sqrt{x^2-1}$ is in F_p; otherwise $T_{ord} = p+1$ is equivalent to $\sqrt{x^2-1} \notin F_p$, and the proof is similar. ■

According to the proposition, the ordinary period of Chebyshev polynomial sequence should be factor of $p+1$. That state results in the succeeding discussion about the selection of p.

If all the factors of T_{min} are small, then the Pohlig-Hellman algorithm can be used to break the cryptosystem with complexity of $O(\log^2(T_{min}))$ [16]. So T_{min} should have at least one large prime factor. In present circumstance, $p+1$ should satisfy the same condition.

The odd symmetry can reduce the key space of the cryptosystem by half. When $T_{min} = p+1$ and $\frac{p+1}{2}$ is odd, then the odd symmetry can be avoided. Therefore, to achieve the greatest key space $p+1$ should have only one factor of 2.

Therefore, the recommended prime p should satisfy: (1) it is large enough; (2) $p+1$ has at least one large prime factor; (3) $p+1$ has only one factor of 2.

C. Initial value

After prime p is selected, a proper x should be chosen to guarantee: (1) the Chebyshev polynomial sequence is on $F_{p^2}{}^*$; (2) the minimal period of the sequence equals to $p+1$.

For the first condition, one only need to find a x that x^2-1 is a quadratic nonresidue, i.e. the Legendre symbol

$$\left(\frac{x^2-1}{p}\right) = -1 \pmod p$$

For the second condition, in order to generate a sequence with the minimal period of $p+1$, parameter x must be a "prime generator". The method to find a prime generator for Chebyshev polynomial sequence is analogous to that for a cyclic group. The process can be described as Algorithm V.1:

Algorithm V.1 Find a prime generator for Chebyshev polynomial sequence

Require: Prime number p
Ensure: A generator x
1. Choose a random element x in $F_p{}^*$, where $x \neq 1$.
2. Suppose $p+1 = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ where p_i is prime. For i from 1 to k do the following:
   2.1 Let $n = \frac{p+1}{p_i}$, Compute $y = T_n(x)$.
   2.2 If $y = 1$ then go to step 1.
return x.

When p and x is chosen properly, the cryptosystem can resist various attacks against the GDLP. Notice the even symmetry still exists in such a sequence, so the factual private key space of the cryptosystem is $\frac{p+1}{2}$.

VI. CONCLUSION

In this paper a new representation of Chebyshev polynomial is introduced to study the security of a public key cryptosystem. First the properties of Chebyshev polynomial sequence are investigated. Based on these properties two kinds of attacks are analyzed. It is found if parameters are not selected properly the cryptosystem could be broken easily. To make the cryptosystem secure, some principles for parameter selection have been proposed. Some other problems stated in previous references are not mentioned in this paper, but they can also be studied by the representation. For example, as a Chebyshev polynomial sequence is corresponding to a group whose order is known, the period distribution density of the sequence can be proved. Therefore the method adopted in this paper is supposed to be useful to future researches on this topic.

VII. ACKNOWLEDGMENT

This work is supported by China 973 Program(Grant No.2009CB320505), China 863 Program(Grant No.2010AA012501), National Natural Science Foundation of China(Grant No. 61002011).

REFERENCES

[1] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644 – 654, nov. 1976.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[3] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Cambridge, MA, USA, Tech. Rep., 1979.
[4] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *Information Theory, IEEE Transactions on*, vol. 31, no. 4, pp. 469 – 472, jul. 1985.
[5] P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev, "Security of public-key cryptosystems based on chebyshev polynomials," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 52, no. 7, pp. 1382 – 1393, jul. 2005.
[6] L. Kocarev and Z. Tasev, "Public-key encryption based on chebyshev maps," vol. 3, Bangkok, Thailand, may. 2003, pp. III–28 – III–31 vol.3.
[7] K. Cheong and T. Koshiba, "More on security of public-key cryptosystems based on chebyshev polynomials," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, vol. 54, no. 9, pp. 795 –799, sep. 2007.
[8] D. Xiao, X. Liao, and S. Deng, "A novel key agreement protocol based on chaotic maps," *Information Sciences*, vol. 177, no. 4, pp. 1136 – 1142, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/B6V0C-4KM45Y6-4/2/247571c6d878910d1a505481c458be35
[9] K. Prasadh, K. Ramar, and R. Araman, "Public key cryptosystems based on chaotic-chebyshev polynomials," Kottayam, Kerala, oct. 2009, pp. 4 –8.
[10] G. J. Fee and M. B. Monagan, "Cryptography using chebyshev polynomials," Burnaby, Canada, 2004. [Online]. Available: http://oldweb.cecm.sfu.ca/CAG/papers/Cheb.pdf
[11] L. Kocarev, J. Makraduli, and P. Amato, "Public-key encryption based on chebyshev polynomials," *Circuits, Systems, and Signal Processing*, vol. 24, pp. 497–517, 2005, 10.1007/s00034-005-2403-x. [Online]. Available: http://dx.doi.org/10.1007/s00034-005-2403-x
[12] H. Ning, Y. Liu, and D. He, "Public key encryption algorithm based on chebyshev polynomials over finite fields," vol. 4, Guilin, China, nov. 2006.
[13] X. Liao, F. Chen, and K. wo Wong, "On the security of public-key algorithms based on chebyshev polynomials over the finite field z_n," *Computers, IEEE Transactions on*, vol. 59, no. 10, pp. 1392 –1401, oct. 2010.
[14] J. Lima, R. Campello de Souza, and D. Panario, "Security of public-key cryptosystems based on chebyshev polynomials over prime finite fields," Toronto, Canada, jul. 2008, pp. 1843 –1847.
[15] A. J. Menezes, P. C. V. Oorschot, S. A. Vanstone, and R. L. Rivest, *Handbook of Applied Cryptography*. New York: CRC Press, 1997.
[16] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over $gf(p)$ and its cryptographic significance (corresp.)," *Information Theory, IEEE Transactions on*, vol. 24, no. 1, pp. 106 – 110, jan. 1978.
[17] L. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," San Juan, Puerto Rico, oct. 1979, pp. 55 –60.
[18] A. Odlyzko, "Discrete logarithms: the past and the future," *Designs, Codes, and Cryptography*, vol. 19, pp. 129–145, 1999.