International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 147-156
http://dx.doi.org/10.14257/ijsia.2015.9.6.15

A Chebyshev-Map Based One-Way Authentication and Key Agreement Scheme for Multi-Server Environment

Zengyu Cai, Yuan Feng, Junsong Zhang, Yong Gan and Qikun Zhang

Institute of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China
mailczy@163.com

Abstract

One-way authentication and key agreement scheme can achieve strong user anonymity and transmitted data confidentiality over insecure public communication channel, which is very useful for the user who cares about his/her identity information. In conventional networks, Public Key Infrastructure (PKI) is a very useful component to design one-way authentication key agreement scheme. However, it will consume large amounts of computing resources. Therefore, it is inappropriate to PKI in a resource-constrained environment. In this paper, we proposed a new one-way authentication and key agreement scheme based on Chebyshev chaotic map. Compared with the related research activities, our proposed scheme has not only the high efficiency and unique functions, but also robust to various attacks and achieves perfect forward secrecy. Security and performance analyses demonstrate that the proposed scheme can solve various types of security problems and can meet the requirements of computational complexity for low-power mobile devices.

Keywords: *One-Way Authentication, Anonymity, Chebyshev chaotic map*

1. Introduction

Nowadays, mobile devices (*i.e.*, smart phones, PDAs) are widely used in many mobile applications, such as online shopping, mobile pay-TV, and electronic transactions. Along with the increasing number of mobile applications, the security issues have been received more and more attention. Authenticated key exchange (AKE) [1] is one of the most important cryptographic components which is used for establishing an authenticated and confidential communication channel between communicating participants. Generally, the user must be authenticated by the remote server before he accesses the services provided by the remote servers. The password-based authentication scheme [2-3] [7-10] is one of widely used AKE mechanisms to verify the validity of the remote users over an insecure communication channel, and is a protective barrier that can prevent unauthorized personnel from accessing services provided by the application server. Recently many researchers achieve AKE in the multi-server environment called multi-server authenticated key agreement (MSAKA) protocols [6, 8, 10, 12]. MSAKA protocols allow the user to register at the registration center (RC) once and can access all the permitted services provided by the eligible servers.

In 2001, Li *et al.*, [9] proposed a remote password authentication scheme for multi-server environments. In Li *et al.*, the password authentication system is a pattern classification system based on an artificial neural network. Therefore, their scheme needs long time to train neural networks. Then, Lin *et al.*, [23] proposed an improved authentication scheme based on ElGamal digital signature. Juang [6] proposed a new multi-server password authentication protocol using the hash function and symmetric key cryptosystem. However, Chang and Lee [14] pointed out that Juang's protocol lacks efficiency and is vulnerable to off-line dictionary attack. Therefore, Chang and Lee

ISSN: 1738-9976 IJSIA

proposed a novel authentication scheme to remedy these weaknesses. Then, Tsai [12] proposed an efficient multi-server authentication protocol based on one-way hash function.

However, most existing AKE or MSAKA schemes are focus on mutual authentication, in which both parties authenticate themselves to each other. In many applications, we do not need mutual authentication and just need only one-way authentication. Take patient-to-expert model for instance: In network medical treatment system, patients reluctant to leak his/her identity to the doctor when he/she obtain the medical advice from the doctor, while he/she still wants the system could maintain the confidentiality of their request and assurance that the medical advice received comes from an authentic, qualified source.

The core concept of one-way AKE is that one party wishes for no one to be able to determine his/her identity, including all the authentication entities. Recently, only a few authentication schemes have considered the problem of one-way authentication. In 2006, Goldberg [17] proposed a specialized one-way AKE security definition for the Tor authentication scheme. Kate *et al.*, [18] described an identity based anonymous authentication key exchange scheme with improved forward secrecy. Morrissey *et al.*, [19] analyzed the security of the Transport Layer Security (TLS) protocol in the context of one-way authentication with specialized security definition. Generally, public key encryption can be used for one-way authentication key exchange schemes. However, the public key encryption will consume large amounts of computing resources, which is unsuitable in resources-limited environment.

In this paper, we proposed a novel one-way authentication key agreement scheme for multi-server environment. The proposed scheme is based on Chebyshev chaotic map. Compared with the authentication scheme based on modular exponentiation and scalar multiplication on elliptic curve, our proposed scheme is more efficient. Security and performance analyses demonstrate that the proposed scheme can solve various types of security problems such as impersonation attack, man-in-the-middle attack, replay attack and provide forward secrecy.

The remainder of this paper is organized as follows. In Section 2, we briefly review some preliminaries used in this paper. Section 3 describes the proposed one-way authentication and key agreement scheme. Then, we present the security analysis and performance evaluation about the proposed scheme in Section 4 and Section 5, respectively. Finally, Section 6 concludes the paper.

2. Preliminaries

In this section, we briefly introduce the basic concepts of Chebyshev chaotic map [21] and its related mathematical properties. And then, the basic concepts of one-way hash function and Symmetric encryption are described. In the end of this section, the security requirements about a secure and efficient authentication scheme are given.

2.1. Chebyshev Chaotic Map

Let n be an integer and x be a variable with the interval [-1, 1]. The Chebyshev polynomial $T_n(x)$: [-1, 1] → [-1, 1] is defined as $T_n(x) = \cos(n \arccos(x))$, Chebyshev polynomial map Tn: $R \rightarrow R$ of degree n is defined by the following recurrent relation:

$$T_n(x) = 2xT_n\text{-}_1(x) - T_{n-2}(x), \qquad (1)$$

where $n \geq 2$, $T_0(x) = 1$ and T1$(x) = x$.

The first few Chebyshev polynomials are as follows.

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

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

$$T_r(T_s(x)) = \mathrm{Tr}_{-s}(x). \quad (2)$$

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

$$T_r(T_s(x)) = \mathrm{Ts}(T_r(x)). \quad (3)$$

In order to improve the security of Chebyshev polynomials, Zhang [] proved that semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$.

The enhanced Chebyshev polynomials are expressed in the form.

$$T_n(x) = (2xT_{n-1}(x) - \mathrm{Tn}_{-2}(x)) \pmod N, \quad (4)$$

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

$$T_{r-s}(x) = T_r(T_s(x)) = \mathrm{Ts}(T_r(x)). \quad (5)$$

2.2. Computational Problems

To prove the security of our proposed protocol, we present some important mathematical properties of Chebyshev chaotic map as follows.

1) Semi-group: Given $x \in [-1. 1]$, $T_r(\mathrm{Ts}(x)) = \cos(r \cos^{-1}(s \cos^{-1}(x))) = \cos(rs \cos^{-1}(x)) = T_{sr}(x) = T_s(T_r(x))$.

2) Chaotic Maps-based Discrete Logarithm Problem (CMBDLP): Given x and y, it is intractable to find the integer s, such that $T_s(x) = y$.

3) Chaotic Maps-based Diffie-Hellman Problem (CMBDHP): Given x, $T_r(x)$ and $T_s(x)$, it is intractable to find $T_{rs}(x)$.

2.3. One-way Hash Function

One-way hash function [8] is an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, and it is easy to compute on every input but hard to compute the input from a given output. Here "easy" and "hard" are to be understood in the sense of computational complexity theory. A secure cryptographic one-way hash function has the following properties.

For any given input x, it is easy to compute the output.

1)·It is infeasible to deriving x from the given value $y = h(x)$.

2)·It is infeasible to find two different inputs with the same output.

3)·It is infeasible to modify an input without changing the output.

2.4. Symmetric Encryption

A symmetric encryption scheme $E(Kgen, E, D)$ consists of three algorithms as follow.

1) Randomized key generation algorithm $Kgen$: it returns a key k drawn from the key pool $Keys(E_k)$ randomly.

2) Encryption algorithm E: it makes the key $k \in Keys(E_k)$ and a plaintext $M \in \{0, 1\}^*$ as the input and a ciphertext $C \in \{0, 1\}^*$ as its output. And it can be written $C = E_k(M)$.

3) Decryption algorithm D: it takes the key k and a ciphertext $C \in \{0, 1\}^*$ as the input and outputs a plaintex $M \in \{0, 1\}^*$, it can be written $M = D_k(C)$.

2.5. Security Requirements

In general, a secure and efficient remote user authentication scheme should satisfy the following requirements.

• User anonymity: The adversary cannot track a special user by the user's identity, therefore it can protect the user's privacy.

• No password table: The registration center should be without the user's password table to authenticate the users.

• Low computation and communication cost: Due to the limited energy, processing and storage resources of mobile devices, the design of authentication scheme must take computation efficiency into consideration

• Security: The authentication scheme must be able to prevent from various kinds of attacks.

• Mutual/one-way authentication and session key agreement.

3. The Proposed One-Way Authentication and Key Agreement Scheme

In this section, a Chebyshev chaotic maps-based one-way authentication and key agreement scheme is proposed. Without loss of generality, the proposed authentication scheme consists of two phases: the registration phase and the authentication and session key agreement phase. For the sake of clarity, the notations used in this paper are summarized and defined in Table 1.

Table 1. List of Notations

Notation	Description
SID_A	A temporary session
S_i, ID_{Si}	The *i*th server, the identity of the *i*th server, respectively
a, r_i	Nonce used in this paper
$(x, T_k(x))$	Public key based on Chebyshev chaotic maps
k	Secret key based on Chebyshev chaotic maps
RC	Registration center
$E_K( )/D_K( )$	A pair of secure symmetric encryption/decryption functions with the key K
H	An secure one-way hash function
$\|\|$	Concatenation operation

3.1. Server Registration Phase

Without loss of generality, it is assumed that the multi-server environment includes three kinds of participants: a trusted registration center (RC), users and servers. In addition, it is assumed that the servers can register at the registration center via secure communication channel. The detailed server registration phase steps are performed as follows.

Step R1. When a server S_i or an authenticated expert wants to be a new legal service provider, it must choose its identity ID_{Si} with its identification card. Then the server submits the identity ID_{Si} to the RC via a secure channel.

Step R2. Upon receiving from the server ID_{Si} or an authenticated expert, the RC computes $R = H(ID_{Si} \| k)$, where k is the secret key of RC. Then the RC returns the value R to the server or the authenticated expert via a secure channel.

The server registration phase are depicted in Figure 1.

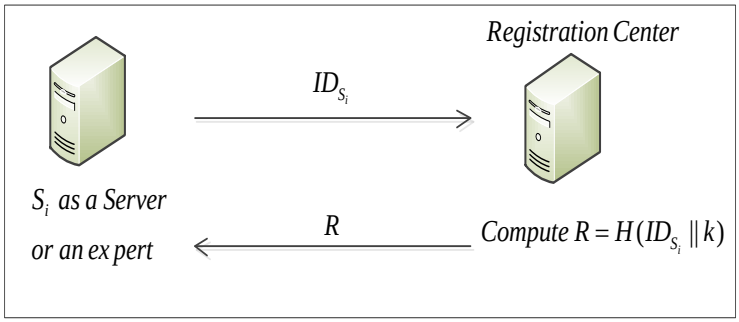

Figure 1. Server Registration Phase

3.2. One-way Authentication and Key Agreement Phase

In this phase, the server or the RC can be authenticated by the other two communication entities, but the user cannot be authenticated by the server or the RC. By this way, the user can be maintained his/her anonymity in the multi-server architecture. The concrete process is presented in Figure 2.

Step A1. When a user U_j (assume U_j as an anonymous user) wants to consult some personal issues from S_i (or an expert) in a secure way, he/she will choose a random integer number a and a temporary session SID_A. Then U_j computes $K_{A\text{-}RC} = T_aT_k(x)$, $H_A = H(SID_A \| ID_{Si} \| T_a(x))$, $C_1 = E_{K_{A\_RC}}(SID_A \| ID_{Si} \| H_A)$. Next, U_j sends $m_1 = \{SID_A, T_a(x), C_1\}$ to the server Si where she/he wants to obtain the service.

Step A2. Upon receiving the message $m_1 = \{SID_A, T_a(x), C_1\}$, S_i will do the following tasks to ask RC to authenticate itself: S_i selects a random number r_i and computes $T_{ri}(x)$, $C_2 = H(ID_{Si} \| m_1 \| R \| T_{ri}(x))$. Then, S_i sends the message $m_2 = \{ID_{Si}, T_{ri}(x), C_2, m_1\}$ to RC.

Step A3. Next, RC will help the user U_j to authenticate the legality of the server S_i and verify the temporary information by helping them to compute the session key. Upon receiving the message $m_2 = \{ID_{Si}, T_{ri}(x), C_2, m_1\}$, RC needs to proceed as follows.

1) Authenticating the legality of the server S_i. Based on the server's identity ID_{Si}, RC computes $R' = H(ID_{Si} \| k)$. Then, RC computes $C_2' = H(ID_{Si} \| m_1 \| R' \| T_{ri}(x))$ and checks whether $C_2' = C_2$. If they are equal, RC believes that the server S_i is a legal sever.

2) Confirm S_i is the right server which the user U_j wants to communicate with: RC computes $K_{RC\text{-}A} = T_kT_a(x)$ and then decrypts C_1 to obtain the values $SID_A \| ID_{Si} \| H_A$. Then, RC caculates $H_A' = H(SID_A \| ID_{Si} \| T_a(x))$ and checks whether $H_A' = H_A$. If they are equal and ID_{Si} is the same as the value extract from C_1, that means S_i is the server that the user U_j wants to communicate with.

3) Assisting the server S_i and the user U_j to generate the session key: RC computes $C_3 = H(ID_{RC} \| ID_{Si} \| m_1 \| R \| T_{ri}(x))$, $H_{RC} = H(SID_A \| ID_{Si} \| ID_{RC} \| T_{ri}(x))$ and $C_4 = E_{K_{RC\_A}}(ID_{RC} \| ID_{Si} \| m_1 \| T_{ri}(x) \| H_{RC})$. Then, RC sends the message $\{ID_{RC}, C_4\}$ to the user U_j and sends the message $\{ID_{RC}, C_3\}$ to the server S_i.

If any of above authentication process cannot be established, the authenticate scheme will be terminated immediately.

Step A4. For the user U_j: After receiving the message $\{ID_{RC}, C_4\}$, the user U_j computes the key $K_{A\text{-}RC}$ and then uses the key to decrypt C_4. Next, U_j computes $H_{RC}' = H(SID_A \| ID_{Si} \| ID_{RC} \| T_{ri}(x))$ and checks whether $H_{RC}' = H_{RC}$. If they are equal, the user U_j computes the session key $SK = T_aT_{ri}(x)$.

For the server S_i: After receiving the message $\{ID_{RC}, C_3\}$, S_i computes $C_3' = H(ID_{RC} \| ID_{Si} \| m_1 \| R \| T_{ri}(x))$ and checks whether $C_3' = C_3$. If they are equal, the server S_i computes the session key $SK = T_{ri}T_a(x)$.

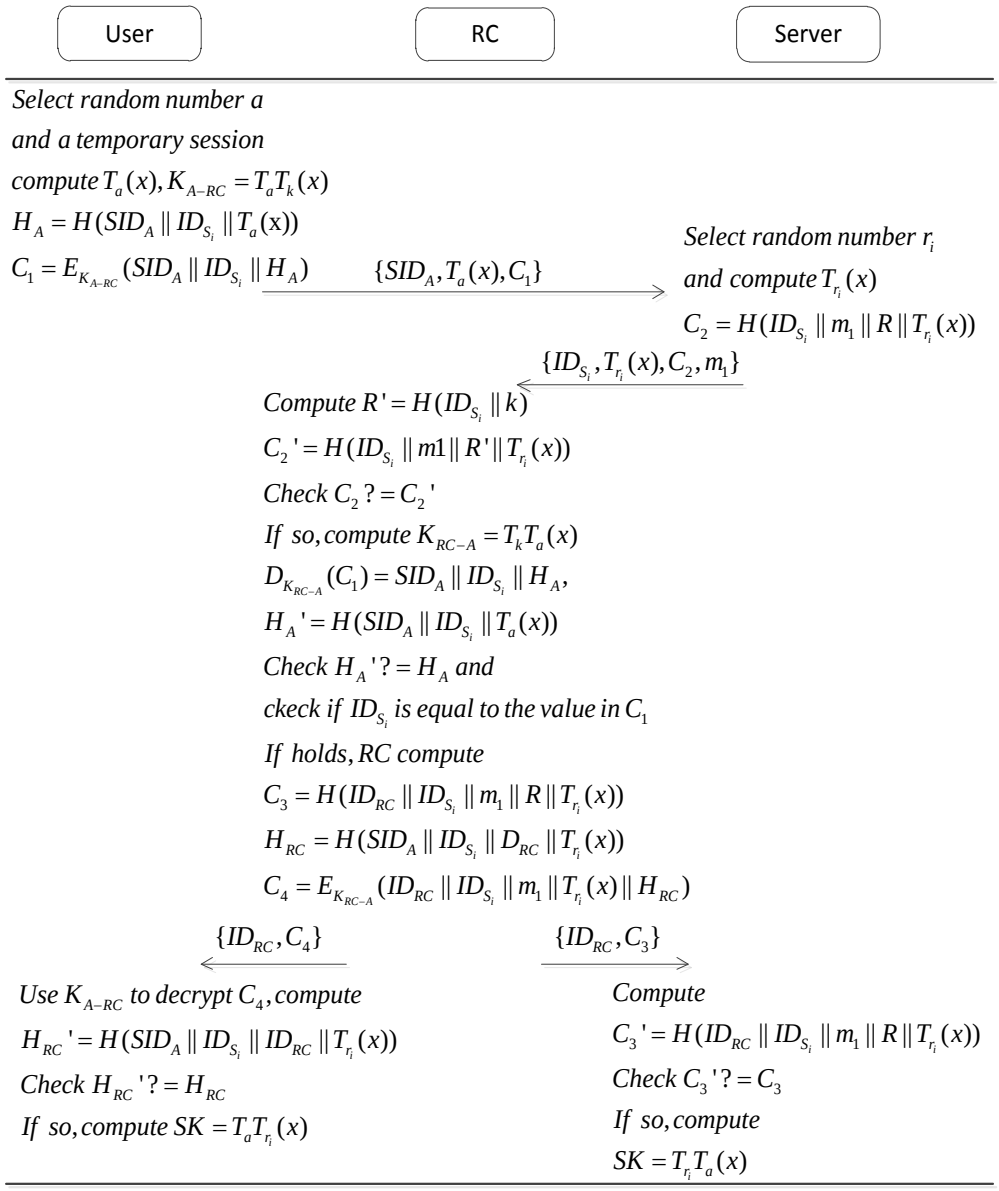

Figure 2. The Authentication and Key Agreement Phases of Our Scheme

4. Security Analysis of the Proposed Scheme

In this section, we analyze the security of the proposed authentication and key agreement scheme. We consider the assumptions and threat model presented in Section 2 and prove that the proposed scheme is secure against the following attacks.

Corollary 1. The Proposed Authentication can Resist Impersonation Attack

Proof: In the proposed scheme, any adversary cannot impersonate anyone of the server S_i and the RC. The proposed authentication scheme has already authenticated each other between the server S_i and the RC, and the user U_j authenticates S_i and RC based on the secrets *k*, *R* and the nonce *a* and *ri*. Therefore, there is no way for an adversary to have a chance to carry out impersonation attack.

Corollary 2. The Proposed Authentication can Resist Replay Attack

Proof: If an adversary replays any message of the user U_j, he/she cannot be authenticated successfully. Because the user U_j is an anonymous user, the adversary can as an anonymous user to initiate the protocol legally as his wish.

For the messages between S_i and RC, an adversary cannot start a replay attack against our authentication scheme because of the freshness of the values a and r_i in each session. If $T_a(x)$ and $T_{ri}(x)$ have appeared before or the status shows in process, any of the participants in instance protocol will reject the session request. If the adversary wants to launch the replay attack successfully, it must have the ability to compute the correct $T_a(x)$, $T_{ri}(x)$ and C_i ($1 \leqslant i \leqslant 4$). Unfortunately, it is impossible.

Corollary 3. The Proposed Protocol can achieve perfect forward secrecy

Proof: In the proposed scheme, the session key $SK = T_aT_{ri}(x) = T_{ri}T_a(x)$ is related to the parameters a and r_i, which are randomly chosen by the user U_j and the server S_i, respectively. Therefore, any session key has not related with the secret key (i.e. k) of each of the communicating participants. In addition, based on Chaotic Maps-based Discrete Logarithm Problem (CMBDLP) and Chaotic Maps-based Diffie-Hellman problem (CMBDHP), the adversary cannot compute the previously established session keys.

Corollary 4. The Proposed Protocol can achieve session key security

Proof: In the authenticated key agreement phase of the proposed scheme, a session key SK is generated by the parameters a and r_i. These parameters are different in different sessions, and each of them is only known by the user U_j and the server S_i, respectively. At the end of the session between the user U_j and the server S_i, the session key will immediately be invalidated and will not be reused. Therefore, even though the attacker has obtained a session key, he/she cannot use this session key to decode the message in other communication processes.

In addition, since the random values a and r_i are very large, attackers cannot guess the values a and r_i to generate session key. Therefore, the proposed authentication scheme is able to provide session key security.

Corollary 5. The Proposed Protocol can Achieve One-Way Authentication and Key Agreement

Proof: In our proposed authentication scheme, one-way authentication means that RC helps an anonymous user U_j to authenticate the server S_i. So we can divide the one-way authentication process into three steps.

1) U_j authenticates RC: Because only RC has the secret k, RC can compute $K_{RC\text{-}A} = T_kT_a(x)$ which is equal to $K_{A\text{-}RC} = T_aT_k(x)$. Therefore, when the user U_j decrypts C_4 to get the necessary information and check whether $H_{RC}' = H_{RC}$, he/she has the ability to authenticate the RC.

2) RC and S_i authenticate each other: The proposed authentication scheme can use the shared key R to achieve this task. First, based on the server's identity ID_{Si}, RC can compute the value $R' = H(ID_{Si} \| k)$ by its private key k. Then, RC computes $C'_2 = H(ID_{Si} \| m_1 \| R' \| T_{ri}(x))$ and checks whether $C'_2 = C_2$. If they are equal, RC considers that the server S_i is a legal server.

After receiving the message $\{ID_{RC}, C_3\}$, the server S_i computes $C'_3 = H(ID_{RC} \| ID_{Si} \| m_1 \| R \| T_{ri}(x))$ and checks whether $C'_3 = C_3$. If they are equal, the server S_i believes that the RC is a legal entity. From the above analysis, it can be seen that the server S_i and the RC have the ability to authenticate each other.

3) U_j authenticates S_i: If the user U_j has already authenticated the RC, then he/she can authenticate the server S_i based on the information $ID_{RC} \| ID_{Si} \| m_1 \| T_{ri}(x) \| H_{RC}$ which were decrypted by the RC in the value C_4. The trust transference model is the user $U_j \rightarrow$ RC $\rightarrow S_i$.

As for the key agreement, after authenticating each other, the temporary $T_a(x)$, $T_{ri}(x)$ and the value $SID_A \| ID_{Si} \| ID_{RC}$ are already authenticated by RC. Therefore, the user U_j and the server S_i can make the key agreement simultaneously.

5. Performance Evaluation

In this section, we evaluate the performance of our scheme and compare it with other related authentication schemes. It is generally known that most of the mobile devices have limited power resources and computing capability. Therefore, one of the most important concerns of design authentication scheme in mobile environment is power consumption (include computation cost and communication cost). Compared to RSA and ECC, Chebyshev polynomial computation problem offers smaller key sizes, faster computation. In our proposed authentication scheme, there is no time-consuming modular exponentiation and scalar multiplication on elliptic curves needed. Since exclusive-OR operation requires extremely small computational cost, we neglect its computation cost.

For the convenience of evaluating the computational cost, we define some notations as follows.

T_h: The time for executing the hash function.

T_{sym}: The time for executing a symmetric key cryptography.

T_{exp}: The time for executing a modular exponentiation computation.

T_{CH}: The time for executing the Tn(x) mod p in Chebyshev polynomial using the algorithm in [21].

In Table 2, we demonstrate the comparisons between our proposed scheme and the previously authentication schemes. The scheme in [17] consumes more computations than our proposed scheme. The schemes in [5] own high-efficiency, but from the security point of view, they cannot resist some common attacks and cannot provide some common functionality such as session key secrecy. Therefore, we can draw a conclusion that our proposed scheme is more suitable for the mobile client server environments.

Table 2. Comparisons between our Proposed Scheme and the Previously Authentication Schemes

		Chen *et al*. [17]	Tsai [5]	Our scheme
login phase		$2T_h + T_{exp}$	$T_h + T_h$	$T_{sym} + T_h + T_{CH}$
Authentication phase	User	$T_h + T_{exp}$	$4T_h$	$T_h + T_{CH}$
	Server	$2T_h + 2T_{exp}$	$4T_h$	$2T_h + T_{CH}$
	RC	$6T_h$	-	$5T_h + T_{CH} + T_{sym}$
Password change phase		$2T_h$	$2T_h$	No need
Known attacks		masquerading attack	Impersonation attack	Provably secure

6. Conclusion

This paper provides a novel approach to design one-way authenticated key establishment towards multi-server architecture. The core concept of the proposed authentication scheme is establishing the mutual authentication for the servers and RC and the anonymity for the users. Subsequently, we explain the practical motivations for authentication and secrecy assurances of parties engaging in one-way AKE protocols and

some related terms. Based on our discussion we proposed a suitable protocol that covers those goals and offered an efficient protocol that formally meets the proposed security definition. Finally, after comparing with related literatures (multi-server authentication schemes and one-way authentication scheme) respectively, we found our proposed authentication scheme has satisfactory security, efficiency and functionality. Therefore, our proposed authentication scheme is more suitable for practical applications.

Acknowledgements

The authors are grateful to the editor and anonymous reviewers for their valuable suggestions which improved this paper. This research was partially supported by the National Natural Science Foundation of China under Grant No.61340059. It also was partially supported science and technology key projects of He'nan province (142102210081).

References

[1] L. Lamport, "Password authentication with insecure communication", Communication of ACM, vol. 24, no. 11, **(1981)**.
[2] C. Lee, C. Li and C. Hsu, "A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps", Nonlinear Dynamics, vol. 73, no. 1-2, **(2013)**.
[3] L. Hui, C. Wu and J. Sun, "A general compiler for password-authenticated group key exchange protocol", Information Processing Letters, vol. 110, no. 4, **(2010)**.
[4] T. Y. Wu, Y. M. Tseng and T. T. Tsai, "A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants", Computer Networks, vol. 56, no. 12, **(2012)**.
[5] H. Tseng, R. Jan and W. Yang, "A chaotic maps-based key agreement protocol that preserves user anonymity", IEEE International Conference on Communications (ICC'09), Dresden, Germany, **(2009)** June 14-18.
[6] W. S. Juang, "Efficient multi-server password authenticated key agreement using smart cards", IEEE Transaction on Consumer Electronics, vol. 50, no. 1, **(2004)**.
[7] D. He, J. H. Chen and J. Hu, "An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security", Information Fusion, vol. 13, no. 3, **(2012)**.
[8] J. S. Zhang, J Ma, X Li, WD Wang, "A Secure and Efficient Remote User Authentication Scheme for Multi-server Environments Using ECC", KSII Transaction on Internet and Information Systems, vol. 8, no. 8, **(2014)**.
[9] L. H. Li, L. C. Lin and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks", IEEE Transactions on Neural Networks, vol. 12, no. 6, **(2001)**.
[10] X. Li, J. Ma, W. D. Wang, Y. P. Xiong and J. S. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments", Mathematical and Computer Modeling, vol. 58, no. 1-2, **(2013)**.
[11] C. Li, C. Lee, C. Weng and C. Fan, "An Extended Multi-Server-Based User Authentication and Key Agreement Scheme with User Anonymity", KSII Transactions on Internet & Information Systems, vol. 7, no. 1, **(2013)**.
[12] J. L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table, Compute Secure", vol. 27, no. 3-4, **(2008)**.
[13] T. Y. Chen, C. C. Lee, M. S. Hwang and J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments", The Journal of Supercomputing, vol. 66, no. 2, **(2013)**.
[14] C. C. Chang and J. S. Lee, "An efficient and secure multi-server password authentication scheme using smart cards", Proc. of the third international conference on cyberworlds, Tokyo, Japan, **(2004)** November 18-20.
[15] H. C. Hsiang and W. K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment", Computer Standards & Interfaces, vol. 31, no. 6, **(2009)**.
[16] S. K. Sood, A. K. Sarje and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture", Journal of Network and Computer Applications, vol. 34, no. 2, **(2011)**.
[17] I. Goldberg, "On the security of the Tor authentication protocol", In George Danezis and Philippe Golle, editors, Privacy Enhancing Technologies (PET), LNCS, vol. 4258, **(2006)**.
[18] A. Kate, Greg M. Zaverucha and I. Goldberg, "Pairing-based onion routing with improved forward secrecy", ACM Transactions on Information and System Security, vol. 13, no. 4, **(2010)**.
[19] P. Morrissey, N. P. Smart, and B. Warinschi, "A modular security analysis of the TLS handshake protocol", Advances in Cryptology, LNCS, vol. 5350, **(2008)**.

[20] I. Goldberg, D. Stebila and B. Ustaoglu, "Anonymity and one-way authentication in key exchange protocols", Designs, Codes and Cryptography, vol. 67, no. 2, **(2013)**.
[21] X. Wang and J. Zhao, "An improved key agreement protocol based on chaos", Communications in Nonlinear Science and Numerical Simulation, vol. 15, no. 12, **(2010)**.
[22] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems", Chaos Solitons Fractals, vol. 37, no. 3, **(2008)**.
[23] I. C. Lin, M. S. Hwang, and L. H. Li, "A new remote user authentication scheme for multi-server architecture", Future Generation Computer Systems, vol. 19, no. 1, **(2003)**.

Authors

Zengyu Cai, he received his master degree in computer application technology from Northeast Normal University, Changchun, China, in 2006. He is a lecturer at Zhengzhou University of Light Industry. His research interests include trusted computing, plan recognition and information security.

Yuan Feng, she received her master degree in communication and information system from Chongqing University of Posts and Telecommunications, Chongqing, China, in 2006. She is a lecturer at Zhengzhou University of Light Industry. Her research interests include mobile communication, network engineering and information security.

Junsong Zhang, he received his master's degree in computer software and theory from Zhengzhou University (ZZU) in 2008 and Ph.D. degree in computer science and technology from Beijing University of Posts and Telecommunications (BUPT) in 2014. Dr. Zhang is a lecturer of Zhengzhou University of Light Industry (ZZULI). His research interests include information security and mobile network, etc.

Yong Gan, he received his Ph.D. degree in computer application technology from Xi`an Jiaotong University, Xi'an, China, in 2013. He is a professor at Zhengzhou University of Light Industry. His research interests include information security, cryptography, multimedia communications and network engineering.

Qikun Zhang, he received his Ph.D. degree in in Computer Science from Beijing University of Technology, Beijing, China, in 2013. He is a lecturer at Zhengzhou University of Light Industry. His research interests include network engineering, information security and cryptography.

