Information Sciences 312 (2015) 104–130

Contents lists available at ScienceDirect

Information Sciences

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

Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps

SK Hafizul Islam *

Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani Campus, Rajasthan 333031, India

ARTICLE INFO

Article history:
Received 19 May 2014
Received in revised form 21 October 2014
Accepted 23 March 2015
Available online 28 March 2015

Keywords:
Chaotic map
Smartcard
Password
Hash function
Session key
Key exchange protocol

ABSTRACT

Recently, the theory and application of Chebyshev polynomials have been studied extremely by the cryptographic research community; many symmetric and asymmetric cryptographic protocols have been designed based on extended chaotic maps. In this paper, a computation cost efficient and robust three party password-based authenticated key exchange (ECM-3PAKE) protocol with key confirmation has been designed using extended chaotic maps and smartcard. In this protocol, two users can establish a common session key with the help of a trusted server. The proposed protocol is shown to be provably secure in the random oracle model and formally validated through the simulation of Automated Validation of Internet Security Protocols and Applications (AVISPA) software. The simulation results from different model checkers of AVISPA proved that the protocol can withstand the active and passive attacks. Besides, the informal security analysis gives the evidence of security and functional efficiencies of the protocol. In addition, the comparative analysis illustrates that the protocol performs better than the existing protocols.

1. Introduction

With the rapid development of internet and the growing popularity of internet-based applications, communicating users are extremely keen to perform secure message exchanges over any insecure networks. In order to achieve the confidentiality of the sensitive messages, the secure symmetric key exchange of two users becomes a great challenge to peer-to-peer communications [20,21]. In a key exchange protocol for peer-to-peer environment, a common secret key is computed by two users as a function of random numbers contributed by them [22,23]. However, none of the users can determine that the session key to be a pre-selected value or lies within a set having a small number of elements [24]. The Diffie-Hellman key exchanging protocol is the first and fundamental approach in this direction; however, it was proven to be insecure against the man-in-the-middle attack. Due to the easy memorization of the low-entropy password, Bellovin and Merritt [4] firstly proposed the password-based authenticated key exchange (PAKE) protocol. After that, many PAKE protocols [8,38,39] have been proposed in the literature. In 2009, Deng et al. [13] proposed a three party password-based authenticated key exchange (3PAKE) protocol where two communicating users can establish a secure and common session key between them through a

* Tel.: +91 823348791/8797369160.
E-mail addresses: hafi786@gmail.com, hafizul.ism@gmail.com, hafizul@pilani.bits-pilani.ac.in.

http://dx.doi.org/10.1016/j.ins.2015.03.050
0020-0255/

trusted server over an insecure channel. The intension of this paper is to design an extended chaotic map- and password-based three party authenticated key exchange protocol using smartcard for secure communication over any hostile networks.

1.1. Applications of chaotic maps

Due to the security robustness and computation cost efficiencies of the extended chaotic maps, recently many cryptographic protocols and schemes have been developed. With the m-chaotic systems-based pseudo-random number generator (m-CS PRNG), some public key protocols have been developed in the literature [51,66]. These protocol can be viewed as an analog of Diffie-Hellman key exchange protocol. In these systems, m number of chaotic systems and a set of linear functions are used to established a key exchange mechanism over a public channel. The security of the proposed algorithm is $(NP)^m$, where N, P and m indicates the size of the key, the computational complexity of the linear functions and the number of linear functions respectively. In public key cryptography, many two-party authenticated key exchange protocols [16,18,34,37,40,49,54,61,63,64] have also been introduced based on the chaotic maps. In these protocols, two participants can perform a secret session key computation, that can be used to achieve to data confidentiality between them in subsequent communications. The chaotic maps have also gained importance for image encryption systems [9,42,43,48,52,53,67,68]. For this purpose, a one-time key is computed based on chaotic map and the linear chaotic map is used to compute a pseudo-random key stream sequence, which will be taken as the key of a symmetric stream cipher algorithm. The authors in [50] have discussed an efficient design of pseudo-random bit generator that can generate a random key stream sequence for constructing a stream cipher.

In the literature, many password authentication protocols [17,35,36,41,47,57,58,62] are also devised based on the chaotic maps for establishing the mutual authentication between a remote user and a server. In these systems, after achieving the mutual authentication, both the server and the user compute a common session key that may be used in the future communications for message confidentiality [46]. In symmetric key encryption system, the substitution-box (S-Box) is an important cryptographic permeative, which is used to achieved good confusion property between plaintext and ciphertext. Formally, S-Box is an $n \times n$ nonlinear mapping $f : \{0,1\}^n \to \{0,1\}^n$, where $\{0,1\}^n$ represents the vector spaces of n elements from the Galois field $GF(2)$ [10]. Recently, three-dimensional chaotic maps are also employed to design an efficient and robust S-Box for symmetric cipher [53,55]. In 2011, Jye [32] proposed a two-channel speech encryption technique based on the fractional Lorenz systems. In this design, the fractional chaotic map is used for encryption purpose which must possesses the high nonlinearity. For the encryption/decryption of the speech signal, the key sequences are calculated using fractional Lorenz system. The key sequences are tuple of the form $\langle \alpha, \beta, b, c \rangle$, where $\langle \alpha, \beta \rangle$ represents the fractional derivative orders of the Lorenz system and $\langle b, c \rangle$ represents the system parameters.

In 2010, Wang and Gao [56] proposed a novel secure digital communication system based on discrete chaos synchronization and adaptive chaos synchronization. In their scheme, the compound non-linear function transformation is used that intercalate the secret key and thus, it makes difficult for the adversary to retrieve the message using forecasting method. Recently, the chaotic maps are enormously applied in designing of one-way cryptographic hash function [14,59,60]. Deng et al. [14] design an improved hash algorithm that possesses good diffusion and confusion capability, better collision resistance, extreme sensitivity to message and secret key. In information security applications, digital signature become more and more important primitive. The digital signatures are used to obtain the message integrity and non-repudiation. In 2013, Chain and Kuo [7] proposed a novel signature scheme based on chaotic maps. The security of their digital signature scheme is based on the Chaotic map-based discrete logarithm (CDL) problem. However, the scheme [7] requires high computation costs.

1.2. Studies on earlier ECM-3PAKE protocols

In the following, we discussed many three party password-based authenticated key exchange (ECM-3PAKE) protocols based on extended chaotic map. In 2010, Wang and Zhao [54] proposed an ECM-3PAKE protocol but, Yoon and Jeon [63] showed that their protocol is insecure against the modification attack. In order to solve the problem of Wang and Zhao's protocol [54], Yoon and Jeon [63] proposed an enhanced ECM-3PAKE protocol with the semi-group property of Chebyshev polynomials. They claimed that the protocol [54] is designed to provide low computational costs and to threat the various security attacks. It can be noted that, in Wang and Zhao's protocol [54] and Yoon and Jeon's protocol [63], the server and the users should share long-term secret keys to achieve mutual authentication. However, it is inconvenient that the users should protect the long-term secret keys. According to the discussions made in [11,12,28,29], Yoon and Jeon's protocol [63] is vulnerable to known session specific temporary attack (ephemeral secret leakage (ESL) attack) and strong replay attack.

In 2012, Lai et al. [34] proposed an ECM-3PAKE protocol to overcome the weaknesses of previous designs. Unfortunately, Zhao et al. [64] demonstrated that Lai et al.'s protocol [34] suffers from the privileged-insider attack and off-line password guessing attack. It has been observed that, Lai et al.'s protocol [34] does not have a password change phase and suffers from known session specific temporary attack [28,29] and strong replay attack [11,12]. Besides, the protocol [34] does not verify the legitimacy of the password and the login identity during key exchange phase. As a result, if the user keys a wrong