Password Authenticated Key Exchange Protocol for Multi-Server Mobile Networks Based on Chebyshev Chaotic Map

Chien-Lung Hsu
Information Management
Chang-Gung University
Tao-Yuan, Taiwan (R.O.C.)
clhsu@mail.cgu.edu.tw

Tzu-Wei Lin
Information Management
Chang-Gung University
Tao-Yuan, Taiwan (R.O.C.)
elliot.lin49@gmail.com

***Abstract*—In a single-server mobile network, authorized users can dynamically login to the server for requiring internet services or resources. A password authenticated key exchange protocol can be used to authenticate user's legitimacy and establish a secure communication between a user and his logon server by using his friendly memorized password. In generally, users can dynamically access internet resources and services from multiple servers via mobile networks. However, it is difficult for users and servers to easily and securely manage passwords and secret keys in multi-server mobile networks. This paper proposes a password authenticated key exchange protocol for multi-server mobile networks based on Chebyshev chaotic map. Properties of the proposed protocol are given below. (i) The user can easily memorize a single password to login different servers without the assistance of a trusted registration authority. (ii) The user can share distinct secret information with different servers, and hence a malicious server cannot use it to masquerade as the user to login the other server(s). (iii) It is secure against some potential attacks. (iv) An authenticated key shared between the user and the server can be established for securing their communications. (v) It can provide key confirmation for the shared session key. (vi) It can provide higher security assurance in generating secret keys.**

Keywords-multi-server; mobile network; cryptography; authenticate; password; Chebyshev chaotic map

I. INTRODUCTION

The Internet environment has become a single society in which all of the services required for daily living are implemented online nowadays [5]. The more mobile communication technology is being developed, the more people can take services they want through mobile devices whenever and wherever they are [8]. For such reasons, a user might register to several remote servers for requesting different services. In a mobile network, all messages are transmitted over the air and it might be suffered from some potential attacks, such as interception, masquerade, compromising attacks, etc. A password-based authenticated key exchange protocol can be used to provide the security assurance for mobile networks. It allows the user to login to server by using his memorized password and establish a secret key shared among them for securing subsequent communications. Multi-server mobile network has a fantastic property called mobility which means users can pass through multiple access points while maintaining progressional connections. This kind of network can provide users more diversified services. Namely, a user can login different servers through mobile network to obtain diversified services. If utilizing traditional password-based authenticated key exchange protocol to ensure security of multi-server wireless mobile network, we might face some problems: (1) A user has to manage more than one pairs of identifiers and passwords which might increase user's load and risk of managing passwords. (2) In general cases, if user utilizes one single password to login different servers, we will need a registration center (RC) which must be trusted. In 2008, Tsai proposed a multi-server authentication protocol based on one-way hash function without verification table [10]. The user and server have both to authenticate with registration center before verifying each other. There are many protocols that utilize the similar methods for the past several years [2, 4, 6, 11, 12]. (3) A malicious server might masquerade as the user to login the other server(s). (4) The cost of logging in and establishing session key, such as computational complexity, storage, rounds, etc., is related to number of servers. In other words, the cost of our protocol is not related to how many servers there are.

For guaranteeing the security and confidentiality of subsequent transmission, a shared session key will be established after authenticated key exchange protocol. In 2012, Hsu et al. proposed a password-based authenticated key exchange protocol [3] with smart card, and the protocol has properties below: (1) It can be applied in the multi-servers architecture. (2) It can avoid attacks from malicious person in the registration center. (3) It can transfer information publically. (4) It can apply smart card. We will point out the vulnerabilities of Hsu et al.'s protocol [3] and demonstrate three kinds of attacks.

A chaotic system is characterized by sensitive dependence on initial conditions, pseudo-randomness and ergodicity. These features have excellent properties of diffusion and confusion which are important to cryptography, especially secret key cryptosystems [14]. In 2003, Kocarev et al. proposed a public key encryption protocol based on Chebyshev chaotic maps [7]. Because of the mathematical properties and characterizes of Chebyshev chaotic maps, it is more secure to utilize Chebyshev chaotic maps in public-key cryptosystems. Wang et al. have implemented it, and experimental results and performance analyses had been proved that it is secure and practical [13]. In 2005, Bergamo et al. [1] pointed out that Kocarev et al.'s protocol [7] is not secure because the adversary can recover the plaintext from

978-1-4244-9529-0/13/$31.00 ©2013 IEEE

given ciphertext without any private key based on the periodicity of cosine function. In 2010, Wang et al. pointed out that some key agreement protocols based on chaos have several drawbacks as follows [13]: (1) Some protocols are vulnerable to Bergamo et al.'s proposed attack [1] because the periodicity of the cosine function makes public encryption. (2) Some protocols cannot resist man-in-the-middle attack or replay attack. (3) Some protocols did not provide mutual authentication of both communication sides. (4) Clock synchronization is difficult to achieve in some cases. (5) Because of sharing secret key between every two parties, it becomes difficult to distribute keys.

In this paper, we propose an authenticated key exchange protocol for multi-server mobile networks based on Chebyshev chaotic map not only solving problems above but remaining some general properties, such as mutual authentication, session key establishment, no verification table, etc. We sketch the remaining organization of this paper below. In section II, we briefly review Hsu et al.'s protocol [3]; we demonstrate three kinds of attack in section III; we introduce our protocol in section IV; some security analyses are detailed in section V; finally, a conclusion is made in section VI.

II. REVIEW OF HSU ET AL.'S PROTOCOL

Hsu et al.'s protocol [3] is divided into four phases: the system initialization, the user registration, the authenticated key exchange and password changing phase. Some used notations are defined as Table 1.

TABLE I. NOTATIONS OF HSU ET AL.'S PROTOCOL

Notations	Description
ID_{U_i}	User U_i's identity
ID_{S_j}	Remote server S_j's identity
$\oplus$	Exclusive OR (XOR) operation
$H(\cdot)$	Collision-resistant one-way hash function
PW_i	User U_i's password
X_j	Remote server S_j's secret
k	Encryption/decryption key k
$E_k(\cdot)$	Symmetric encryption algorithm with key k
$D_k(\cdot)$	Symmetric decryption algorithm with key k
r	Random number
g, p, q	Parameters of Digital Signature Algorithm (DSA)
T	Timestamp
USB	Portable USB device

In the system initialization phase, each user sets up his smart card by entering identifier and password into it. Let remote servers generate the following parameters according to the Digital Signature Algorithm (DSA) [9]: p and q are two large primes satisfying that $q|(p-1)$; g is a generator of order q over GF(p). Figures 1, 2, and 3 illustrate these phases. Figure 1 illustrates the registration phase. Figure 2 illustrates the authenticated key exchange phase. User and server verify each other and establish session key in this phase. Figure 3 is password changing phase which can let user update the password of smart card.

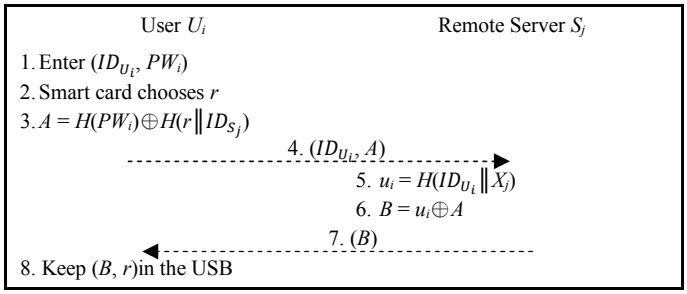


Figure 1. Registration phase of Hsu et al's [3] protocol

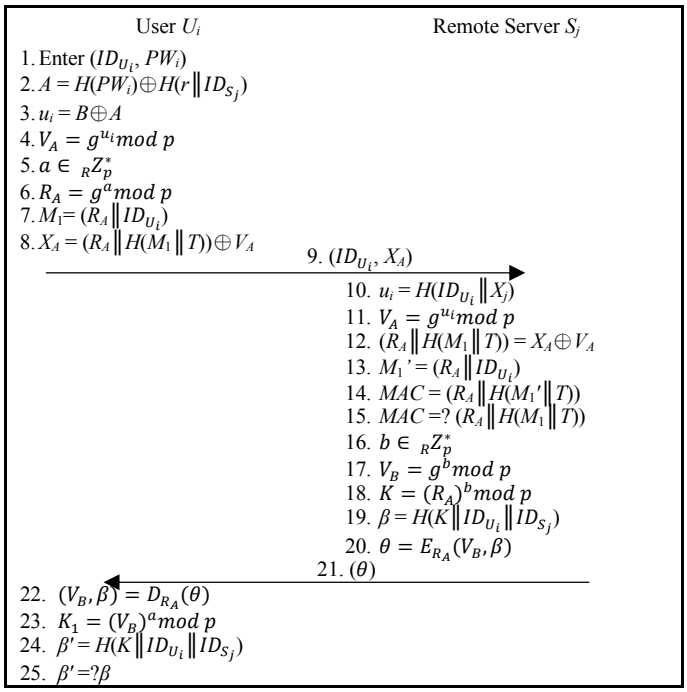


Figure 2. Authenticated key exchange phase of Hsu et al's [3] protocol

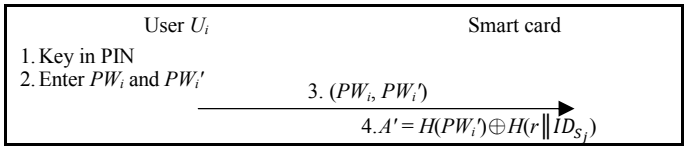


Figure 3. Password changing phase of Hsu et al's [3] protocol

III. THE PROPOSED ATTACKS ON HSU ET AL.'S PROTOCOL

Recall that the random number r of user and B server calculated are stored in portable USB device. If user loses the USB and the adversary gets it, the adversary might obtain B and r. If the password that the adversary guesses is match to user's, the adversary can compute user's $A = H(PW_i) \oplus H(r \| ID_{S_j})$. Because $B = u_i \oplus A = H(ID_{U_i} \| X_j) \oplus H(PW_i) \oplus H(r \| ID_{S_j})$, we can obtain u_i from $u_i = B \oplus A$. The adversary can use u_i in the authenticated key exchange phase for online user impersonating, online server spoofing, and offline user impersonating attack. There are the details for the attacks below.

A. Online User Impersonating

If the adversary has the USB of legitimate user and obtains B and r, the adversary can guess a password PW^*_i, compute u_i and the message with the same method, and send it to server. If the server verifies MAC successfully, server will use the adversary's message to establish session key and send it to the adversary for authenticating without knowing the user has been impersonated. There is the detail below.

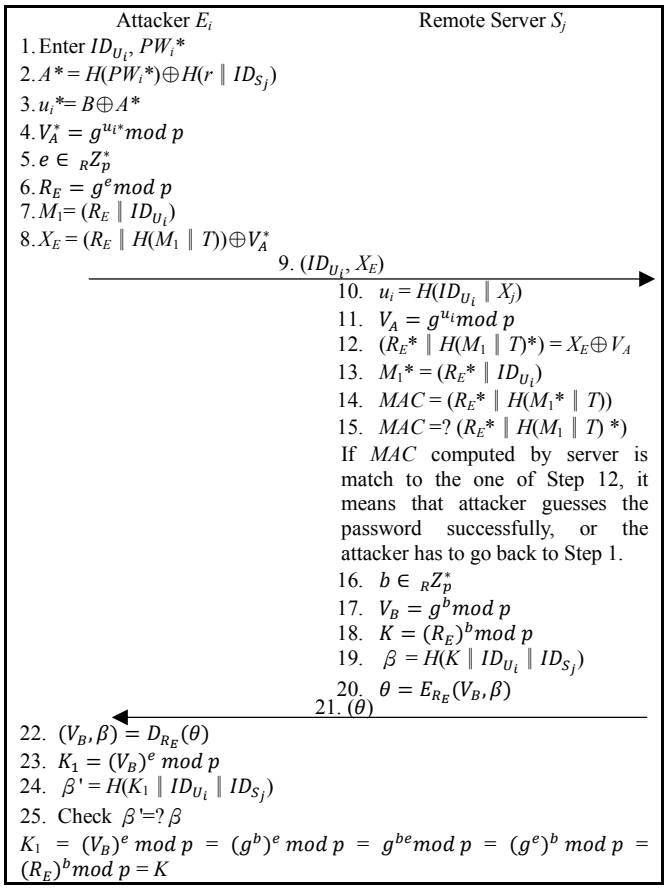


Figure 4. Online user impersonating attack at authenticated key exchange phase of Hsu et al's protocol [3]

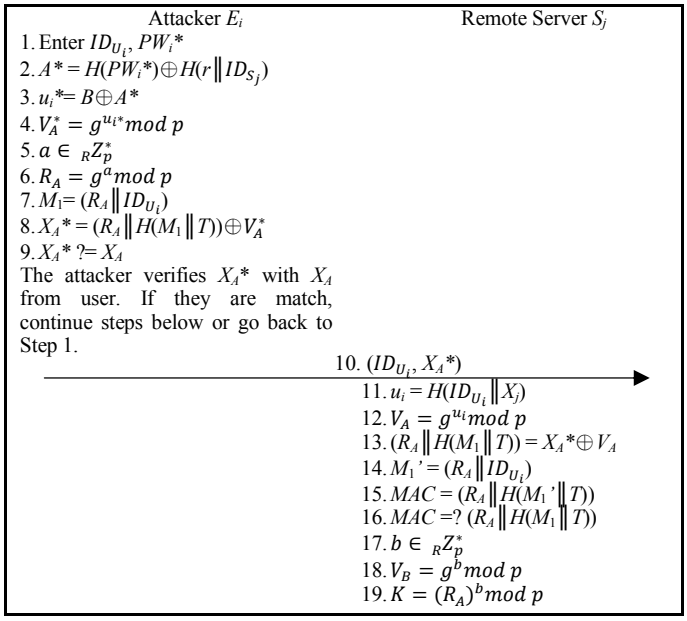
B. Online Server Spoofing

If the adversary has the USB of legitimate user and obtains B and r, the adversary can guess a password PW^*_i and compute u_i. The adversary gets the message (ID_{U_i}, X_A) from user. If attacker guesses the correct password, MAC will be verified successfully, and the adversary will establish session key and send it to user for authenticating without user knowing that the server is spoofed.

Figure 5. Online server spoofing attack at authenticated key exchange phase of Hsu et al's protocol [3]

C. Offline User Impersonating

The adversary eavesdrops on the message (ID_{U_i}, X_A) from user and gets X_A for authentication. If the adversary has the USB of legitimate user and obtains B and r, the adversary can guess a password PW^*_i, compute u_i, and use u_i to compute X_A^*. If $X_A^* = X_A$, the adversary impersonates user successfully.



20. $\beta = H(K \| ID_{U_i} \| ID_{S_j})$
21. $\theta = E_{R_A}(V_B, \beta)$
22. (θ) ←
23. $(V_B, \beta) = D_{R_A}(\theta)$
24. $K_1 = (V_B)^a \bmod p$
25. $\beta' = H(K_1 \| ID_{U_i} \| ID_{S_j})$
26. $\beta' = ?\beta$

$K_1 = (V_B)^a \bmod p = (g^b)^a \bmod p = g^{ab} \bmod p = (g^a)^b \bmod p = (R_A)^b \bmod p = K$

Figure 6. Offline user impersonating attack at authenticated key exchange phase of Hsu et al's protocol [3]

IV. PROPOSED PROTOCOL

We propose an authenticated key exchange protocol for multi-server mobile networks based on Chebyshev chaotic map. We will introduce some mathematical theory and our protocol below.

A. Chebyshev chaotic map

This section describes the Chebyshev chaotic map, which has semi-group property [14].

Definition 1 (*Chebyshev polynomials*). Let n be an integer, and let x be a variable taking values over the interval $[-1, 1]$. Chebyshev polynomial maps T_n: $R \rightarrow R$ of degree n is defined using the following recurrent relation:

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

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

The first few Chebyshev polynomials are:

$$T_2(x) = 2x^2 - 1, \quad (2)$$

$$T_3(x) = 4x^3 - 3x, \text{ and} \quad (3)$$

$$T_4(x) = 8x^4 - 8x^2 + 1. \quad (4)$$

The interval $[-1, 1]$ is invariant under the action of the map T_n : $T_n([-1, 1]) \rightarrow [-1, 1]$. Therefore, the Chebyshev polynomial restricted to the interval $[-1, 1]$ is a well-known chaotic map for all $n > 1$. It has a unique absolutely continuous invariant measure with positive Lyapunov exponent ln n. For $n = 2$, the Chebyshev map reduces to the well-known logistic map.

Definition 2 Let n be an integer, and let x be a variable taking values over the interval $[-1, 1]$. The polynomial $T_n(x)$: $[-1, 1] \rightarrow [-1, 1]$ is defined as:

$$T_n(x) = \cos(n \cos^{-1}(x)). \quad (5)$$

Definition 3 (*Semi-group property*). One of the most important properties of Chebyshev polynomials is the so called semi-group property which establishes that:

$$T_r(T_s(x)) = T_{rs}(x). \quad (6)$$

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

$$T_r(T_s(x)) = T_s(T_r(x)). \quad (7)$$

Definition 4 (*Enhanced Chebyshev polynomials*). In order to enhance the property of the Chebyshev chaotic map, Zhang proved that the semi-group property holds for Chebyshev polynomials defined on interval $[-\infty, +\infty]$, and he had the experimental result and cryptanalysis to prove that the enhanced Chebyshev polynomials is more secure than the original one [15]. This paper utilizes the following enhanced Chebyshev polynomials:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) (\text{mod } N), \quad (8)$$

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

$$T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x)), \quad (9)$$

so the semi-group property still holds and the enhanced Chebyshev polynomials also commute under composition.

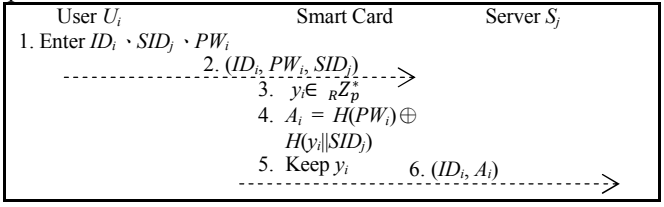
B. Proposed protocol

Our protocol is divided into four phases: the system initialization, the user registration, the authenticated key exchange and password changing phase. Some used notations are defined as Table 2.

TABLE II. NOTATIONS OF OUR PROTOCOL

Notations	Description
ID_i	User U_i's identity
SID_j	Remote server S_j's identity
$\oplus$	Exclusive OR (XOR) operation
$H(\cdot)$	Collision-resistant one-way hash function
PW_i	User U_i's password
x_{S_j}	Remote server S_j's secret
k	Encryption/decryption key k
$E_k(\cdot)$	Symmetric encryption algorithm with key k
$D_k(\cdot)$	Symmetric decryption algorithm with key k
x, y_i	Random numbers
$h_k()$	Collision-resistance secure one-way chaotic hash function
USB	Portable USB device
s	Server's new chaotic random number
r_i	User's new chaotic random number

In the system initialization phase, each user sets up his smart card by entering identifier and password into it. Figures 7, 8, and 9 illustrate these phases. Figure 7 illustrates the registration phase. Figure 8 illustrates the authenticated key exchange phase. User and server verify each other and establish session key in this phase. Figure 9 is password changing phase which can let user update the password of smart card offline.



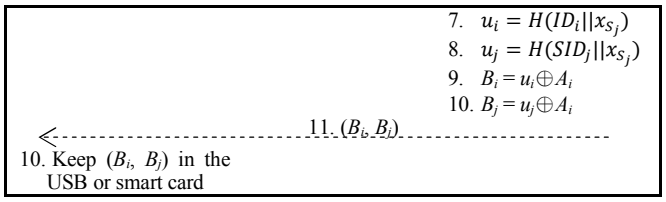


Figure 7. Registration phase of our protocol

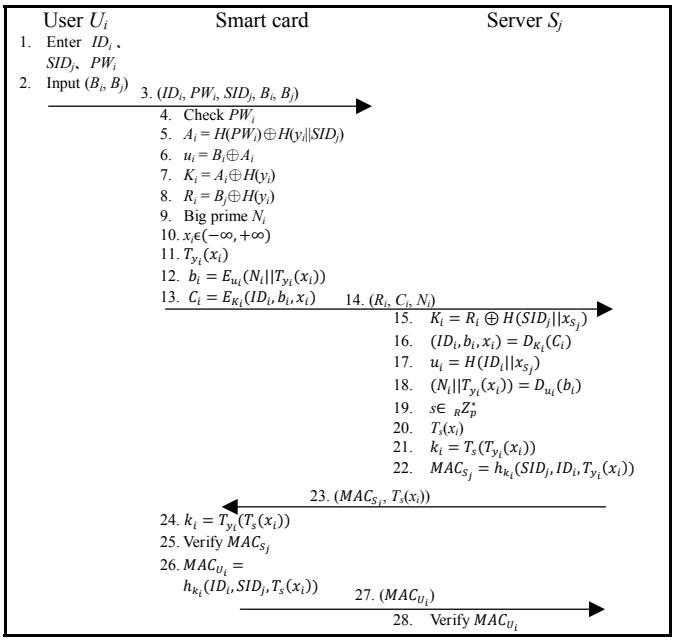


Figure 8. Authenticated key exchange phase of our protocol

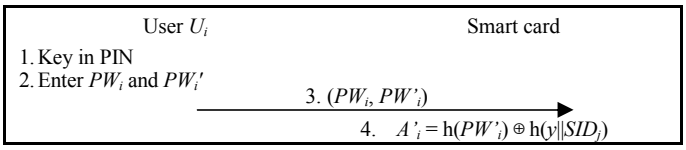


Figure 9. Offline password changing phase of our protocol

V. SECURITY ANALYSIS

We present several security analyses of the proposed key agreement protocol. Theoretical analyses prove the proposed protocol could resist common attacks.

A. Resistance to attacks Hsu et al.'s protocol might face

In Hsu et al.'s protocol [3], user's random number r and server's secret value B are stored in USB. We keep user's random number y_i in smart card, so adversary can only get B_j even getting the USB. If adversary wants to attack, he has to have user's smart card and correct password. We keep user's random number y_i in smart card, and it is hard to obtain the information in the smart card. There is a limited number of times for entering the password, or the card will be lock when entering over the times, and the attack will be terminated. As a result, our protocol can resist online user impersonating, online server spoofing, and offline user impersonating attacks.

B. Security resistant to Bergamo et al.'s attack

Bergamo et al.'s attack [1] is based on two conditions. The first is the attackers could obtain the related elements x, $T_{y_i}(x_i)$ and $T_s(x)$, and the second is several Chebyshev polynomials passing through the same point due to the periodicity of the cosine function. In Step 18 of the authenticated key exchange phase of proposed protocol, although attackers could obtain $T_s(x)$ easily, they cannot obtain $T_{y_i}(x_i)$ because it is encrypted in all the messages and only the sender and the receiver know the decryption key. Besides, the proposed protocol utilizes the enhanced Chebyshev polynomials, in which the periodicity of the cosine function is avoided by extending the interval of x to $(-\infty, +\infty)$, and it had been proved that the enhanced Chebyshev polynomials is more secure than the original one [15]. As a result, Bergamo et al.'s method [1] does not work.

C. Mutual authentication and key agreement

In Step 17 of the authenticated key exchange phase of proposed protocol, server encrypts SID_j, ID_i, and $T_{y_i}(x_i)$ from user to message authentication code MAC_{S_j} with session key $k_i = T_s(T_{y_i}(x_i))$ and sends MAC_{S_j} and $T_s(x_i)$ to user. At Step 19, user uses $T_s(x_i)$ form server and $T_{y_i}(x_i)$ which user generated at Step 9 to obtain session key k_i and uses it to verify $MAC_{S_j} = h_{k_i}(SID_j, ID_i, T_{y_i}(x_i))$. Server verifies the message authentication code sent by user $MAC_{U_i} = h_{k_i}(ID_i, SID_j, T_s(x_i))$ at Step 23. MAC_{S_j} and MAC_{U_i} are included the session key $k_i = T_{y_i s}(x) = T_{y_i}(T_s(x)) = T_s(T_{y_i}(x))$ that only two parties of the communication have it, so only user U_i and server S_j can verify each other.

D. Resistant to man-in-the-middle attack

In the proposed protocol, the adversary cannot modify message authentication code MAC_{S_j} and MAC_{U_i} without obtaining session key k_i. User and server can confirm the message is resent, modified, and replaced or not by checking information in the message authentication code. In authenticated key exchange phase, user verifies $MAC_{S_j} = h_{k_i}(SID_j, ID_i, T_{y_i}(x_i))$ at Step 20, and server verifies $MAC_{U_i} = h_{k_i}(ID_i, SID_j, T_s(x_i))$ at Step 23. As a result, the proposed protocol can resist man-in-the-middle attack.

E. Resistant to replay attack

In the proposed protocol, we use random numbers y_i and s to resist replay attack. Because two parties of the communication can put session key $k_i = T_{y_i}(T_s(x_i))$ and random numbers y_i and s into message authentication code, they can confirm that the message is resent or not by checking information on the message authentication code. As a result, the proposed protocol can resist replay attack.

F. User anonymity

User's identity is protected by encrypting it as $C_i = E_{K_i}(ID_i, b_i, x_i)$ before sending it. ID_i is encrypted in C_i with K_i, and server has to obtain K_i first by computing $K_i = R_i \oplus$

$H(SID_j||x_{S_j})$. The adversary cannot get ID_i even he gets R_i and C_i because only server knows the secret x_{S_j}. The adversary cannot obtain K_i without knowing x_{S_j} and decrypt C_i, so he cannot get ID_i, either. As a result, the proposed protocol can satisfy user anonymity on communication.

VI. CONCLUSIONS

We proposed an authenticated key exchange protocol for multi-server mobile networks based on Chebyshev chaotic map, and the proposed protocol can resist some probable attacks and drawbacks at previous research, and it can also provide user anonymity. We proposed security analysis of Hsu et al.'s [3] protocol and describe the attack scenario first. Then, we proposed the enhanced protocol and analyzed security. Moreover, the proposed protocol is based on Chebyshev chaotic map, so it is more practical and efficient. Properties of the proposed protocol are given below. (i) The user can easily memorize a single password to login different servers without the assistance of a trusted registration authority. (ii) The user can share distinct secret information with different servers, and hence a malicious server cannot use it to masquerade as the user to login the other server(s). (iii) It is secure against some potential attacks. (iv) An authenticated key shared between the user and the server can be established for securing their communications. (v) It can provide key confirmation for the shared session key. (vi) It can provide higher security assurance in generating secret keys.

VII. ACKNOWLEDGMENT

We would like to thank anonymous referees for their valuable suggestions. This work was supported in part by National Science Council under the grants NSC 100-2628-H-182-001-MY3.

REFERENCES

[1] Bergamo, P., D'Arco, P, De Santis, A., Kocarev, L., "Security of Public-Key Cryptosystems Based on Chebyshev Polynomials," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 52, no. 7, pp. 1382-1393, 2005.

[2] Chang, C. C., and Kuo, J. Y., "An Efficient Multiserver Password Authenticated key Agreement Scheme Using Smart Cards with Access Control," 2005.

[3] Hsu, C. L., Wu, T. S., Lin, H. Y., "Password-Based Authenticated Key Exchange Protocol without Trusted Third Party for Multi-Server Environments," *International Journal of Innovative Computing, Information and Control,* vol. 8, no. 3 A, pp. 1541-1555, 2012.

[4] Hwang, R. J., and Shiau, S. H., "Provably Efficient Authenticated Key Agreement Protocol for Multi-Servers," *The Computer Journal,* vol. 50, no. 5, pp. 602-615, 2007.

[5] Jeun, I., Kim, M., Won, D., "Enhanced Password-Based User Authentication Using Smart Phone," in 7th International Conference on Advances in Grid and Pervasive Computing, Hong Kong, 2012, pp. 350-360.

[6] Juang, W. S., "Efficient Multi-Server Password Authenticated Key Agreement Using Smart Cards," *IEEE Transactions on Consumer Electronics,* vol. 50, no. 1, pp. 251-255, 2004.

[7] Kocarev, L., and Tasev, Z., "Public-Key Encryption Based on Chebyshev Maps," in Proceedings of the 2003 IEEE International Symposium on Circuits and Systems, Bangkok, 2003, pp. III28-III31.

[8] Mun, H., Han, K., Lee, Y. S., Yeun, C. Y., Choi, H. H., "Enhanced Secure Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks," *Mathematical and Computer Modelling,* vol. 55, no. 1-2, pp. 214-222, 2012.

[9] National Institute of Standards and Technology, "Digital Signature Standard (DSS)," 1998.

[10] Tsai, J. L., "Efficient Multi-Server Authentication Scheme Based on One-Way Hash Function without Verification Table," *Computers & Security,* vol. 27, no. 3-4, pp. 115-121, 2008.

[11] Tsaur, W. J., Li, J. H., Lee, W. B., "An Efficient and Secure Multi-Server Authentication Scheme with Key Agreement," *Journal of Systems and Software,* vol. 85, no. 4, pp. 876-882, 2012.

[12] Wang, R. C., Juang, W. S., Lei, C. L., "User Authentication Scheme with Privacy-Preservation for Multi-Server Environment," *IEEE Communications Letters,* vol. 13, no. 2, pp. 157-159, 2009.

[13] Wang, X., and Zhao, J., "An Improved Key Agreement Protocol Based on Chaos," *Communications in Nonlinear Science and Numerical Simulation,* vol. 15, no. 12, pp. 4052-4057, 2010.

[14] Yoon, E. J., and Jeon, I. S., "An Efficient and Secure Diffie–Hellman Key Agreement Protocol Based on Chebyshev Chaotic Map," *Communications in Nonlinear Science and Numerical Simulation,* vol. 16, no. 6, pp. 2383-2389, 2011.

[15] Zhang, L., "Cryptanalysis of the Public Key Encryption Based on Multiple Chaotic Systems," *Chaos, Solitons & Fractals,* vol. 37, no. 3, pp. 669-674, 2008.