Information Sciences 181 (2011) 5110–5118

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Security analysis of the public key algorithm based on Chebyshev polynomials over the integer ring Z_N

Fei Chen *, Xiaofeng Liao, Tao Xiang, Hongying Zheng

State Key Laboratory of Power Transmission Equipment and System Security, College of Computer Science, Chongqing University, Chongqing 400044, PR China

ARTICLE INFO

Article history:
Received 30 June 2010
Received in revised form 10 May 2011
Accepted 1 July 2011
Available online 13 July 2011

Keywords:
Public key algorithm
Chaos
Period distribution
Security analysis
Periodic orbit
Dynamical system

ABSTRACT

Recently Kocarev and Tasev [20] proposed to use Chebyshev polynomials over real numbers to design a public key algorithm by employing the semigroup property. Bergamo et al. [4] pointed out that the public key algorithm based on Chebyshev polynomials working on real numbers is not secure and devised an attack which permits to recover the corresponding plaintext from a given ciphertext. Later Kocarev et al. [19] generalized the Chebyshev polynomials from real number fields to finite fields and finite rings to make the public key algorithm more secure and practical. However, we analyzed the period distribution of the sequences generated by the Chebyshev polynomials over finite fields [21]. When the modulus N is prime, we found this algorithm was also not secure and proposed an attack on this algorithm over finite fields. We then proposed some schemes to improve the security. In this paper, we further analyze in detail the period distribution of the sequences generated by Chebyshev polynomials over the integer ring Z_N when N is composite. It turns out that the period distribution is poor if N is not chosen properly and there are many small periods, which are not secure in the sense of cryptology. Based on these findings, we devise an attack on the public key algorithm based on Chebyshev polynomials over the integer ring Z_N. We also propose some suggestions to avoid this attack.

1. Introduction

Since 1976 when Diffie and Hellman published their epoch-making paper "New directions of Cryptology" [9], there have been tremendous efforts to construct public key algorithms. Over the past 30 years, some famous public key algorithms, such as RSA [30], Rabin [29], ElGamal [11] and ECC [26,18], have been proposed, studied and applied extensively. RSA is based on the concept of an exponentiation cipher that employs multiplication to generate the ciphertext. RSA and Rabin algorithms depend on the difficulty of factoring large numbers for their security while the ElGamal cipher [11] developed by ElGamal relies on the difficulty of solving the discrete logarithm problem. In 1985, both Koblitz and Miller in their separate researches suggested the use of elliptic curves in the development of a new type of public key cipher [26,18]. Compared with RSA, systems based on the discrete logarithm over elliptic curves are able to maintain the same security level with shorter key sizes. Hence, elliptic curve cryptography (ECC) seems to be suitable for low computational devices such as smart cards.

In recent years, there are many sparking works using chaos to construct cryptosystems [17,33,5,24,40,1,2,23,16,20,19,41,36,28,12,42], most of which are symmetric algorithms [17,33,5,24,40,1,2,23], but there are also some efforts to design asymmetric algorithms [16,20,34,19] and key agreement protocols [41,42,36,28,12]. It is worthy to note that many chaotic systems are defined over real numbers while traditional cryptography deals with systems mainly defined over finite fields. This

* Corresponding author. Tel.: + 86 23 65125420.
E-mail addresses: chenfeiorange@163.com (F. Chen), xfliao@cqu.edu.cn (X. Liao), xiangtaooo@gmail.com (T. Xiang), zhenghongy@cqu.edu.cn (H. Zheng).

0020-0255/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2011.07.008

yields some immediate consequences. Some ordinary design strategies and standard cryptanalytic methods cannot be applied to cryptosystems based on chaotic systems working over real numbers. Just to exemplify, traditional cryptosystems have secure parameters taking values over a large finite field and hence a brute force attack which simply tries all elements of the field in searching the secret values might be infeasible but possible. But if the range of the parameters of a cryptosystem is a continuous infinite interval, i.e. the parameters are defined over real numbers, an exhaustive search is just impossible. However, at the state of current knowledge, the security of chaos-based cryptosystems defined over real numbers is not well understood both in theory and practice.

In [16], the author presented the first chaotic public key algorithm by employing a one dimensional difference equation, i.e. a quadratic difference equation which is first defined over real numbers and then generalized to finite fields. His system also makes use of ElGamal's scheme to accomplish the encryption process. In particular, a one-dimensional difference equation (i.e. iteration map) is well suitable to be a one-way function. Viewing this, a trapdoor is built by letting the legitimate owner know iteration times of the difference equation. Note that the security of this system depends on the infeasibility of solving discrete logarithm over finite fields. It is exactly the same as ElGamal public key encryption algorithm except adopting another one-way function. However, this algorithm is not useful and practical because for general digital chaotic maps, there are no efficient algorithms to compute the n-th iteration value of the map when n is large such as $n = 2^{160}$.

Another asymmetric algorithm called DDE (distributed dynamical encryption) [34] was proposed which distributes a high dimensional chaotic system between the transmitter and receiver, and characterizes the binary information by different attractors formed in the whole system. The two subsystems are timely and mutually coupled by integrating signals through different functions. The dynamics of the transmitter, including the function which generates the coupling signal to the receiver, are regarded as the public key. However, to improve the security, one has to alter the dynamics of the receiver at the beginning of each transmitted bit and construct the attractors off line. This increases dramatically the computation load for the receiver. The improvement of bit error rate also compromises the security.

In [20], Kocarev and Tasev proposed a public key algorithm based on Chebyshev polynomials over real numbers by replacing the multiplications in conventional algorithms with the iterations of Chebyshev polynomials defined on real numbers. One advantage is that this algorithm enriches the current public key family and opens new research directions in the cryptography field. Another advantage is that the underlying mathematical problem is different with traditional RSA. Here the hard mathematical problem is that given an initial point x_0 and the sth iteration value $T_s(x_0)$, to find the large integer s is difficult, while RSA is based on the integer factorization problem which is also hard. However, more and more sophisticated algorithms have been proposed to solve the problem and the trend is continuing [39]. Moreover, this algorithm can also be used in authentication applications such as in key distribution center (KDC) systems [27]. Chebyshev polynomials are also employed in some key agreement protocols [41,36]. The paper [20] claimed that the proposed algorithm was both secure and practical and could be used both for encryption and digital signature. Unfortunately, this algorithm was quickly analyzed and attacked by Bergamo et al. [4] and others [25,6]. The fundamental defect of this algorithm is that the Chebyshev polynomial of order n has an explicit algebraic expression over real numbers which makes this kind of algorithm vulnerable to some sophisticated attacks.

To avoid this attack, Kocarev et al. improved their algorithm by extending the definition of Chebyshev polynomials to finite fields and finite rings [19]. Obviously in this situation, explicit algebraic expression over real number fields of the Chebyshev polynomial of order n does not help to find n over finite fields (rings) giving an initial value x_0 and a final iteration value $T_n(x_0)$. Furthermore, Kocarev et al. pointed out that the problem of computing n reduces to a DLP (discrete logarithm problem). But this is not always true and it depends on the choice of N as the analysis in [21]. There the authors analyzed the period distribution of sequences generated by Chebyshev polynomials over finite fields when the modulus N is prime. An attack on the public key algorithm was also proposed, followed by an improvement of the algorithm to make it fit for real world applications.

The situation when N is prime has been studied in [21] while its security over the integer ring still remains to be an open problem which is this paper's concern. Here we continue to study the situation when N is composite and investigate the security of the algorithm over the integer ring Z_N. Although the algebraic structures of Z_N are quite different between a prime N and a composite N, it turns out that the period distribution is also not good if the composite N is not chosen properly, the case in which there are many small periods which is not secure from the point of cryptology. Based on these findings, we then propose an attack on the public key algorithm over the integer ring Z_N and give some suggestions to make the public key algorithm more secure and practical.

It is well known that in the study of chaotic maps a central problem is the calculation and classification of periodic orbits. However, the detailed information about these orbits is buried so deep in the structure of a given system that there is no systematic method which can extract it analytically. But general information concerning, for example, their density in phase space and the distribution of their periods, can be partially obtained for Chebyshev polynomials via the approach in this paper. This is another contribution of this paper.

This paper is organized as follows. To make this paper self-contained, Section 2 presents some preliminaries that help to understand our analysis. Some classical recurrence equation theory is also introduced. In Section 3, detailed analysis of the period distribution of the sequences generated by Chebyshev polynomials over the integer ring Z_N is given. Then Section 4 introduces an attack on the public key algorithm based on Chebyshev polynomials according to the analysis of sequences' period distribution and gives some suggestions to avoid this attack. Finally, conclusion and some suggestions for future work are made in Section 5.