Provably Secure Public Key Cryptosystem Based on Chebyshev Polynomials

Shijie Yan[1], Ping Zhen[1], and Lequan Min[1, 2]
[1] School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing 100083, China
[2] School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China
Email: {yanshijie0303, minlequan}@sina.com; zhenping1989@126.com

Abstract —Chebyshev polynomials based public key cryptosystem (CPPKC), proposed by L. Kocarev in 2003, has emerged as a new research field in cryptography and attracted a lot of attentions in recent years. Although provable security in traditional public key cryptosystem has already been developed about twenty years, no relevant security proof research has been found about CPPKC. Aiming at the disability of CPPKC to resist against the adaptive chosen ciphertext attack, we construct a provably secure CPPKC, namely PS-CPPKC, which is designed utilizing the benefits of hash function and its security proof is completed under the Cheybshev Diffie-Hellman problem (CDHP) assumption by probabilistic analyses and computation in random oracle model. This is our primary exploration and it shows that provable security theory can combine well with CPPKC.

Index Terms—Chebyshev polynomials, public key cryptosystem, chosen ciphertext attack, provable security

I. Introduction

In 1976, the publication of the paper "New directions in cryptography" by Diffie and Hellman [1] opened the new exploration filed of public key cryptosystem. Since then, numerous public key algorithms have been proposed utilizing the one way trapdoor function. The most widely used traditional public key cryptosystems include RSA, Elgamal cryptosytem and elliptic curve cryptosystem. Besides, there are also knapsack based public key cryptosystem [2], lattice based public key cryptosystem [3], algebraic coding based public key cryptography [4] and so on. In this paper, we will focus on a kind of chaos based public key cryptosystem, which is constructed by Chebyshev polynomials [5], [6].

Security is the basic principle of designing public key cryptosystem. Previous work mainly relies on the analyses of cryptanalyst to guarantee the security of cryptosystem, which is recurrence of analyses-improvement process. But this method is not complete and reliable. With the further research, formal security proof is quite necessary. The proof can be accomplished by the reduction of public key cryptosystem security to the mathematical hard problem security. If the security of cryptosystem can be reduced to the mathematical hard problem without any other assumption, then the cryptosystem is called provably secure in standard model [7]. But security proof in standard model is very difficult. So random oracle, usually regarded as ideal hash function, is introduced to prove the security [8]. In this situation, provably secure public key cryptosystem is called secure in random oracle model. Even if provably secure cryptosystem cannot guarantee the security completely in random oracle model, it is still a widely accepted method to measure the security of public key cryptosystem.

Since Rackoff and Simon [9] introduced the notion called indistinguishability under adaptive chosen ciphertext attack (IND-CCA2), which is equivalent to non-malleability [10], IND-CCA2 security has become a standard security goal for public key encryption. In 1994, Bellare and Rogaway proposed the Optimal Asymmetric Encryption Padding (OAEP) scheme [8], which was proved to provide semantic security against adaptive chosen-ciphertext attack in the random oracle model. Then many provably secure schemes [11]-[13] have been proposed in the random oracle model.

Chebyshev polynomials based public key cryptosystem (CPPKC), as a kind of chaos based cryptography, attracted a lot of attentions in recent years [5], [6], [14]-[17]. Compared to traditional cryptosystem, the private key of CPPKC can guarantee the security even for small integer, so there is no need to look for very large numbers; for the Chebyshev chaotic maps, x and $T_r(x)$ are independent random variables, which also enhance the security. As far as we know, there is no relevant research about security proof of CPPKC. Since CPPKC is not secure against IND-CCA2, our main contribution is to construct provably secure CPPKC, called PS-CPPKC, which is the primary exploration to combine CPPKC with security proof theory. Our scheme, constructed by hash function, is provably secure under the Cheybshev Diffie-Hellman problem (CDHP) in random oracle model. We will present the detailed proof procedure in this paper.

This paper is organized as follows. Section II introduces the preliminaries about CPPKC, relevant mathematical hard problem about CPPKC and the definition of IND-CCA2. Then the constructed PS-

Manuscript received March 30, 2015; revised June 24, 2015.
This work was supported by National Natural Science Foundation of China (Grant No. 61170037) and the Specialized Research Fund for Doctoral Program of Higher Education of China (No. 11280102).
Corresponding author email: zhenping1989@126.com.
doi:10.12720/jcm.10.6.380-384

CPPKC, with explicit security proof, is described in Section III. Brief implementation of the PS-CPPKC is given in Section IV. Then the last section presents the conclusions.

II. Preliminaries

A. Chebyshev Polynomial

Definition 1 (Chebyshev polynomial [5]). Let $n \in Z^+$ and $x \in [-1,1]$, the Chebyshev polynomial of order n, $T_n(x):[-1,1] \to [-1,1]$, is defined as algebraic expression:

$$T_n(x) = \cos(n \cdot \arccos(x)) \quad (1)$$

Its equivalent recurrence definition is:

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

where $T_0(x) = 1$ and $T_1(x) = x$.

The Chebyshev polynomials exhibit the following important properties: the semi-group property and the chaotic property.

The semi-group property

$$T_r(T_s(x)) = T_{sr}(x) = T_s(T_r(x)) \quad (3)$$

where r and s are positive integer numbers and $x \in [-1,1]$.

(1) The chaotic property

When the degree $n > 1$, the Chebyshev polynomial map $T_n(x):[-1,1] \to [-1,1]$ is a chaotic map with its invariant density $f^*(x) = 1/(\pi\sqrt{1-x^2})$, and positive Lyapunov exponent $\lambda = \ln n > 0$.

TABLE I: THE ORIGINAL CPPKC SCHEME

Public parameters: select a large prime P and a random positive number $x \in F_P$, $x \neq 1$.

Key generation: Randomly generate a large integer s and compute $T_s(x)$. The public key is $T_s(x)$ and private key is s.

Message encryption: To encrypt the message $m \in Z_P$,

1). randomly select a positive integer $r \in Z_P$

2). compute $c_1 = T_r(x)$ and $c_2 = m \cdot T_r(T_s(x))$

Output the ciphertext $c = (c_1, c_2)$.

Message decryption: To decrypt the ciphertext c,

1). use the private key to compute $T = T_s(c_1) = T_s(T_r(x))$

2). recover the plaintext by computing $m = c_2 \cdot T^{-1}$

Remark: The modular symbol " $\bmod P$ " is omitted for the simple description.

The semi-group property is very useful to construct public key cryptosystem [5]. When $x \in [-1,1]$, the explicit algebraic expression of $T_n(x)$ can lead to security loophole in the public-key cryptosystem [18]. To resist this attack, Kocarev et al. extended the definition of $T_n(x)$ to the finite field F_P (see the equation(4)) and improved the public key cryptosystem [6], as shown in the Table I.

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \bmod P \quad (4)$$

where $n \geq 2$ and P is a large prime.

It is obvious that the CPPKC is not secure against IND-CCA2 attack. Specifically, suppose the adversary wants to decrypt the ciphertext $c = (c_1, c_2) = (T_r(x), m \cdot T_{rs}(x))$. The adversary can select an integer k and construct the ciphertext $c' = (c_1', c_2') = (c_1, k \cdot c_2)$. Then he request to decrypt c' and get $m' = T_{rs}(x)^{-1} c_2' = km$. So the adversary can recover the plaintext of c by computing $m = k^{-1}m'$. In this paper, we construct a secure scheme based on CPPKC and prove its security in rand oracle model.

B. Mathematical Hard Problem

This part introduces some basic mathematical hard problems about Chebyshev polynomials. They are not only the basic intractable problems to construct public key cryptosystem, but also the key points to prove the security.

Definition 2. Chebyshev discrete logarithm problem (CDLP): given the element (x, y), it is computationally infeasible to find the integer s, such that $T_s(x) = y$.

Definition 3. Chebyshev Diffie-Hellman problem (CDHP): given the element $(x, T_r(x), T_s(x))$, it is computationally infeasible to get $T_{rs}(x)$.

The two problems are both conjectured to be hard and can be used as assumptions to prove the security of CPPKC. There are obvious polynomial-time reductions from CDHP to CDLP, but the reductions in the reverse direction are unknown. Moreover, CDHP assumption is stronger than CDLP.

C. Security Against IND-CCA2

According to Rackoff and Simon's definition [9], security against IND-CCA2 is defined via a game played between the adversary and simulator. The game consists of two stages: find stage and guess stage. In the find stage, the adversary makes arbitrary decryption query from the simulator, decrypting the ciphertext of his choice. Next in the guess stage, the adversary chooses two messages (m_1, m_2), and sends them to the simulator. The simulator randomly chooses a bit $b \in \{0,1\}$, and returns the ciphertext c of m_b to the adversary. After receiving the ciphertext c, the adversary can continue to ask for decryption query with the restriction that the query ciphertext c' is different from c. In the end, adversary outputs $b' \in \{0,1\}$, as the guess value of b. The adversary's advantage is defined as follows:

$$Adv(A) = \Pr[b = b'] - \frac{1}{2} = \varepsilon \quad (5)$$

where $\Pr[b = b']$ denotes the probability of $b' = b$.

The public key cryptosystem is said to be secure against IND-CCA2 if the advantage ε of any-polynomial time adversary is negligible.

III. The Proposed PS-CPPKC

A. Description of PS-CPPKC

As mentioned above, the CPPCK is not secure against IND-CCA2 attack. To enhance its security, we make use of the one-way hash function to construct the provably secure CPPKC, as shown in Table II, and will prove its security in random oracle.

TABLE II. DESCRIPTION OF PS-CPPKC

Public parameters: select a large prime P, a random positive number $x \in F_P$, $x \neq 1$ and a one-way hash function $H: \{0,1\}^* \to \{0,1\}^k$.

Key generation: Randomly generate a large integers s and compute $y = T_s(x)$. The public key is y and private key is s.

Message encryption: To encrypt the message $m \in Z_P$ with the length of l bits

1). randomly selects two positive integers $r_1, r_2 \in Z_P$

2). compute $c_1 = T_{r_1}(x)$ and $c_2 = T_{r_2}(x)$

3). compute $h_1 = T_{r_1}(y)$ and $h_2 = T_{r_2}(y)$

4). Let $t = h_1 \| h_2$, $\alpha = H(t)$ and $M = (m \| \alpha) \oplus h_2$

5). compute $c_3 = Mh_1 \bmod P$

Output the ciphertext $c = (c_1, c_2, c_3)$.

Message decryption: To decrypt the ciphertext c with the private key s,

1). compute $h_1 = T_s(c_1)$, $h_2 = T_s(c_2)$ and $M = h_1^{-1} c_3$

2). compute $m = [M \oplus h_2]_{1\cdots l}$ and $\alpha = [M \oplus h_2]_{l+1, \cdots, l+k}$

If $\alpha = H(h_1 \| h_2)$, m is the legitimate plaintext; otherwise, output $\perp$.

Remark: " $\|$ " denotes the concatenation of binary string; " $[\cdot]_{i\cdots j}$ " denotes extracting the bits from position i to j.

B. Security Proof in Random Oracle Model

In this section, we prove the security PS-CPPKC referring to the method in [8], [19]. We show that it is secure against IND-CCA2 in random oracle model. Namely, the following theorem holds.

Theorem. The PS-CPKC is indistinguishable against adaptive chosen-ciphertext attack under the CDHP assumption in random oracle model.

Suppose the adversary A has the advantage e in IND-CCA2 attack, then there exists a polynomial time algorithm, which has the advantage e' in breaking the CDHP assumption, where

$$e' \geq 2e - n_D 2^{-k} \tag{6}$$

where n_D is the query number of decryption oracle $\mathcal{O}_D(\cdot)$, k is the bit length of hash value.

The explicit procedure of reduction proof is as follows:

The proof is conducted by an IND-CCA2 attacking game between the adversary A and simulator M. M is given a random target ciphertext c^* and tries to decrypt it without private key. If M can decrypt c^*, this can help to solve the CDHP assumption. A can only communicates with M according to the game rules.

The reduction proof is divided into the following two stages.

1) Find stage: M simulates the random oracle $\mathcal{O}_H(\cdot)$ and decryption oracle $\mathcal{O}_D(\cdot)$ to the adversary A. This helps A learn some valuable knowledge about PS-CPKC. The precise simulation is necessary to guarantee that it seems like a real attack for adversary A rather than playing a game. In this stage, A can construct any ciphertext by his choice. But A needs to request the service of random oracle $\mathcal{O}_H(\cdot)$; otherwise, A can only construct the legitimate ciphertext with negligible probability.

2) Guess stage: A sends M a pair of plaintext (m_0, m_1) with equal length. M chooses a random bit $b \in \{0, 1\}$ and regards the target c^* as the ciphertext of m_b. It is almost impossible for A to find that he is tricked by M, which will be explained explicitly below. In the IND-CCA2 attack, A can still get the random oracle $\mathcal{O}_H(\cdot)$ and decryption oracle $\mathcal{O}_D(\cdot)$ service from M. But A cannot request to decrypt c^*, which is the target ciphertext M needs to decrypt in the simulation game. According to the knowledge learnt from the procedure, A guesses b' as the value of b and finishes the game.

In the procedure, M needs to conduct two kinds of simulation: random oracle $\mathcal{O}_H(\cdot)$ and decryption oracle $\mathcal{O}_D(\cdot)$. Let us explain the details.

1) Simulation of random oracle $\mathcal{O}_H(\cdot)$

The simulation of $\mathcal{O}_H(\cdot)$ is simple. M firstly initializes an empty table T. When A requests an random oracle query t, M searches the table list to see whether t exists. If it exists, M returns the corresponding value $\alpha = H(t)$ to A; otherwise, M provides A with a random hash value, and adds (t, α) to the table list.

If the query happens in the guess stage, M will try to decrypt $c^* = (c_1^*, c_2^*, c_3^*)$ by (t, α), $t = h_1 \| h_2$, $\alpha = H(t)$. Then M computes:

$$M^* = h_1^{-1} c_3^* \bmod P,$$

$$m^* = [M^* \oplus h_2]_{1\cdots l},$$

$$\alpha^* = [M^* \oplus h_2]_{l+1, \cdots, l+k},$$

Then M checks whether $\alpha = \alpha^*$ holds. If so, M can get m^* as the plaintext of target ciphertext c^*. Then M can obtain $h_1 = T_{r_1 s}(x)$ with $y = T_s(x)$ and $c_1^* = T_{r_1}(x)$. That is to say, M can break CDHP assumption and win the game.

2) Simulation of decryption oracle $\mathcal{O}_D(\cdot)$

When receiving the ciphertext $c' = (c_1', c_2', c_3')$ for decryption from A, M will search whether there is $\alpha = H(t)$ in the table T. For each pair (t, α), M computes

$$M' = h_1^{-1} c_3' \bmod P$$
$$m' = [M' \oplus h_2]_{1\cdots l},$$
$$\alpha' = [M' \oplus h_2]_{l+1,\cdots,l+k},$$

If $\alpha = \alpha'$, M returns m to A as the plaintext of c'; otherwise, M returns $\perp$.

The decryption simulation procedure is also very precise. A cannot realize that he is tricked by M even with a legitimate ciphertext except with a negligible probability. If A wants to construct a legitimate ciphertext $c = (c_1, c_2, c_3)$, he first needs to request the random oracle service. If α has been queried, then M can perform the decryption procedure accurately; otherwise, M rejects the decryption request, which is almost correct except with negligible probability 2^{-k}.

Then let us analyze the advantage e' of the simulator M. For the simple description, we define some probabilistic events. Let the bad event E_1 denotes that M mistakenly rejects a legitimate ciphertext in the decryption query, then

$$\Pr[E_1] \approx n_D \cdot 2^{-k} \tag{7}$$

Another bad event for M is that A discovers the target ciphertext c^* has nothing to do with the chosen plaintexts $\{m_0, m_1\}$. This is almost impossible except when $\alpha = \alpha^*$ is in the table T. We denote this event by E_2.

Let E_{Bad} denotes the union of E_1 and E_2, namely, $E_{Bad} = E_1 \cup E_2$. Let E_{Awin} denotes the event when A finally can guess the bit b and win the game. Let E_{Mwin} denotes M can decrypt the ciphertext c^* without the private key at last. Only when E_2 happens, M can decrypt c^* and win the game, so

$$\Pr[E_{Mwin}] = \Pr[E_2] \tag{8}$$

For the adversary A, if the event E_{Bad} does not appear, then bit b and the target ciphertext c^* are independent with each other because of the uniform distribution of random oracle, namely:

$$\Pr[E_{Awin} \mid \overline{E_{Bad}}] = \frac{1}{2} \tag{9}$$

According to the conditional probability formula, we can get

$$\begin{aligned} \Pr[E_{Awin} \cap \overline{E_{Bad}}] &= \Pr[E_{Awin} \mid \overline{E_{Bad}}] \Pr[\overline{E_{Bad}}] \\ &= \frac{1}{2} \Pr[\overline{E_{Bad}}] = \frac{1}{2}(1 - \Pr[E_{Bad}]) \end{aligned} \tag{10}$$

The attack advantage of A can be defined as :

$$Adv(A) = \Pr[b' = b] - \frac{1}{2} = e \tag{11}$$

So

$$\Pr[E_{Awin}] = \frac{1}{2} + e \tag{12}$$

According to the law of total probability,

$$\Pr[E_{Awin}] = \Pr[E_{Awin} \cap \overline{E_{Bad}}] + \Pr[E_{Awin} \cap E_{Bad}] \tag{13}$$

Since

$$\Pr[E_{Awin} \cap E_{Bad}] \le \Pr[E_{Bad}] \tag{14}$$

Then

$$\Pr[E_{Awin} \cap \overline{E_{Bad}}] + \Pr[E_{Bad}] \ge \frac{1}{2} + e \tag{15}$$

According to the above result,

$$\frac{1}{2}(1 - \Pr[E_{Bad}]) + \Pr[E_{Bad}] \ge \frac{1}{2} + e \tag{16}$$

$$\Pr[E_{Bad}] \ge 2e \tag{17}$$

Since

$$E_{Bad} = E_1 \cup E_2 \tag{18}$$

So

$$\begin{aligned} \Pr[E_{Bad}] &= \Pr[E_1 \cup E_2] \\ &\le \Pr[E_1] + \Pr[E_2] \\ &= \Pr[E_1] + \Pr[E_{Mwin}] \end{aligned} \tag{19}$$

So

$$\Pr[E_{Mwin}] \ge \Pr[E_{Bad}] - \Pr[E_1] = 2e - n_D 2^{-k} \tag{20}$$

$$e' \ge 2e - n_D 2^{-k} \tag{21}$$

Since under the CDHP assumption and in the random oracle , e' and $n_D 2^{-k}$ are both negligible, so e is negligible. This completes the proof of the theorem.

IV. The Implementation of PS-CPPKC

In PS-CPPKC, the hash function can be instantiated by the one based on coupled chaotic map lattices [20], which has the extreme sensitivity of chaotic system. With the properties of one-way, good confusion, diffusion and approximate uniform distribution, it can approach an ideal hash function to be the random oracle. What is more, the hash function is also flexible and efficient to satisfy the requirement of PS-CPPKC.

The computation of Chebyshev polynomials is the key point to influence the efficiency of PS-CPPKC. There are two common methods to compute them. The first one [5] utilizes the semi-group property of Cheybshev polynomials. It can reach high efficiency but with limited application. The second one [18], making use of matrix exponentiation, is a universal method with computational complexity of $O(\log n)$. Recently, a new method [21] has also been proposed to further improve the efficiency of Chebyshev polynomials computation, which will make PS-CPPKC more practical.

V. Conclusions

In order to guarantee the security of Chebyshve polynomials based public key cryptosystem against

adaptive chosen ciphertext attack, we propose a new scheme and prove their security explicitly. The constructed scheme, PS-CPPKC, relies on the random oracle, which is an effective technique to evaluate the security of CPPKC. This is the primary exploration to combine provably secure theory with CPPKC. However, provable security in random oracle may be controversial in cryptography and more investigations are still needed to construct secure and efficient cryptosystem in standard model for real applications. This will be our future research work. Provably secure digital signature and key agreement protocol based on Cheybyshev polynomials, are also very interesting topics worth further research.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for helpful comments and suggestions. The work is supported by the National Natural Science Foundation of China (Grant No.61170037) and the Specialized Research Fund for Doctoral Program of Higher Education of China (No. 11280102).

REFERENCES

[1] W. F. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 10, pp. 644–655, 1976.

[2] M. S. Lee, "Improved cryptanalysis of a knapsack-based probabilistic encryption scheme," *Inf. Sci.*, vol. 222, pp. 779-783, 2013.

[3] V. Lyubashevsky, "Lattice Signatures without Trapdoors," *Advances in Cryptology-EUROCRYPT*, vol. 7237, pp. 738-755, 2012.

[4] H. Fujita, "Quantum McEliece public-key cryptosystem," *Quantum Information & Computation*, vol. 12, no. 3-4, pp. 181-202, 2012.

[5] L. Kocarev and Z. Tasev, "Public-key encryption based on Chebyshev maps," in *Proc. IEEE International Symposium on Circuits System*, May25-28, 2003, vol. 3, pp. 28-31.

[6] 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.

[7] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," *Advances in Cryptology-CRYPTO '99*, LNCS, Springer-Verlag, 1998, vol. 1462, pp.13–25.

[8] M. Bellare and P. Rogaway, "Optimal asymmetric encryption - how to encrypt with RSA," in *Advances in Cryptology - Eurocrypt*, LNCS, Springer-Verlag, 1994, vol. 950, pp. 92-111.

[9] C. Rackoff and D. Simon, "Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack," in *Advances in Cryptology-Crypto '91*, 1991, pp. 433-444.

[10] D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography," *SIAM Journal on Computing*, vol. 30, no. 2, pp. 391-437, 2000.

[11] E. Fujisaki and T. Okamoto, "How to enhance the security of public-key encryption at minimum cost," *IEICE Transaction of Fundamentals of Electronic Communications and Computer Science*, vol. E83-A, pp. 24-32, 2000.

[12] T. Okamoto and D. Pointcheval, "REACT: Rapid enhanced-security asymmetric cryptosystem transform," in *CT - RSA 2001*, LNCS 2020, Springer-Verlag, 2001, pp. 159-175.

[13] D. H. Phan and D. Pointcheval, "OAEP 3-Round: A generic and secure asymmetric encryption padding," in *Asiacrypt*, LNCS 3329, Springer-Verlag, 2004, pp. 63-77.

[14] X. Liao, F. Chen, and K. Wong, "On the security of public-key algorithms based on Chebyshev polynomials over the finite field Z_N," *IEEE Transactions on Computers*, vol. 59, no. 10, pp. 1392-1401, 2010.

[15] Q. Xie, J. Zhao, and X. Yu, "Chaotic maps-based three-party password-authenticated key agreement scheme," *Nonlinear Dynamics*, vol.72, no. 4, pp. 1021-1027, 2013.

[16] C. Guo and C. C. Chang, "Chaotic maps-based password-authenticated key agreement using smart cards," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 6, pp. 1433-1440, 2013.

[17] X. Y. Wang and D. P. Luan, "A secure key agreement protocol based on chaotic maps," *Chin. Phys. B*, vol. 22, no. 11, 2013.

[18] P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev, "Security of public-key encryption based on Chebyshev polynomials," *IEEE Transaction on Circuits and Systems I: Regular Paper*, vol. 52, no. 7, pp. 1382-1393, 2005.

[19] J. Liu, G. L. Chen, and J. H. Li, "Revision of security proof on f-OAEP," in *Proc. International Conference on Information Security and Assurance*, Busan, Korea, 24-26 April 2008, pp. 280-284.

[20] P. Zhen, G. Zhao, and L. Q. Min Lequan, "Novel hash function based on coupled chaotic map lattices," *Chinese Journal of Electronics*, vol. 23, no. 4, pp. 836-841, 2014.

[21] Z. H. Li, Y. D. Cui, and H. M. Xu, "Fast algorithms of public key cryptosystem based on Chebyshev polynomials over finite field," *The Journal of China Universities of Posts and Telecommunications*, vol. 16, no. 2, pp. 86-93, 2011.

Shijie Yan was born in Shanxi Province, China. He is a Ph.D. candidate in School of Automation and Electrical Engineering in University of Science and Technology Beijing, China. His research interests include cryptography, information security and knowledge security. (Email: yanshijie 0303@sina.com)

Ping Zhen was born in Henan Province, China. He is a Ph.D. candidate in School of Automation and Electrical Engineering in University of Science and Technology Beijing, China. His research interests include chaos-based cryptography and chaos theory. (Email: zhenping1989@126. com)

Lequan Min was born in Beijing, China. He is a professor in School of Mathematics and Physics in University of Science and Technology Beijing, China. His research interests include complex network and chaos theory and application. (Email: minlequan@sina. com)