Journal of Information Hiding and Multimedia Signal Processing ©2013 ISSN 2073-4212
Ubiquitous International Volume **4**, Number **2**, April **2013**

Chaotic Maps-Based Mutual Authentication and Key Agreement using Smart Cards for Wireless Communications

Cheng Guo

School of Software,
Dalian University of Technology, Dalian 116620, China
guo8016@gmail.com

Chin-Chen Chang

Department of Information Engineering and Computer Science
Feng Chia University, Taichung 40724, Taiwan
alan3c@gmail.com
Department of Computer Science and Information Engineering
Asia University, Taichung 41354, Taiwan
alan3c@gmail.com

Chin-Yu Sun

Department of Information Engineering and Computer Science
Feng Chia University, Taichung 40724, Taiwan
sun.chin.yu@gmail.com

Received December, 2012; revised January, 2013

Abstract. *Mobile users can roam into foreign networks and transmit messages to foreign agents, and they can access the services provided by a foreign agent by using their mobile devices. Thus, mobile user authentication and key agreement for wireless communications are becoming more and more important. In recent years, most of the existing user authentication and key-agreement protocols with smart cards for wireless communications utilized modular exponential computing and scalar multiplication on elliptic curves to ensure their security. Inspired by the key-agreement protocols based on chaotic maps, we proposed a novel, chaotic maps-based authentication and key-agreement protocol using smart cards for wireless communications. In our protocol, mobile users and foreign agents can authenticate each other and establish a common session key for further communications. Analysis of the security and functionality of our protocol showed that it can satisfy essential security and functionality requirements. In addition, performance analysis showed that our protocol can refrain from consuming modular exponential operation and scalar multiplication on elliptic curves. The computational cost of the proposed protocol compares favorably with the cost of related protocols.*
Keywords: Chaotic maps, authentication, key agreement, smart cards, wireless communications

1. **Introduction.** The convenience of using the Internet has facilitated communications for those who use the Internet. Thus, the goal of mutual authentication is to help ensure that those who communicate on the Internet know the true identity of those with whom they are communicating. To do so, they must establish a common session key that can be

used to encrypt their communications. Password-based authenticated key-agreement protocols [1, 5, 9, 11] are regarded as one of the simplest and most convenient authentication mechanisms.

Recently, with the rapid development of wireless devices and their increasing popularity, wireless communication has become more and more important. Open access to wireless services for wireless networking has raised a number of security concerns among mobile users and service providers. In wireless networks, a mobile user can obtain the desired service provided by a foreign server by roaming the foreign network and establishing mutual authentication with the corresponding foreign agent. Therefore, mobile user authentication and establishment of session keys for mobile users and foreign agents have become very important security issues for wireless applications.

There has been extensive development of authentication and key-agreement protocols for wireless communications [3, 4, 6-8, 14, 15, 19, 20, 22, 24]. Currently, using a smart card is also a convenient way to provide authentication for mobile users due to the smart cards low computational cost and convenient portability. Authentication and key agreement with smart cards have been deployed extensively for various types of authentication applications, especially for wireless communications in the last decades. In 2004, for example, Zhu and Ma [24] proposed an authentication protocol based on the smart card that provided the user with anonymity for wireless environments. Unfortunately, in 2006, Lee, Hwang, and Liao [6] showed that Zhu and Ma's scheme had several security weaknesses and that it could not achieve mutual authentication. In 2008, Wu, Lee and Tsaur [15] found that Lee et al.'s did not possess the property of perfect backward secrecy. Then, they improved Lee et al.'s. However, Lee, Chang and Lee [7] determined that Wu et al.'s scheme could not provide anonymity as the authors had claimed. In 2011, Xu, Zhu and Feng [19] proposed a new authentication and key-agreement protocol in mobile networks that was immune to various known types of attacks and could achieve user anonymity, key-agreement fairness, and user friendliness. In 2011, He, Ma, Zhang, Chen and Bu [3] developed a strong user authentication scheme with smart cards for wireless communications. Even when the information stored in the smart card is disclosed, their scheme is still secure. In the same year, Yoon, Yoo and Ha [22] proposed a user-friendly authentication scheme that overcame the weaknesses of the previous related scheme and that was efficient.

Based on previous research [3, 6, 7, 15, 19, 22], a smart card-based authentication and key-agreement protocol for wireless communications should satisfy the following essential requirements:

1. Mutual authentication;
2. User friendliness;
3. No password/verification table;
4. Fairness in key agreement;
5. User's identity anonymity;
6. Withstanding the insider attack;
7. Withstanding the smart card-loss case;
8. Withstanding the replay attack;
9. Confidentiality of the session key.

In recent years, cryptography based on chaos theory has been studied extensively, and many chaotic-based cryptosystems [12, 23] have been proposed. In 2007, Xiao, Liao and Deng [16] proposed a novel key-agreement protocol based on chaotic maps. In their scheme, the semi-group property of the Chebyshev chaotic map was used to establish the session key. A chaotic-based, public cryptosystem can reduce computation costs

effectively. In 2008, based on their own protocol, Xiao, Liao and Deng [17] proposed a new, chaotic map-based key-agreement protocol by employing a time-stamp to improve the security of the original protocol. In 2011, Cuo and Zhang [2] proposed a secure, group-key-agreement protocol based on chaotic hash that utilized the chaotic hash function to achieve the contributory nature and enhance security. The interested reader can find more on key-agreement protocols based on chaotic maps in the following references [10, 13, 18, 21].

To the best of our knowledge, no authentication and key-agreement protocols based on chaotic maps for wireless communications have been proposed in the literature to date. In this paper, we proposed a novel, chaotic map-based authentication and key-agreement protocol for wireless communications. Our proposed protocol satisfies all essential functionality requirements, and it also can withstand various known types of attacks. In addition, the computational costs of chaotic map-based protocols are very low compared with other protocols based on modular exponential computing or scalar multiplication on elliptic curves. This feature is more suitable for the low-power and resource-limited mobile devices.

The remainder of the paper is organized as follows. In Section 2, we introduce some preliminary information that provides the building blocks for the proposed protocol. In Section 3, we propose our mutual authentication and key-agreement protocol based on chaotic maps for wireless communications. The security and performance analyses are presented in Sections 4 and 5, respectively. Our conclusions are presented in Section 6.

2. Preliminaries.

In this section, we briefly introduce Chebyshev chaotic maps, which have semi-group and chaotic properties, and a key-agreement protocol based on the Chebyshev chaotic map proposed by Xiao et al. [18] in 2005, 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 that has values over the interval [-1, 1]. The Chebyshev polynomial $T_n(x)$ of degree n is defined as:

$$T_n(x) = \cos(n * \arccos x). \tag{1}$$

The recurrent formulas are defined as follows:

$$\begin{aligned} &T_0(x) = 1, T_1(x) = x, \\ &T_2(x) = 2x^2 - 1, \\ &\cdots \\ &T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x), n \geq 2. \end{aligned} \tag{2}$$

One of the most important properties of the Chebyshev polynomial is the so-called semi-group property, which establishes that:

$$\begin{aligned} T_r(T_s(x)) &= \cos(r * \arccos(\cos(s * \arccos x))) \\ &= \cos(rs * \arccos(x)) = T_{sr}(x) = T_s(T_r(x)). \end{aligned} \tag{3}$$

2.2. Chebyshev chaotic maps-based key-agreement protocol.

The basic key-agreement protocol [18] based on the Chebyshev chaotic map is similar to the Diffie-Hellman key-agreement protocol. A session key can be established between the two communication entities, A and B.

1. A and B jointly choose a random number $x \in [-1, 1]$, and x does not require secrecy.
2. A chooses a random large integer r, computes $X = T_r(x)$, and sends X to B.
3. B chooses a random, large integer s, computes $Y = T_s(x)$, and sends Y to A.

4. A can compute the secret key $k = T_r(Y) = T_r(T_s(x))$, and B can compute the secret key $k' = T_s(X) = T_s(T_r(x))$.

Due to the semi-group property, $k = k' = T_{rs}(x)$, A and B can achieve the common secret session key used to encrypt the communications between them. However, the above key-agreement protocol is simple and has some security problems; it is especially vulnerable to the man-in-the-middle attack.

3. **The proposed protocol.** In this section, we propose a chaotic maps-based mutual authentication and key-agreement protocol for wireless communications using smart cards that almost satisfies all the requirements of the existing authentication and key-agreement protocols for wireless communications and is immune to various known types of attacks. In addition, our protocol is simple and has a reasonable cost.

The notations used in this section are listed in Table 1. Our protocol consists of three phases, i.e., (1) the registration phase; (2) the mutual authentication and session key-agreement phase; and (3) the password change phase.

TABLE 1. Notations used in the proposed protocol

Notations	Descriptions
MU	A mobile user
HA	Home agent of a mobile user
FA	Foreign agent of the network visited by the user
pw	The password
ID_X	The identity of an entity X
$h(\cdot)$	A one-way hash function
T_X	Time stamp by an entity X
$\|\|$	String concatenation operation
$E_K(\cdot)$	Symmetric encryption of a message using key K
$T_n(x)$	The Chebyshev polynomial of degree n

3.1. **Registration phase.** In this phase, the home agent (HA) must choose a public key cryptosystem based on the Chebyshev chaotic map; the corresponding public key is $(x; T_s(x))$, and his private key is s. When a mobile user (MU) wants to register to the home agent HA, MU chooses her or his identity ID_{MU} and password pw, selects a random number b, and submits ID_{MU} and $h(pw||b)$ to HA for registration over a secure channel. HA computes $V = E_{KS}(ID_{MU}||h(pw||b))$, where KS is a secret key kept by HA, and issues a smart card to MU over a secure channel, which contains V, x, $T_s(x)$, $E_K(\cdot)$ and a one-way hash function $h(\cdot)$. When MU receives the smart card, he or she

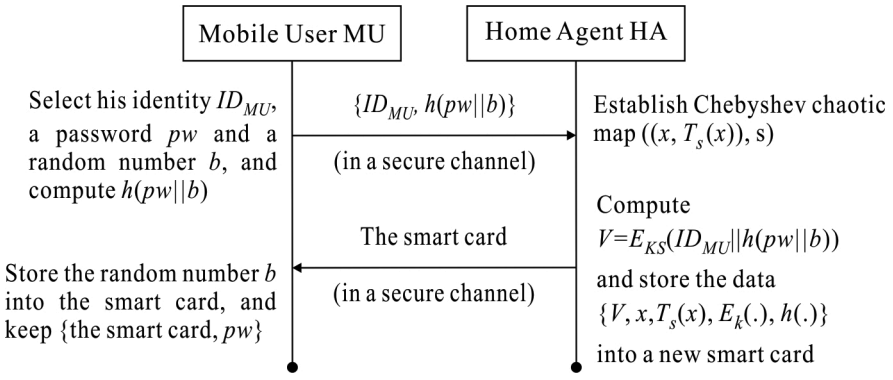

FIGURE 1. The registration phase of the proposed protocol

stores b into the smart card. Finally, the smart card contains $\{b, V, x, T_s(x), E_K(\cdot), h(\cdot)\}$. This phase is outlined in Fig. 1.

3.2. **Mutual authentication and session key agreement phase.** When MU visits a new foreign network, if he or she wants to access several services or establish a session with the foreign agent (FA), MU and FA must perform mutual authentication and agree on a session key. Similar to Xu et al.'s protocol [19], HA pre-shares a distinct symmetric key K_{HF} with each FA. As is shown in Fig. 2, the following steps are performed in this phase.

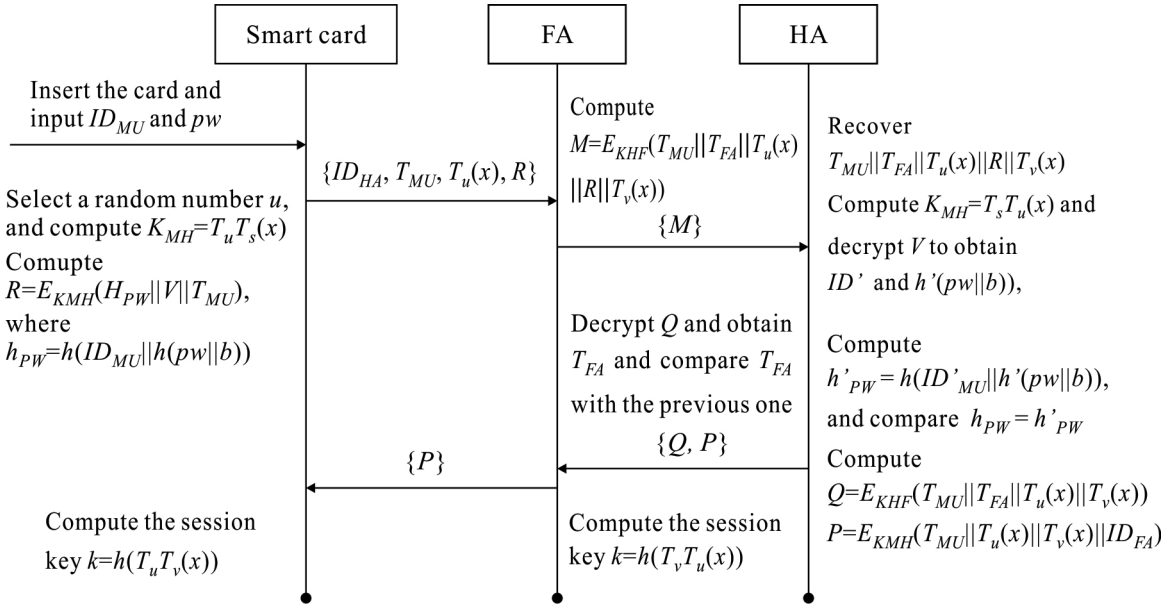

FIGURE 2. The authentication and key agreement phasse of the proposed protocol

Step1. MU inserts her or his smart card into a card reader and inputs her or his identity ID_{MU} and password pw. Then, the device selects a random number u and computes $K_{MH} = T_uT_s(x)$, and $R = E_{K_{MH}}(h_{pw}||V||T_{MU})$, where $h_{pw} = h(ID_{MU}||h(pw||b))$, and T_{MU} is the current timestamp.

Step2. MU sends an authentication request message $m_1 = \{ID_{HA}, T_{MU}, T_u(x), R\}$ to FA.

Step3. FA checks to determine whether the T_{MU} is valid. If it is valid, FA selects a random number v and computes $T_v(x)$. Then, FA computes $M = E_{K_{HF}}(T_{MU}||T_{FA}||T_u(x)||R||T_v(x))$, where T_{FA} is the current timestamp, and sends the message $m_2 = \{M\}$ to HA.

Step4. HA decrypts M with K_{HF} to recover $T_{MU}||T_{FA}||T_u(x)||R||T_v(x)$. First, HA checks the timestamp T_{FA} with the current time. If the timestamp is valid, HA computes $K_{MH} = T_sT_u(x)$ with her or his private key s. Then, HA decrypts R with K_{MH} to recover h_{PW}, V , and T_{MU}. HA checks whether the T_{MU} is equal to the previous one that was decrypted from M. If they are identical, HA decrypts V by using his secret key KS to obtain ID'_{MU} and $h'(pw||b)$. Finally, HA computes $h'_{PW} = h(ID'_{MU}||h'(pw||b))$ and compares the computed value of h'_{PW} with the recovered value of h_{PW}. If they are equal, HA can be sure that MU is an authorized user.

Step5. HA computes $Q = E_{K_{HF}}(T_{MU}||T_{FA}||T_u(x)||T_v(x))$ and $P = E_{K_{MH}}(T_{MU}||T_u(x)||T_v(x)||ID_{FA})$ and sends the message $m_3 = \{Q, P\}$ to FA.

Step6. FA decrypts Q with K_{HF} to obtain T_{MU}, T_{FA}, $T_u(x)$ and $T_v(u)$. If the recovered T_{FA} is equal to the original choice, FA confirms that MU is authenticated by HA. Then, FA forwards P to MU.

Step7. MU decrypts P to recover T_{MU}, $T_u(x)$, $T_v(x)$ and ID_{FA}. If the recovered T_{MU} is equal to the previous one and ID_{FA} is the assigned foreign agent, MU believes that message P is from HA, and FA is authenticated.

Step8. Finally, MU and FA compute their common session key $k = h(T_uT_v(x)) = h(T_vT_u(x))$.

3.3. **Password change phase.** In case of changing her or his password, MU inserts her or his smart card into a card reader and performs the following steps:

Step1. MU inputs her or his identity ID'_{MU} and her or his old password pw' and requests to change the password. Then, MU submits her or his new password $pw*$.

Step2. The smart card selects a random number u' and computes the $\tilde{V} = E_{\tilde{K}_{MH}}(ID'_{MU} ||h(pw'||b))$, where $\tilde{K}_{MH} = T_{u'}T_s(x)$. Then, the device sends u', V , and $\tilde{V}$ to the corresponding HA.

Step3. HA computes the session key $\tilde{K}_{MH} = T_sT_{u'}(x)$, and decrypts $\tilde{V}$ to obtain ID'_{MU} and $h(pw'||b)$. Then, HA compares whether $V = E_{KS}(ID'_{MU}||h(pw'||b))$. If the equation holds, HA computes $V^* = E_{KS}(ID_{MU}||h(pw^*||b))$ and replaces V with V^*.

4. **Security and functionality analysis.** In this section, we analyze the security and functionality of the proposed protocol to verify whether the essential security and functionality requirements mentioned in Section 1 have been satisfied. In order to examine the proposed protocol further, we compared it with the other related protocols [3, 6, 19] in Table 2.

(1) Mutual authentication

In the proposed protocol, the goal of mutual authentication was to ensure that MU and HA are legitimate and to establish an agreed-upon session key between MU and FA for further communications.

1. Mutual authentication between MU and HA:
   In Step 4 of the mutual authentication and session key-agreement phase, because $K_{MH} = T_sT_u(x)$, only HA can compute this secret key K_{MH} with her or his private key s. HA can decrypt R with K_{MH} to recover h_{PW}, V and T_{MU}. Then, HA can decrypt V by using her or his secret key KS to obtain ID'_{MU} and $h'(pw||b)$. HA can compare whether $h'_{PW} = h(ID'_{MU}||h'(pw||b))$ is equal to h_{PW}. If they are equal, HA can be sure that MU is an authorized user.

   Meanwhile, in Step 7 of the same phase, upon receiving the message P from FA, MU can decrypt it using her or his secret key K_{MH} and obtain T_{MU}. If the recovered T_{MU} is equal to the previous one, MU believes that the message P is from HA since only HA has the secret key K_{MH}.
2. Mutual authentication between FA and HA:
   In Step 3 of the mutual authentication and session key-agreement phase, FA computes $M = E_{K_{HF}}(T_{MU}||T_{FA}||T_u(x)||R||T_u(x))$ using a distinct symmetric key K_{HF} , which is shared between FA and HA. In Step 4 of the same phase, if HA can decrypt M with K_{MH}, he or she can ensure that the message is from FA. In Step 6 of the same phase, for the same reason, if FA can decrypt Q with the K_{HF} , he or she can ensure that the message Q is from HA.
3. Mutual authentication between MU and FA:
   In Step 6 of the mutual authentication and session key-agreement phase, FA can ensure that MU is authenticated by HA. Therefore, FA believes that MU is a

legitimate user and forwards P to MU. In Step 7 of the same phase, since the message P is from HA and encrypted with the key K_{HF} , MU can decrypt the message and recover T_{MU} and ID_{FA}. If these messages are equal to the previous one, MU can be sure that FA is legitimate.

(2) User friendliness

User friendliness means that the mobile user MU can choose and update her or his password freely. In our protocol, MU can choose her or his identity ID_{MU} and password pw freely and submit ID_{MU} and $h(pw||b)$ to HA for registration. When MU wants to change her or his password pw to a new pw', he or she can perform the steps stated in Section 3.3. Therefore, the proposed protocol allows mobile users to choose their passwords and to change their passwords freely.

(3) No password/verification table

In the registration phase, MU submits her or his identity and password to HA for registration. In some password-based authentication protocols, HA must store a password table or a registration table for every mobile user who wishes to be verified. That is, HA must maintain a secret and large table, which provides the opportunity for an inside attacker to access the password or the registration information. In our protocol, HA computes $V = E_{KS}(ID_{MU}||h(pw||b))$ and stores V into the smart card. V contains the identity of the mobile user and the corresponding password. In the authentication phase, FA can determine whether the mobile user is legitimate with the assistance of HA and the information V. Therefore, HA does not need to keep a password table or a verification table at her or his local site.

(4) Fairness in key agreement

Fairness in key agreement means that a session key contains equal contributions from both parties.

1. MU selects a random number u and sends to FA.
2. FA also selects a random number v and encrypts $T_u(x)$ and $T_v(x)$ using the session key between FA and HA and sends this message to HA.
3. HA retrieves $T_u(x)$ and $T_v(x)$ and encrypts them using the session key between HA and MU. Then, he or she sends this message to FA, and FA forwards this message to MU.
4. Finally, both MU and FA can compute the agree-upon session key $k = h(T_uT_v(x))$.

(5) Anonymity of the user's identity

In the authentication and key-agreement phase, the real identity of the mobile user should be unknown to any other entity except his or her HA. Furthermore, our protocol provides identity untraceability and identity anonymity.

In our protocol, the anonymity of the mobile user is ensured by symmetric encryption and hash function techniques. This can be analyzed from the following aspects:

1. ID_{MU} is hidden in $V = E_{KS}(ID_{MU}||h(pw||b))$, where KS is a secret key kept by HA. Therefore, only HA has the capability to retrieve the identity ID_{MU} from V. Even if the message V were revealed, an attacker could not obtain the identity message of the MU.
2. In the authentication and key-agreement phase, ID_{MU} also is hidden in $R = E_{K_{MH}}($ $h_{pw}||V||T_{MU})$, where $h_{PW} = h(ID_{MU}||h(ID_{MU}||h(pw||b)))$ and $K_{MH} = T_uT_v(x)$, which is the session key between the MU and the HA. So, no third party can retrieve the identity ID_{MU} from R.
3. Identity untraceability is a stronger characteristic than identity anonymity, and it requires that any attacker not be able to link one MU interacting with an FA to another transcript. That is, any attacker cannot determine which foreign agents the

same MU visited. In the authentication phase, the device utilizes a different session key $K_{MH} = T_u T_s(x)$ each time, where u is a random number selected by the device. Therefore, the messages communicated between MU and FA are different each time. Consequently, any attacker cannot determine whether the same MU visited this FA.

(6) Withstanding the insider attack

The insider attack is when the mobile user's password is obtained by an inside attacker on the server side of the registration phase. In the registration phase, the device selects a random number b and computes $h(pw||b)$. Then, the device sends this message to HA for registration. In this phase, HA cannot obtain the password of the MU. Furthermore, HA does not need to store the password table and the verification table in her or his local server. So, an inside attacker has no opportunity to access any information about the MU's password.

(7) Withstanding the smart card-loss case

In this case, we assume that the attacker can obtain the secret information stored in the smart card by some means. In order to withstand this attack, we need to ensure that the attacker cannot obtain the right password even if he or she obtains the secret information stored in the smart card.

In the proposed protocol, the password stored in the smart card with a random number b and ID_{MU} included in $V = E_{KS}(ID_{MU}||h(pw||b))$ is encrypted by a secret key KS. Only HA can use the secret key KS to decrypt V and obtain ID_{MU} and $h(pw||b)$. Since no attacker can obtain ID_{MU} and the hashed password, he or she cannot compute the verification information $R = E_{K_{MH}}(h_{PW}||V||T_{MU})$.

In our protocol, the identity and password of the MU must report to the help of the corresponding home agent HA. That is only the corresponding HA has a capabitily to obtain the MU's identity and $h(pw||b)$ by decrypting V using the secret key KS. Therefore, when the information stored in the smart card is compromised, no attacker can guess the right identity and his or her password.

(8) Withstanding the replay attack

A replay attack refers to the process in which an adversary intercepts the login messages between the user and the server and replays these messages to the server maliciously aimed at impersonating this user.

In Step 1 of the authentication phase, the smart card selects a current time T_{MU} as a timestamp and encrypts some messages including this timestamp using a session key K_{MH} between MU and FA. Upon receiving these messages from MU, FA can obtain the timestamp and check whether the T_{MU} is valid. Using the same method, HA also can obtain the timestamp T_{FA} from FA and determine whether the delay is within an acceptable range by checking T_{FA} and the current time.

(9) Confidentiality of the session key

In the authentication and key-agreement protocol, MU and FA must prove each other's identity and establish a secret session key for further communications. Therefore, the session key must be confidential. However, in [6, 9, 10], the HA also has the capability of calculating the session key. In the proposed protocol, we have improved this issue. In our protocol, the session key is $k = h(T_u T_v(x)) = h(T_v T_u(x))$, where u and v are the secret numbers of MU and FA, respectively. HA cannot obtain these two secret numbers. So, MU and FA are the only two entities who can compute this session key.

Finally, we summarize the security and the functionality of our protocol and make comparisons with these aspects of related works [3, 6, 19] in Table 2.

5. **Performance analysis.** In wireless communication environments, battery-powered mobile devices have limited energy resources and computing capability. Therefore, the

computation cost is a very important issue. In this section, we analyze the performance of the proposed protocol and compare our protocol with related works [3, 6, 19] in terms of cryptographic operations performed.

Compared with the traditional mutual authentication and key agreement protocols [3, 6, 19] for wireless communications, our proposed protocol utilizes the property of Chebyshev chaotic maps to achieve mutual authentication and establish the session key instead of using modular exponential computing and scalar multiplication on elliptic curves. In reference [13], some software implementation issues of Chebyshev chaotic maps were discussed. The authors established a table that they used to store the most commonlyused expression of Chebyshev polynomials of different degrees. Therefore, the practical application of the proposed protocol is more efficient than that of the traditional protocols [3, 6, 19].

The computational costs of MU, FA, and HA for the proposed protocol and the related protocols [3, 6, 19] are presented in Table 3.

TABLE 2. Security and functionality comparisons between the related protocols and the proposed protocol

	Our protocol	He et al.'s protocol[3]	Xu et al.'s protocol[19]	Lee et al.'s protocol[6]
S1	YES	YES	YES	YES
S2	YES	YES	YES	NO
S3	YES	YES	YES	YES
S4	YES	NO	YES	YES
S5	YES	NO	YES	NO
S6	YES	YES	NO	NO
S7	YES	YES	YES	YES
S8	YES	YES	YES	YES
S9	YES	NO	NO	NO

S1: Mutual authentication; S2: User friendliness; S3: No password/verification table; S4: Fairness in key agreement; S5: Users identity anonymity; S6: Withstanding the insider attack; S7: Withstanding the smart card-loss case; S8: Withstanding the replay attack; S9: Confidentiality of the session key.

TABLE 3. Performance comparisons between the related protocols and the proposed protocol

Primitives		Our protocol	He et al.'s protocol[3]	Xu et al.'s protocol[19]	Lee et al.'s protocol[6]
H	MU	3	10	1	2
	FA	1	5	N/A	N/A
	HA	1	5	N/A	3
E	MU	N/A	N/A	2	N/A
	FA	N/A	N/A	N/A	N/A
	HA	N/A	N/A	1	N/A
S	MU	1	2	3	2
	FA	2	1	2	1
	HA	4	2	6	1
M	MU	N/A	N/A	N/A	N/A
	FA	N/A	3	N/A	N/A
	HA	N/A	3	N/A	N/A
T	MU	$3u + s$	N/A	N/A	N/A
	FA	$2v$	N/A	N/A	N/A
	HA	$2s$	N/A	N/A	N/A

H: hash operation; E: modulus exponential operation; S: symmetric encryption or decryption; M: scalar multiplication on elliptic curve; T: Chebyshev maps

6. **Conclusions.** In this paper, we proposed a novel, chaotic map-based, mutual authentication and key-agreement protocol for wireless communications. We utilized Chebyshev chaotic maps to achieve mutual authentication and to establish a common session key between MU and FA instead of using modular, exponential computing and scalar multiplication on elliptic curves. The security and functionality analysis showed that our proposed protocol satisfies all essential functionality requirements and also can withstand various known types of attacks. In addition, the performance analysis demonstrated that the computational costs of chaotic map-based protocols are very low compared with other protocols that are based on modular exponential computing or scalar multiplication on elliptic curves. This feature makes our protocol more suitable for use with low-power and resource-limited mobile devices.

REFERENCES

[1] C. I. Fan, Y. C. Chan, and Z. K. Zhang, Robust remote authentication scheme with smart cards, *Journal of Computers & Security*, vol. 42, no. 8, pp. 619-628, 2005.

[2] X. F. Guo, and J. S. Zhang, Secure group key agreement protocol based on chaotic hash, *Journal of Information Sciences*, vol. 180, no. 20, pp. 4069-4074, 2010.

[3] D. J. He, M. D. Ma, Y. Zhang, C. Chen, and J. J. Bu, A strong user authentication scheme with smart cards for wireless communications, *Journal of Computer Communications*, vol. 34, no. 3, pp. 367-374, 2011.

[4] M. S. Hwang, S. K. Chong, and T. Y. Chen, DoS resistant ID-based password authentication scheme using smart cards, *Journal of Systems and Software*, vol. 83, no. 1, pp. 163-172, 2010.

[5] W. S. Juang, S. T. Chen, and H. T. Liaw, Robust and efficient password-authenticated key agreement using smart card, *IEEE Trans. Industrial Electronics*, vol. 55, no. 6, pp. 2551-2556, 2008.

[6] C. C. Lee, M. S. Hwang, and I. E. Liao, Security enhancement on a new authentication scheme with anonymity for wireless environments, *IEEE Trans. Industrial Electronics*, vol. 53, no. 5, pp. 1683-1686, 2006.

[7] J. S. Lee, J. H. Chang, and D. H. Lee, Security flaw of authentication scheme with anonymity for wireless communications, *Journal of IEEE Communications Letters*, vol. 13, no. 5, pp. 292-293, 2009.

[8] C. T. Li and C. C. Lee, A novel user authentication and privacy preserving scheme with smart cards for wireless communications, *Journal of Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 35-44, 2012.

[9] X. X. Li, W. D. Qiu, D. Zheng, K. F. Chen, and J. H. Li, Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards, *IEEE Trans. Industrial Electronics*, vol. 57, no. 2, pp. 793-800, 2010.

[10] Y. J. Niu, and X. Y. Wang, An anonymous key agreement protocol based on chaotic maps, *Journal of Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 4, pp. 1986-1992, 2011.

[11] D. Z. Sun, J. P. Huai, J. Z. Sun, J. X. Li, J. W. Zhang, and Z. Y. Feng, Improvements of Juang et al.'s password-authenticated key agreement scheme using smart cards, *IEEE Trans. Industrial Electronics*, vol. 56, no. 6, pp. 2284-2291, 2009.

[12] K. Wang, W. J. Pei, L. H. Zou, Y. M. Cheung, and Z. Y. HE, Security of public key encryption technique based on multiple chaotic system, *Journal of Physics Letters A*, vol. 360, no. 2, pp. 259-262, 2006.

[13] X. Y. Wang, and J. F. Zhao, An improved key agreement protocol based on chaos, *Journal of Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 4052-4057, 2010.

[14] F. T. Wen, and X. L. Li, An improved dynamic ID-based remote user authentication with key agreement scheme, *Journal of Computers and Electrical Engineering*, vol. 38 no. 2, pp. 381-387, 2012.

[15] C. C. Wu, W. B. Lee, and W. J. Tsaur, A secure authentication scheme with anonymity for wireless communications, *Journal of IEEE Communications Letters*, vol. 12, no. 10, pp. 722-723, 2008.

[16] D. Xiao, X. F. Liao, and S. J. Deng, A novel key agreement protocol based on chaotic maps, *Journal of Information Sciences*, vol. 177, no. 4, pp. 1136-1142, 2007.

[17] D. Xiao, X. F. Liao, and S. J. Deng, Using time-stamp to improve the security of a chaotic maps-based key agreement protocol, *Journal of Information Sciences*, vol. 178, no. 6, pp. 1598-1602, 2008.

[18] D. Xiao, X. F. Liao, and K. W. Wong, An efficient entire chaos-based scheme for deniable authentication, *Journal of Chaos, Solitons & Fractals*, vol. 23, no. 4, pp. 1327-1331, 2005.

[19] J. Xu, W. T. Zhu, and D. G. Feng, An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks, *Journal of Computer Communications*, vol. 34, no. 3, pp. 319-325, 2011.

[20] K. H. Yeh, C. H. Su, N. W. Lo, Y. J. Li, and Y. X. Hung, Two robust remote user authentication protocols using smart cards, *Journal of Systems and Software*, vol. 83, no. 12, pp. 2556-2565, 2010.

[21] E. J. Yoon, and II. S. Jeon, An efficient and secure Diffie-Hellman key agreement protocol based on Chebyshev chaotic map, *Journal of Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 6, pp. 2383-2389, 2011.

[22] E. J. Yoon, K. Y. Yoo, and K. S. Ha, A user friendly authentication scheme with anonymity for wireless communications, *Journal of Computers and Electrical Engineering*, vol. 37, no. 3, pp. 356-364, 2011.

[23] L. H. Zhang, Cryptanalysis of the public key encryption based on multiple chaotic systems, *Journal of Chaos, Solitons & Fractals*, vol. 37, no. 3, pp. 669-674, 2008.

[24] J. M. Zhu, and J. F. Ma, A new authentication scheme with anonymity for wireless environments, *IEEE Trans. Consumer Electronics*, vol. 50, no. 1, pp. 231-235, 2004.