Commun Nonlinear Sci Numer Simulat 18 (2013) 1433–1440

Contents lists available at SciVerse ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Chaotic maps-based password-authenticated key agreement using smart cards

Cheng Guo [a], Chin-Chen Chang [b,c,*]

[a] School of Software, Dalian University of Technology, Dalian 116620, China
[b] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan
[c] Department of Biomedical Imaging and Radiological Science, Chinese Medical University, Taichung 40402, Taiwan

ARTICLE INFO

Article history:
Received 9 April 2012
Received in revised form 19 August 2012
Accepted 29 September 2012
Available online 17 October 2012

Keywords:
Chaotic map
Authentication
Key agreement
Smart card

ABSTRACT

Password-based authenticated key agreement using smart cards has been widely and intensively researched. Inspired by the semi-group property of Chebyshev maps and key agreement protocols based on chaotic maps, we proposed a novel chaotic maps-based password-authenticated key agreement protocol with smart cards. In our protocol, we avoid modular exponential computing or scalar multiplication on elliptic curve used in traditional authenticated key agreement protocols using smart cards. Our analysis shows that our protocol has comprehensive characteristics and can withstand attacks, including the insider attack, replay attack, and others, satisfying essential security requirements. Performance analysis shows that our protocol can refrain from consuming modular exponential computing and scalar multiplication on an elliptic curve. The computational cost of our protocol compared with related protocols is acceptable.

1. Introduction

With the rapid growth of network technology [1–3] and its growing popularity, user authentication has become increasingly important. The goal of user authentication is to provide the confirmation of two communication entities' true identities in an open network environment. Meanwhile, in the process of identity authentication, two parties also agree with a common session key used to encrypt their communications over an insecure channel. Many password-based authenticated key agreement protocols [4–6] have been proposed in recent years, where a user can achieve the purpose of identity authentication by submitting his/her identity and password to the server.

Currently, smart card-based user authentication schemes [5,7–18] have been widely and intensively researched due to their low computational cost, convenient portability, and cryptographic properties. In 2000, Hwang and Li [7] utilized public-key cryptography to propose a remote user authentication scheme with smart cards. In 2005, Fan et al. [12] proposed a robust remote authentication scheme using smart cards. Their scheme required neither any password table for verification nor clock synchronization between the user and the server. Meanwhile, their scheme can resist a series of attacks. Juang et al. [13] proposed in 2008 a new password-authenticated key agreement protocol based on elliptic curve cryptosystems. Their scheme not only satisfied all the criteria of Fan et al.'s scheme but also provided identity protection and session key agreement, and enhanced efficiency by using elliptic curve cryptosystems. In 2009, Sun et al. [14] proposed an improved scheme to overcome the weakness of Juang et al.'s protocol, including inability of the password-changing operation, the session-key problem, and inefficiency of the double secret keys. In 2010, Li et al. [17] also proposed an anonymous

* Corresponding author. Address: Department of Information Engineering and Computer Science, Feng Chia University, No. 100, Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC. Tel.: +886 4 24517250x3790; fax: +886 4 27066495.
E-mail addresses: guo8016@gmail.com (C. Guo), alan3c@gmail.com (C.-C. Chang).

1007-5704/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cnsns.2012.09.032

password- authenticated key agreement to strengthen the securities of Juang et al.'s protocol by providing initiator untraceability, as well as identity protection property.

With the rapid development of theory and application of chaos, more and more public key cryptosystems [19,20] based on chaos theory have been studied widely. In 2007, Xiao et al. [21] proposed a novel key agreement protocol based on chaotic maps. In their scheme, following the original Diffie-Hellan key agreement protocol, they utilized the semi-group property of Chebyshev chaotic maps to establish a key agreement protocol. In 2008, Xiao et al. [22] used timestamps to improve the security of original chaotic maps-based key agreement protocols.

Since the smart cards usually do not support powerful computation capability, and cryptographic protocols based on chaotic maps are suitable for environments where processing power, storage space, or power consumption is constrained, it is worthwhile to develop chaotic maps-based authentication and key-agreement protocols with smart cards instead of using modular exponential computing or scalar multiplication on elliptic curves.

To the best of our knowledge, no smart card-based password-authenticated protocols utilize chaotic maps to meet the requirement for key agreement in the literature to date. Enlightened by key agreement [21–27] based on Chebyshev chaotic maps, we propose a novel chaotic maps-based password-authenticated key agreement protocol using smart cards that satisfies almost all the benefits of existing authentication protocols with smart cards, including the following characteristics:

(1) The computational cost of the smart card is low;
(2) The server does not need to keep the table containing IDs and passwords of users;
(3) Our protocol can withstand a series of attacks;
(4) The user's identity can be well-protected;
(5) The common session key can be established;
(6) The user has the ability to choose and change his/her password.

The remainder of the paper is organized as follows: In the next section, we introduce some preliminaries. In Section 3, we demonstrate our proposed protocol. Section 4 presents some evaluations including functionality, security, and performance of the proposed protocol. Finally, we present our conclusions in Section 5.

2. Preliminaries

In this section, we briefly introduce Chebyshev chaotic maps [21] and an original key agreement protocol [21] based on Chebyshev chaotic maps, which are the major building blocks of our protocol.

2.1. Definition and properties of Chebyshev chaotic maps

Let n be an integer and let x be a variable with the interval $[-1,1]$. Chebyshev polynomial map T_n: $R \to R$ of degree n is defined using the following recurrent relation:

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

where $n \geqslant 2$, $T_0(x) = 1$, and $T_1(x) = x$.

The first few Chebyshev polynomials are:

$$T_2(x) = 2x^2 - 1,$$
$$T_3(x) = 4x^3 - 3x,$$
$$T_4(x) = 8x^4 - 8x^2 + 1.$$

One of the most important properties is that Chebyshev polynomials are the so-called semi-group property which establishes that

$$T_r(T_s(x)) = T_{r\cdot s}(x). \tag{2}$$

An immediate consequence of this property is that Chebyshev polynomials commute under composition

$$T_r(T_s(x)) = T_s(T_r(x)). \tag{3}$$

In order to enhance the security, Zhang [19] proved that semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$. In our proposed protocol, we utilize the enhanced Chebyshev polynomials:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) (\mathrm{mod} N), \tag{4}$$

where $n \geqslant 2$, $x \in (-\infty, +\infty)$, and N is a large prime number. Obviously,

$$T_{r\cdot s}(x) = T_r(T_s(x)) = T_s(T_r(x)). \tag{5}$$