Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **3**, May **2016**

A Novel On-Demand Password Scheme Based on BAN Logic

Hongfeng Zhu

Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 China
zhuhongfeng1978@163.com

Dan Zhu

School of Foreign Languages
Shenyang Jianzhu University
No.9, HunNan East Street, HunNan District, Shenyang, P.C 110168 China
zhudan413@163.com

Yifeng Zhang and Yan Zhang

Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 China
1548452125@qq.com; 1505733680@qq.com

Received April, 2015; revised September, 2015

Abstract. *The technology of On-Demand Password (ODP), as an instance of authentication or other secure services technologies, is designed to assist the smart phone users accomplishing to forget their password and access any service with servers and thus having a better quality of life while preserving their privacy. The paper firstly proposed a universal and enhanced ODP scheme which can achieve two kinds of services without remembering any password for users: The first is login service which can make users use the ODP which was sent by the registration center (RC) to login certain server, such as E-mail and E-payment service. The other is session service which can let users use the ODP to get a secure session key with certain server, such as consulting service. Furthermore, our enhanced ODP scheme does not need to input the temporary short password which was sent by RC. Because this short password was already in the right place, the user only need to adopt some confirmed way, such as draw lines to confirm. About practical environment, we adopt multi-server architecture which can allow the user to register at the RC once and can access all the permitted services provided by the eligible servers. Then a new universal and enhanced ODP scheme is given based on chaotic maps. Security of the scheme is based on chaotic maps hard problems, a secure one way hash function and a secure symmetric cryptosystem. Compared with the related literatures recently, our proposed scheme can not only own high efficiency and unique functionality, but is also robust to various attacks and achieves perfect forward secrecy. Finally, we give the security proof and the efficiency analysis of our proposed scheme.*
Keywords: On-demand password, Key agreement, Multi-server architecture, Chaotic maps

1. **Introduction.** Rapid growth of mobile user population has caused an immense increase in demand for the mobile user experience, particularly for any rookie user with simple and secure services such as E-bussiness or log in an account. Mobile phone as a unique and private device, can change people's behavior, and also make some security technologies convert to another form. On-Demand Password (ODP, or called One-time On-Demand Password) [1] is a new authenticated way to let mobile users more secure and more convenient. ODP is proposed firstly by Yahoo, users can login Yahoo account by means of the short passwords which are sent by Yahoo to the mobile phones of users, without having to remember the passwords set up by themselves. In a word, using ODP technology, user's password file is replaced by a "Send my password" button, and then an SMS message with a verification code will be sent to the user's mobile phone. The key of ODP service is to make password stronger and more flexible. In order to make low-entropy password become a high-entropy secret, such as cryptographic key or authenticated code, people adopt many technologies. From the point of positive-going thinking, people usually use cryptology and delicate design protocol to make it, such as authenticated key exchange (AKE) [2-9] which can achieve authentication of the corresponding participants and confidentiality of data transmission. From another perspective, thinking in reverse, that dynamic security mechanism takes the place of static security mechanism can also increase the entropy, such as one-time password (OTP) [10-12] which means that the password can be used only once, or one-time identity password (OTIP) [13] which means the identity and the password can be used only once. Compared with the above-mentioned technologies, ODP technology makes use of privacy of mobile phone to increase the password's entropy, and at the same time, convenience and expansibility are also improved. However, Graham Cluley [1] pointed out that On-Demand Passwords maybe have a big security concern. Anyone can log into Yahoo as the user if he/she obtains the users phone or knows his or her Yahoo account username. People who enable the new service should be able to notice when their phone disappear. The way to avoid this risk is to set up phone screen lock or avoid showing the SMS message until the phone is unlocked. Despite this weakness, the new service called On-Demand Passwords provides a compelling thought for network security. Therefore, how to keep the mobile phone safe, and how to design the ODP to satisfy some specific properties, are the problems of interest to us. The paper is the first study ODP technology inside the ODP application. We can sum up most services on Internet as two types: login service and session service. Based on mobile phone number and ODP idea, we can design a universal scheme to achieve two services simultaneously or one of them individually. In order to get more general setting, multi-server architecture (MSA) [14-17] will be adopted in our scheme. MSA allows the user to register at the registration center (RC) once and can access all the permitted services provided by the eligible servers. In other words, users do not need to register at numerous servers repeatedly. The main contributions are shown as below: The paper firstly presents a new universal and enhanced ODP scheme towards multi-server architecture. Furthermore, the proposed protocol is mainly based on chaotic maps [18] without using modular exponentiation and scalar multiplication on an elliptic curve. In Security aspect, the protocol can resist all common attacks, such as impersonation attacks, man-in-the-middle attacks, etc. About functionality, the protocol also has achieved some well-known properties, such as perfect forward secrecy and execution efficiency. The rest of the paper is organized as follows: Some preliminaries are given in Section 2. Next, a new ODP scheme towards multi-server architecture is described in Section 3. Then, the security analysis and efficiency analysis are given in Section 4 and Section 5. This paper is finally concluded in Section 6.

2. **Preliminaries.**

2.1. **Multi-server architecture.** In the multi-server environment [14], each user must perform authentication procedure to login the server for a transaction. If the user is in a single authentication architecture, then the user must register at various servers and memorize the corresponding identifications and passwords, which could not be convenient for a user. In order to make the registration to various servers easier for users, each user must register with the registration center to obtain a secure account. Then the user uses the secure account to perform the login and authentication procedures with various servers.

2.2. **Security requirements.** Secure communication schemes for remote one-way authentication and session key agreement for the multi-server architecture should provide security requirements [2, 19]: (1) Hiding identity authentication: only the RC and the server know the users identity. (2) Impersonation attack: An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol. (3) Man-in-the-middle attack: The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. (4) Replay attack: A replay attack is a form of network attack in which a valid data transmission is repeated or delayed maliciously or fraudulently. (5) Known-key security: Known-key security is that a protocol can protect the subsequent session keys from disclosing even if the previous session keys are revealed by the intendant user. (6) Perfect forward secrecy: An authenticated key establishment protocol provides perfect forward secrecy if the compromise of both of the nodes secret keys cannot results in the compromise of previously established session keys. (7) Session key security: A communication protocol exhibits session key security if the session key cannot be obtained without any long-term secrets. (8) Resistance to stolen-verifier attacks: An adversary gets the verifier table from servers or RC by a hacking way, and then the adversary can launch any other attack which called stolen-verifier attacks. (9) No verification table: there is no verification table at the RC or the server at all. (10) Securely chosen password and time synchronization: Guarantee securely chosen password and no need for time synchronization among parties.

2.3. **Chebyshev chaotic maps.** Let n be an integer and let x be a variable with the interval $[-1, 1]$.The Chebyshev polynomial [20]$T_n(x) : [-1, 1] \to [-1, 1]$ is defined as $T_n(x) = \cos(ncos^{-1}(x))$. Chebyshev polynomial map $T_n : R \to R$ of degree n is defined using the following recurrent relation:

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

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

.
The first few Chebyshev polynomials are:
$T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$,..... One of the most important properties is that Chebyshev polynomials are the so-called semi-group property which establishes that

$$T_r(T_s(x)) = T_{rs}(x)$$

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

$$T_r(T_s(x)) = T_s(T_r(x))$$

In order to enhance the security, Zhang [21] proved that semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$. The enhanced Chebyshev polynomials are used in the proposed protocol:

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

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

$$T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$$

.

Definition 2.1. *(Semi-group property) Semi-group property of Chebyshev polynomials:* $T_{rs}(x) = T_r(T_s(x)) = \cos(r\cos^{-1}(s\cos^{-1}(x))) = \cos(rs\cos^{-1}(x)) = T_s(T_r(x)) = T_{sr}(x)$.

Definition 2.2. *Given x and y,it is intractable to find the integer s,such that $T_s(x) = y$.It is called the Chaotic Maps-Based Discrete Logarithm problem (CMBDLP).*

Definition 2.3. *Given x, $T_r(x)$ and $T_s(x)$,it is intractable to find $T_{rs}(x)$. It is called the Chaotic Maps-Based Diffie-Hellman problem (CMBDHP).*

3. The Proposed Privacy-Protection System with Multi-Server Architecture.

In this section, under the multi-server architecture, a privacy-protection system is proposed which consists of three phases: server registration phase, user registration phase, universal on-demand password service phase.

3.1. Notations.

In this section, any server i has its identity ID_{S_i}.Only RC has its identity ID_{RC} and public key $(x, T_k(x))$ and a secret key k based on Chebyshev chaotic maps, a secure one-way hash function $H(\cdot)$,and a pair of secure symmetric encryption/decryption functions $E_K()/D_K()$ with key K.The concrete notations used hereafter are shown in Table 1.

Table 1. Notations

Symbol	Definition
SID_A	a temporary session
S_i, ID_{S_i}	The ith server， the identity of the ith server, respectively
ODP	the temporary short password chosen by ***RC***
$Phone_{NO}$	User's phone number
a, r_i	nonces
$(x, T_k(x))$	public key based on Chebyshev chaotic maps
k	secret key based on Chebyshev chaotic maps
RC, ID_{RC}	registration center and its identity
$E_K() / D_K()$	a pair of secure symmetric encryption/decryption functions with the key K
H	A secure one-way hash function
$\|\|$	concatenation operation

3.2. **Server registration phase.** Concerning the fact that the proposed scheme mainly relies on the design of Chebyshev chaotic maps-based in multi-server architecture, it is assumed that the servers can register at the registration center in some secure way or by secure channel. The same assumption can be set up for servers. Fig.1 illustrates the server registration phase. Step 1. When a server wants to be a new legal service provider, the server submits ID_{S_i} to the RC via a secure channel.
Step 2. Upon receiving ID_{S_i} from the server, the RC computes $R = H(ID_{S_i}||k)$,where k is the secret key of RC. Then the server stores R in a secure way via a secure channel.

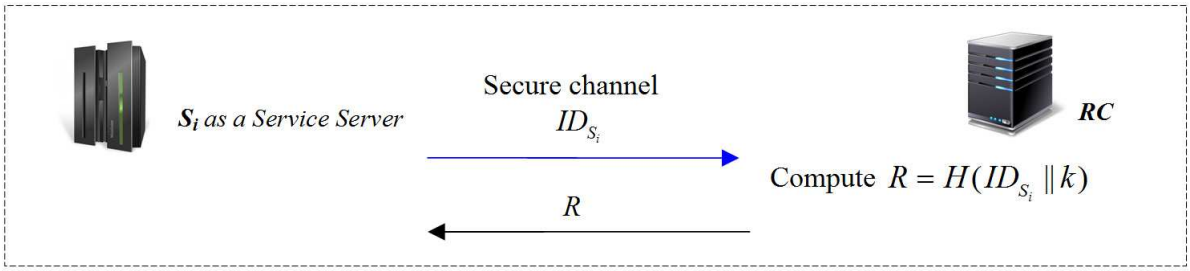

FIGURE 1. Server registration phase

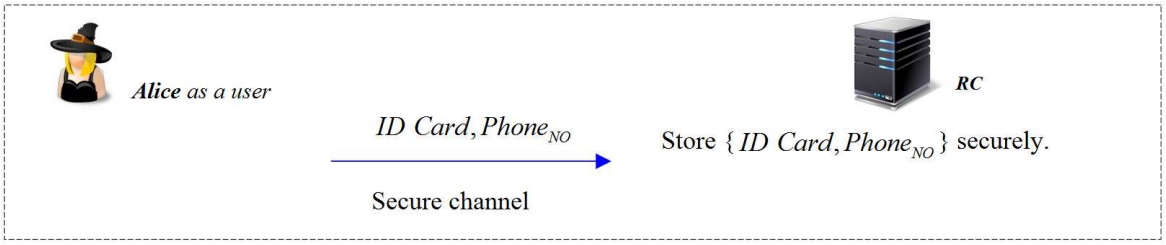

FIGURE 2. a premium user registration phase

3.3. **User registration phase.** Step 1. When a user wants to be a new legal user with on-demand password service, she must use her ID Card to open the phone service. In other words, Alice submits $IDCard, Phone_{NO}$ to the RC via a secure channel.
Step 2. Upon receiving $IDCard, Phone_{NO}$ from Alice, the RC will authenticate that Alices ID Card is valid by law. Then RC stores $IDCard, Phone_{NO}$ in a secure way to avoid losting the smartphone.

Remark 3.1. *If a user lost s/he Phone with the PhoneNumber , s/he can use IDCard to report and find the loss of PhoneNumber .*

3.4. **Universal on-demand password service phase.** In this phase, universal on-demand password service has three meanings: (1) The server and the RC authenticated each other; (2) The RC will help the server to authenticate the legal user. (3) The RC will help the legal user to authenticate the server. And the universal on-demand password service phase has two main functions: (1) The user can enjoy the login service using ODP; (2) The user can enjoy the secure session service between the user and the server. This concrete process is presented in the following Fig. 3.
Step 1. If Alice wishes to enjoy one of the universal on-demand password service with S_i,she just only opens the website of the service provided by some server and waits the ODP. The background computing device will do the followign tasks: (1) Select random a and compute $T_a(x)$, $K_{A-RC} = T_aT_k(x)$,$H_A = H(phone_{NO}||ID_{S_i}||T_a(x))$ and

$C_1 = E_{K_{A-RC}}(Phone_{NO}||ID_{S_i}||H_A)$;(2) Send $m_1 = \{T_a(x), C_1\}$ to S_i where she wants to get the servers service.

Step 2. After receiving the message $m_1 = \{T_a(x), C_1\}$ from Alice, Si will do the following tasks to ask RC for helping Alice to authenticate itself and providing the ODP: S_i selects random r_i and computes $T_{r_i}(x)$ and $C_2 = H(ID_{S_i}||m_1||R||T_{r_i}(x))$.And then S_i sends the message m_2 to RC.

Step 3. Next, RC will help Alice to authenticate S_i and verify the temporary information by helping them to compute the session key (session service) or distribute the ODP (login service). After receiving the message $m_2 = \{ID_{S_i}, T_{r_i}(x), C_2, m_1\}$, RC will do the following tasks:

(1) Authenticate S_i: Based on ID_{S_i}, RC can compute $R' = H(ID_{S_i}||k)$.Then RC computes $C_2' = H(ID_{S_i}||m_1||R'||T_{r_i}(x))$ and check if $C_2'? = C_2$.If above equation holds, that means S_i is legal participant in this instance because only S_i owns R.

(2) Authenticate Alice: RC computes $K_{RC-A} = T_k T_a(x)$ and then uses K_{RC-A} to decrypt $D_{K_{RC-A}}(C_1)$.The RC computes $H_A' = H(Phone_{NO}||ID_{S_i}||T_a(x))$ and verifies if $H_A' = H_A$ holds. If above equation holds and uses the $Phone_{NO}$ to return some cipher text including ODP, that means Alice is a legal user in this instance because only a legal user can receive and retrive the cipher text. (3) Confirm S_i is the server that Alice wants to consult with: RC computes $K_{RC-A} = T_k T_a(x)$ and then decrypts C_2 to get $Phone_{NO}||ID_{S_i}||H_A$.Next, RC computes $H_A' = H(Phone_{NO}||ID_{S_i}||T_a(x))$.RC verifies $H_A'? = H_A$ and checks if ID_{S_i} in the C_1 equals to ID_{S_i} in plaintext or not. If holds,

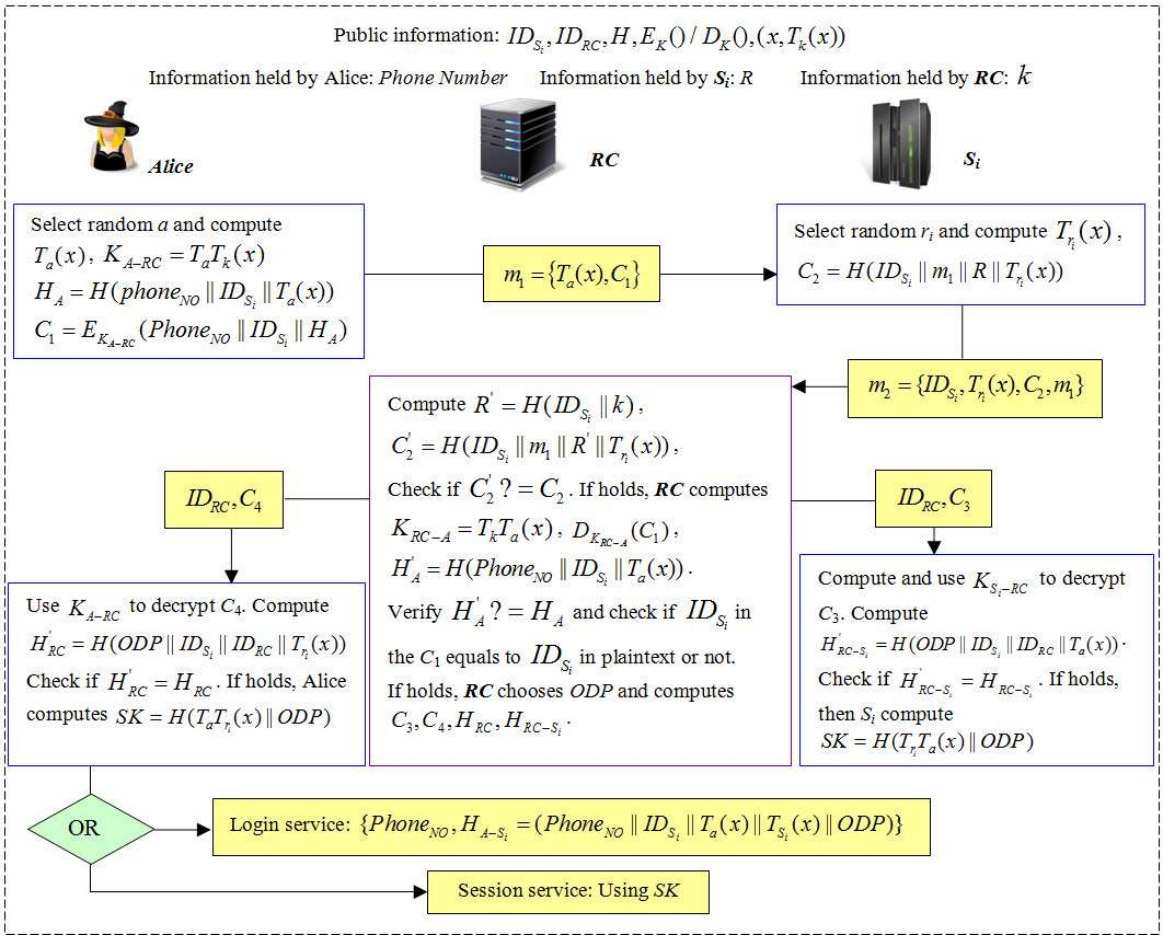

FIGURE 3. Authenticated On-demand Password phase for multi-server environment

that means S_i is the server that Alice wants to consult with.
(4) Help S_i and Alice to get the ODP and/or the session key: RC computes $C_3 = E_{K_{RC-S_i}}(ID_{RC}||ID_{S_i}||m_1||T_{r_i}(x)||ODP||H_{RC-S_i})$, $H_{RC-S_i} = H(ODP||ID_{S_i}||ID_{RC}||T_a(x))$, $C_4 = E_{K_{RC-A}}(ID_{RC}||ID_{S_i}||m_1||T_{r_i}(x)||ODP||H_{RC})$ and $H_{RC} = H(ODP||ID_{S_i}||ID_{RC}||T_{r_i}(x))$.
Then RC sends the message ID_{RC}, C_4 to Alice and sends the message ID_{RC}, C_3 to S_i.
Step 4. For Alice: After receiving the message ID_{RC}, C_4, Alice uses K_{A-RC} to decrypt C_4.Next Alice computes $H'_{RC} = H(ODP||ID_{S_i}||ID_{RC}||T_{r_i}(x))$.Check if $H'_{RC} = H_{RC}$.If holds, Alice computes $SK = H(T_aT_{r_i}(x)||ODP)$.Finally, Alice launches login service with messages $\{Phone_{NO}, H_{A-S_i} = (Phone_{NO}||ID_{S_i}||T_a(x)||T_{S_i}(x)||ODP)\}$ or session service with SK.
For S_i:After receiving the message ID_{RC}, C_3, S_i uses K_{S_i-RC} to decrypt C_3.Then S_i computes $H'_{RC-S_i} = H(ODP||ID_{S_i}||ID_{RC}||T_a(x))$ and checks if $H'_{RC-S_i} = H_{RC-S_i}$.If holds, then S_i computes $SK = H(T_{r_i}T_a(x)||ODP)$.

Remark 3.2. *If any authenticated process does not pass, the protocol will be terminated immediately. If the user only need one service (login or session service), the scheme will omit all another service process (login or session service). The implementation patterns of our proposed ODP scheme is more convenient, because user only need to draw some finger-swipe gesture for confirming the ODP is right or not without inputing ODP process.*

4. Security Analysis.

4.1. Security proof of the proposed scheme. (1) Mutual Authentication and key agreement

Definition 4.1. Mutual authentication and key agreement refers to two parties authenticating each other suitably and getting the session key simultaneously.
Theorem 4.1. *The proposed protocol can achieve mutual authentication and key agreement.*
Proof: In our proposed protocol we can divide the ID hiding authentication process into four steps:
(a) Alice authenticates RC: Because only RC has the secret k, RC can computes $K_{RC-A} = T_kT_a(x)$ which equals to $K_{A-RC} = T_aT_k(x)$. So if Alice decrypts C_4 to get the necessary information and check if $H'_{RC} = H_{RC}$. If above equation is equal, then that means Alice authenticates RC.
(b) RC and S_i authenticate each other: We can use the shared key R to achieve the task. Firstly, based on ID_{S_i}, RC can compute $R' = H(ID_{S_i}||k)$ by its private key k. Then RC computes $C'_2 = H(ID_{S_i}||m_1||R'||T_{r_i}(x))$ and checks if $C'_2 = C_2$. If above equation is equal, then that means RC authenticates S_i. After receiving the messages $\{ID_{RC}, C_3\}$, Si computes $C'_3 = H(ID_{RC}||ID_{S_i}||m_1||R||T_{r_i(x)})$ and chesks if $C'_3 = C_3$. If holds, we can say S_i authenticates RC.
(c) Alice authenticates S_i: If Alice already authenticates RC, then she can authenticate S_i based on the information $\{ID_{RC}||ID_{S_i}||m_1||R||T_{r_i(x)}||ODP||H_{RC}\}$, which were encrypted by RC in C_4. The trust flow is $Alice \rightarrow RC \rightarrow S_i$.
(d) RC helps S_i authenticate Alice: If S_i already authenticates RC, then it can authenticate Alice based on the information $\{ID_{RC}||ID_{S_i}||m_1||R||T_{r_i(x)}||ODP||H_{RC-S_i}\}$, which were encrypted by RC in C_3. The trust flow is $S_i \rightarrow RC \rightarrow Alice$.
As for the key agreement, after authenticating each other, the temporary $T_a(x), T_{r_i}(x), ODP$ and the $Phone_{NO}||ID_{S_i}||ID_{RC}$ were already authenticated by RC. So finally Alice and Si can make the key agreement simultaneously.

(2) Mutual Authentication and ODP Distribution

Definition 4.2. Mutual authentication and ODP distribution refers to two parties authenticating each other suitably and getting the ODP simultaneously.

Theorem 4.2. *The proposed protocol can achieve mutual authentication and ODP distribution.*

Proof: In brief, The mutual authentication and ODP distribution can be proof in some analogous way as section4.1(1). ODP was encrypted all the process with authenticated message in our proposed scheme.

(3) Impersonation attack

Definition 4.3. An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.

Theorem 4.3. *The proposed protocol can resist impersonation attack.*

Proof: An adversary cannot impersonate anyone of Alice, S_i and/or RC. The proposed scheme has already authenticated each other among Alice, S_i and RC, and pairwise mutual authentication (in 4.1.(1)) based on the secrets k, R and the nonces a, r_i. So there is no way for an adversary to have a chance to carry out impersonation attack.

(4) Man-in-the-middle attack

Definition 4.4. The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Theorem 4.4. *The proposed protocol can resist Man-in-the-middle attack.*

Proof: Because $C_i(1 \leq i \leq 4)$ contain the participants identities or $Phone_{NO}$, a man-in-the-middle attack cannot succeed.

(5) Replay attack

Definition 4.5. A replay attack is a form of network attack in which a valid data transmission is repeated or delayed maliciously or fraudulently.

Theorem 4.5. *The proposed protocol can resist replay attack.*

Proof: For any message among Alice, S_i and RC, and an adversary cannot start a replay attack against our scheme because there were the fresh nonces a, r_i in each session. If $T_a(x)$ and $T_{r_i}(x)$ 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 compute and modify $T_a(x)$, $T_{r_i}(x)$ and $C_i(1 \leq i \leq 4)$ correctly which is impossible.

(6) Known-key security

Definition 4.6. Known-key security is that a protocol can protect the subsequent session keys from disclosing even if the previous session keys are revealed by the intendant user.

Theorem 4.6. *The proposed protocol can achieve known-key security.*

Proof: Since the session key $SK = H(T_a T_{r_i}(x)||ODP) = H(T_{r_i} T_a(x)||ODP)$ is depended on the random nonces a, r_i and ODP, and the generation of nonces is independent in all sessions, an adversary cannot compute the previous and the future session keys when the adversary knows one session key. And in the secrets update phase, any session key is only used once, so it has known-key security attribute.

(7) Perfect forward secrecy

Definition 4.7. An authenticated key establishment protocol provides perfect forward secrecy if the compromise of both of the nodes secret keys cannot results in the compromise of previously established session keys.

Theorem 4.7. *The proposed protocol can achieve perfect forward secrecy.*

Proof: In the proposed scheme, the session key $SK = H(T_a T_{r_i}(x)||ODP) = H(T_{r_i} T_a(x)||$

ODP) is related with a, r_i and ODP, which were randomly chosen by Alice, the server S_i and the RC respectively. So any session key has not related with the secret key (such as k) of each of participants. Furthermore, because of the intractability of the CMBDLP and CMBDHP problem, an adversary cannot compute the previously established session keys.

(8) Session key security

Definition 4.8. A communication protocol exhibits session key security if the session key cannot be obtained without any long-term secrets. **Theorem 4.8.** *The proposed protocol can achieve session key security.*

Proof: In the authenticated key agreement phase, a session key SK is generated from a, r_i and ODP. These parameter values are different in each session, and each of them is only known by Alice and S_i. Whenever the communication ends between S_i and Alice, the key will immediately self-destruct and will not be reused. Therefore, assuming the attacker has obtained a session key, and Alice will be unable to use this session key to decode the information in other communication processes. Because the random point elements a and r_i are all generated randomly and are protected by the CMBDLP, CMBDHP, and the secure symmetric encryption, a known session key cannot be used to calculate the value of the next session key. Additionally, since the values a and r_i of the random elements are very large, attackers cannot directly guess the values a and r_i of the random elements to generate session key. Therefore, the proposed scheme provides session key security.

(9) Stolen smart phone attacks

Definition 4.9. Anyone gets the smart phone in some way to execute some kinds of attacks.

Theorem 4.9. *The proposed scheme can resist stolen smart card attacks.*

Proof: It is very clear that the proposed schemes security is based on the $Phone_{NO}$, so keeping smart phone secure is very important. In our scheme, we assume that a smart phone user can detect the lost phone as soon as possible, then he will use his ID card to cancel or retrieve his lost $Phone_{NO}$. Based on the record $\{IDCard, Phone_{NO}\}$ in RCs database and some mobile phone lock applications, and our scheme can minimize loss.

From the Table 2, we can see that the proposed scheme can provide secure session key agreement, perfect forward secrecy and so on. As a result, the proposed scheme is more secure and has much functionality compared with the recent related scheme.

Table 2. Security of our proposed protocol

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12
[22](2013)	Yes	Mutual	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Low	Yes
[23](2008)	Yes	Mutual	Yes	Yes	Yes	No	No	No	No	No	Low	No
[24](2009)	Yes	No	Yes	Yes	Yes	ID hiding	No	No	No	Yes	Low	No
[25](2009)	Yes	No	Yes	No	Yes	ID hiding	No	No	No	Yes	Low	No
Ours	Yes	Mutual	Yes	Yes	Yes	ID hiding	Yes	Yes	Yes	Yes	high	Yes

S1: Single registration; **S2**: Authentication; **S3**: No verification table; **S4**: Securely chosen password;
S5: Session key agreement; **S6**: Privacy protection for a user; **S7**: Freedom from time synchronization;
S8: Session key secrecy; **S9**: Perfect forward secrecy; **S10**: Resistance to replay attack;
S11: user experience; **S12**: Resistance to masquerading attack
Yes/No: Support/Not support the security **NN**: No need

Our proposed protocol can hold the security S1-S12, but the [22-25] have some defects. Our protocol is ID hiding, and [24, 25] assure ID hiding too, and [22-23] have no privacy protect at all. Furthermore, our scheme owns high-level user experience which is better than the others related literatures [22-25].

4.2. **Authentication proof based on the BAN logic [26].** For convenience, we first give the description of some notations (Table 3) used in the BAN logic analysis and define some main logical postulates (Table 4) of BAN logic.

TABLE 3. Notations of the BAN logic

Symbol	Definition
$P \mid\equiv X$	The principal P believes a statement X, or P is entitled to believe X.
$\#(X)$	The formula X is fresh.
$P \mid\Rightarrow X$	The principal P has jurisdiction over the statement X.
$P \lhd X$	The principal P sees the statement X.
$P \mid\sim X$	The principal P once said the statement X.
(X,Y)	The formula X or Y is one part of the formula (X,Y).
$\langle X \rangle_Y$	The formula X combined with the formula Y.
$\{X\}_Y$	The formula X is encrypted under the key K.
$(X)_Y$	The formula X is hash with the key K.
$P \overset{K}{\longleftrightarrow} Q$	The principals P and Q use the shared key K to communicate. The key K will never be discovered by any principal except P and Q.
SK	The session key used in the current session.

TABLE 4. Logical postulates of the BAN logic

Symbol	Definition	
$\dfrac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, P\{X\}_K}{P \mid\equiv Q \mid\sim X}$	The message-meaning rule	(R_1)
$\dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$	The freshness-conjuncatenation rule	(R_2)
$\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$	The nonce-verification rule	(R_3)
$\dfrac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$	The jurisdiction rule	(R_4)
$\dfrac{P \mid\equiv Q \mid\equiv (X,Y)}{P \mid\equiv Q \mid\equiv X}$	The belief rules	(R_5)
$\dfrac{P \mid\equiv Q \mid\sim (X,Y)}{P \mid\equiv Q \mid\sim X}$	The belief rules	(R_6)
Remark 3: Molecule can deduce denominator for above formulas.		

According to analytic procedures of BAN logic and the requirement of authentication protocol for WMSNs, our protocol should satisfy the following goals in Table 5:

First of all, we transform the process of our protocol to the following idealized form as Table 6.

According to the description of our protocol, we could make the following assumptions about the initial state, which will be used in the analysis of our protocol in Table 7.

TABLE 5. Goals of the proposed ODP scheme

Service	Goals
Session service	Goal 1. $Alice \mid\equiv \left(Alice \xleftrightarrow{SK} S_i\right)$; Goal 2. $Alice \mid\equiv S_i \mid\equiv \left(Alice \xleftrightarrow{SK} S_i\right)$; Goal 3. $S_i \mid\equiv \left(Alice \xleftrightarrow{SK} S_i\right)$; Goal 4. $S_i \mid\equiv Alice \mid\equiv \left(Alice \xleftrightarrow{SK} S_i\right)$;
Login service	Goal 5. $Alice \mid\equiv \left(Alice \xleftrightarrow{ODP} S_i\right)$; Goal 6. $Alice \mid\equiv S_i \mid\equiv \left(Alice \xleftrightarrow{ODP} S_i\right)$; Goal 7. $S_i \mid\equiv \left(Alice \xleftrightarrow{ODP} S_i\right)$; Goal 8. $S_i \mid\equiv Alice \mid\equiv \left(Alice \xleftrightarrow{ODP} S_i\right)$;

TABLE 6. Idealized form of our protocol

Idealized form
$(Alice \rightarrow S_i)m_1 : S_i \lhd T_a(x), \{Phone_{NO}, ID_{S_i}, (phone_{NO} \parallel ID_{S_i} \parallel T_a(x))\}_{Alice \xleftrightarrow{K_{A-RC}} RC}$
$(S_i \rightarrow RC)m_2 : RC \lhd ID_{S_i}, T_{r_i}(x), (ID_{S_i} \parallel m_1 \parallel R \parallel T_{r_i}(x)), m_1$
$(RC \rightarrow S_i)m_3 : S_i \lhd ID_{RC}, \{ID_{RC}, ID_{S_i}, m_1, T_{r_i}(x), ODP, (ODP \parallel ID_{S_i} \parallel ID_{RC} \parallel T_a(x))\}_{S_i \xleftrightarrow{K_{RC-S_i}} RC}$
$(RC \rightarrow Alice)m_4 : Alice \lhd ID_{RC}, \{ID_{RC}, ID_{S_i}, m_1, T_{r_i}(x), ODP, (ODP \parallel ID_{S_i} \parallel ID_{RC} \parallel T_{r_i}(x))\}_{Alice \xleftrightarrow{K_{RC-A}} RC}$

TABLE 7. Assumptions about the initial state of our protocol

Initial states	
$P_1 : Alice \mid\equiv \xrightarrow{T_k(x)} RC$	$P_2 : S_i \mid\equiv \xrightarrow{T_k(x)} RC$
$P_3 : S_i \mid\equiv S_i \xleftrightarrow{R} RC$	$P_4 : RC \mid\equiv S_i \xleftrightarrow{R} RC$
$P_5 : RC \mid\equiv Alice \mid\Rightarrow Phone_{NO}$	$P_6 : S_i \mid\equiv Alice \mid\Rightarrow Phone_{NO}$
$P_7 : Alice \mid\equiv \#(a)$	$P_8 : S_i \mid\equiv \#(r_i)$
$P_9 : Alice \mid\equiv RC \mid\Rightarrow Alice \xleftrightarrow{ODP} S_i$	$P_{10} : S_i \mid\equiv RC \mid\Rightarrow Alice \xleftrightarrow{ODP} S_i$
$P_{11} : Alice \mid\equiv Alice \xleftrightarrow{K_{A-RC}} RC$	$P_{12} : RC \mid\equiv Alice \xleftrightarrow{K_{A-RC}} RC$
$P_{13} : S_i \mid\equiv S_i \xleftrightarrow{K_{S_i-RC}} RC$	$P_{14} : RC \mid\equiv S_i \xleftrightarrow{K_{S_i-RC}} RC$

Based on the above assumptions, the idealized form of our protocol is analyzed as follows. The main steps of the proof are described as follows:

For m_2:

Because m_1 is the part of m_2, we view m_2 is the beginning of the proof. According to the message m_2 and $P_1, P_3, P_4, P_5, P_{11}, P_{12}$, and relating with R_1, we could get: $S_1 : RC| \equiv S_i| \sim m_2$

Based on the initial assumptions P_7, P_8, and relating with R_2, we could get: $S_2 : RC| \equiv \#m_2$

Combine $S_1, S_2, P_{11}, P_{12}, P_{13}, P_{14}$ and R_3, we could get: $S_3 : RC| \equiv S_i| \equiv \#ID_{S_i}, T_{r_i}(x), (ID_{S_i}||m_1||R||T_{r_i}(x))$,$S_4 : RC| \equiv Alice| \equiv \#Phone_{NO}, ID_{S_i}, (Phone_{NO}||ID_{S_i}||T_A(x))$

Based on R_5, we take apart S_3, S_4 and get: $S_5 : RC| \equiv S_i| \equiv \#ID_{r_i}$, $S_6 : RC| \equiv S_i| \equiv S_i \xleftrightarrow{R} RC$, $S_7 : RC| \equiv Alice| \equiv \#T_a(x)$, $S_8 : RC| \equiv Alice| \equiv Phone_{NO}$

Based on R_4 and P_3, P_{13}, and relating with S_5, we could get: $S_9 : RC| \equiv \#T_{r_i}(x)$

Based on R_4 and P_1, P_{13}, and relating with S_7, we could get: $S_{10} : RC| \equiv \#T_a(x)$

For m_3:

Based on m_3, and relating with P_2, P_{13} and R_1, we could deduce: $S_{11} : S_i| \equiv RC| \sim m_3$

Based on R_2 and P_8, we could get: $S_{12} : S_i| \equiv \#m_3$

Combine $S_{11}, S_{12}, P_{11}, P_{12}, P_{13}, P_{14}$ and R_3, we could get: $S_{13} : S_i| \equiv RC| \equiv m_3$

Based on $R_5, S_{12}, S_{13}, P_{13}, P_{14}$, we could deduce: $S_{14} : S_i| \equiv \#ODP$, $S_{15} : S_i| \equiv \#T_a(x)$
For m_4:
Based on m_4, and relating with P_1, P_{11} and R_1, we could deduce: $S_{16} : Alice| \equiv RC| \sim m_4$
Based on R_2 and P_7, we could get: $S_{17} : Alice| \equiv \#m_4$
Combine $S_{16}, S_{17}, P_{11}, P_{12}, P_{13}, P_{14}$ and R_3, we could get: $S_{18} : Alice| \equiv RC| \equiv m_4$
Based on $R_5, S_{16}, S_{17}, P_{11}, P_{12}$, we could deduce: $S_{19} : Alice| \equiv \#ODP$, $S_{20} : Alice| \equiv \#T_{r_i}(x)$
Combine:
Because the three-party $(Alice, S_i, RC)$ communicate each other just now, they confirm the other two-party are on-line. Moreover, since $SK = H(T_a T_{r_i}(x)||ODP)$ and based on $S_{14}, S_{15}, S_{19}, S_{20}, R_6$ with chaotic maps problems, we could get:
Goal 1. $Alice| \equiv (Alice \overset{SK}{\longleftrightarrow} S_i)$; Goal 2. $Alice| \equiv S_i| \equiv (Alice \overset{SK}{\longleftrightarrow} S_i)$;
Goal 3. $S_i| \equiv (Alice \overset{SK}{\longleftrightarrow} S_i)$; Goal 4. $S_i| \equiv Alice| \equiv (Alice \overset{SK}{\longleftrightarrow} S_i)$;
Goal 5. $Alice| \equiv (Alice \overset{ODP}{\longleftrightarrow} S_i)$; Goal 6. $Alice| \equiv S_i| \equiv (Alice \overset{ODP}{\longleftrightarrow} S_i)$;
Goal 7. $S_i| \equiv (Alice \overset{ODP}{\longleftrightarrow} S_i)$; Goal 8. $S_i| \equiv Alice| \equiv (Alice \overset{ODP}{\longleftrightarrow} S_i)$;
According to (Goal 1 Goal 8), we know that both Alice and S_i believe that a session key SK and ODP are shared between them.

5. **Efficiency Analysis.** Compared to RSA and ECC, Chebyshev polynomial computation problem offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings. In our proposed protocol, no time-consuming modular exponentiation and scalar multiplication on elliptic curves are needed. However, Wang [21] proposed several methods to solve the Chebyshev polynomial computation problem.
To be more precise, on an Intel Pentium4 2600 MHz processor with 1024 MB RAM, where n and p are 1024 bits long, the computational time of a one-way hashing operation, a symmetric encryption/decryption operation, an elliptic curve point multiplication operation and Chebyshev polynomial operation is 0.0005s, 0.0087s, 0.063075s and 0.02102s separately [18]. Moreover, the computational cost of XOR operation could be ignored when compared with other operations.
Table 8 shows performance comparisons between our proposed scheme and the literature of [22-25] in multi-server architecture. Therefore, as in Table 8 the concrete comparison data as follows:
The total computation cost of our proposed protocol is lower than the literatures [22]. The main reason is that the literatures [22] adopted modular exponentiation computation. At the same time, the literatures [22] cannot provide privacy protection for a user.
The total computation cost of our proposed protocol is higher than the literatures [23-25]. Furthermore, the communication rounds of our proposed protocol is superior to the literature [23][25] and is equal to the literature [24]. The reasons are: one reason is our protocol mainly adopts Chebyshev chaotic maps but the literatures [23-25] mainly adopts one way hash funciton. At the same time, Chebyshev chaotic maps has more attributes which leading to reduce communication rounds. Furthermore, from the perspective of security, our protocol is more secure than the literatures [23-25]. From the Table 2, we can see that the literatures [22-25] cannot resist many attacks and the literatures [24-25] cannot afford any authentication method. Therefore, as in Table 2 and Table 8, we can draw a conclusion that the proposed scheme has achieved the balance of efficiency, security and user experience.

TABLE 8. Efficiency of our proposed scheme

Phase		[22](2013)	[23](2008)	[24](2009)	[25](2009)	Ours
A		$2T_{hash} + 1T_{XOR}$	$2\ T_{hash} + 1T_{XOR}$	$5T_{hash} + 2T_{XOR}$	$8T_{hash} + 4T_{XOR}$	-
B		$1T_{hash}$	$1\ T_{hash}$	$1T_{hash}$	$1T_{hash}$	$1T_{hash}$
C		$2T_{hash} + 1T_{XOR} + 1T_{Exp}$	$1T_{hash} + 2T_{XOR}$	$6T_{hash} + 3T_{XOR}$	$7T_{hash} + 7T_{XOR}$	-
D1	User	$1T_{hash} + 1T_{Exp}$	$4T_{hash} + 3T_{XOR}$	$3T_{hash}$	$2T_{hash}$	$3T_{hash} + 2T_{CH} + 2T_{sym}$
	Server	$2T_{hash} + 2T_{Exp}$	$6T_{hash} + 7T_{XOR}$	$6T_{hash} + 3T_{XOR}$	$8T_{hash} + 6T_{XOR}$	$3T_{hash} + 2T_{CH} + 1T_{sym}$
	RC	$6T_{hash}$	$6T_{hash} + 5T_{XOR}$	0	$5T_{hash} + 7T_{XOR}$	$5T_{hash} + 2T_{CH} + 3T_{sym}$
	Total	$9T_{hash} + 3T_{Exp}$	$16T_{hash} + 15T_{XOR}$	$9T_{hash} + 3T_{XOR}$	$15T_{hash} + 13T_{XOR}$	$11T_{hash} + 6T_{CH} + 6T_{sym}$
D2	User	⊥	⊥	⊥	⊥	$4T_{hash} + 2T_{CH} + 2T_{sym}$
	Server					$4T_{hash} + 2T_{CH} + 1T_{sym}$
	RC					$5T_{hash} + 2T_{CH} + 3T_{sym}$
	Total					$13T_{hash} + 6T_{CH} + 6T_{sym}$
E		$2T_{hash} + 2T_{XOR}$	$2T_{hash} + 2T_{XOR}$	$4T_{hash} + 5T_{XOR}$	$4T_{hash} + 4T_{XOR}$	-
F		4 rounds	7 rounds	3 rounds	5 rounds	3 rounds

A: User registration **B**: Server registration **C**: Login phase
D1: Hiding identity authentication phase for session service **D2**: Authentication phase for login service
E: Password change phase **F**: Communication cost - : No calculated amount ⊥ : No support
T_{hash}: The time for executing the hash function;
T_{sym} : The time for executing the symmetric key cryptography;
T_{XOR}: The time for executing the XOR operation;
T_{Exp}: The time for a modular exponentiation computation;
T_{CH}: The time for executing the $T_n(x)$ mod p in Chebyshev polynomial using the algorithm in literature

6. **Conclusion.** This work provides a new universal and enhanced ODP scheme towards multi-server architecture. The core idea of the proposed scheme is to find a universal ODP scheme for meeting most of services based on the privacy of mobile phone. Be of great widespread significance in Mobile Internet to mobile users, especially for novice users. In other words, our enhanced ODP scheme is more convenient than the original ODP scheme proposed by Yahoo. Next, according to our discussion we proposed a suitable protocol which covers those goals and offered an efficient protocol that formally meets the proposed security definition. Finally, after comparing with related literatures (multi-server schemes) respectively, we found our proposed scheme has satisfactory security, efficiency and functionality. Therefore, our protocol is more suitable for practical applications. In the future, we will study the implementation of our scheme and other secure properties, such as increasing the number of participants, relating to quantum cryptography and so on.

REFERENCES

[1] How Yahoo's New On-Demand Passwords Feature Works, March 16, 2015. *https : //zeltser.com/yahoo − on − demand − passwords/?utm_source = tuicool*

[2] H. F. Zhu, A Provable One-way Authentication Key Agreement Scheme with User Anonymity for Multi-server Environment, *Ksii Transactions on Internet and Information Systems*, vol. 9, no. 2, pp. 811-829, Feb. 2015.

[3] J. Katz, P. MacKenzie, G. Taban, V. Gligor, Two-server password-only authenticated key exchange, *Applied Cryptography and Network Security*, Vol. 3531, pp. 1-16, 2005.

[4] C. Lee, C. Li, and C. Hsu, A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps, *Nonlinear Dyn*, vol. 73, pp. 125-132, 2013.

[5] E. Bresson, O. Chevassut and D. Pointcheval, Group Diffie-Hellman key exchange secure against dictionary attack, *Asiacrypt*, vol. 2501, pp. 497-514, 2002.

[6] H. Li, C.-K. Wu, J. Sun, A general compiler for password-authenticated group key exchange protocol, *Information Processing Letters*, pp.160-167, 2010.

[7] 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, pp. 2994-3006, 2012.

[8] H. Tseng H, R. Jan, W. Yang, A chaotic maps-based key agreement protocol that preserves user anonymity, *In: IEEE International Conference on Communications (ICC09)*, pp.1-6, 2009.

[9] M. Di Raimondo, R. Gennaro, Provably secure threshold password-authenticated key exchange, *J. Comput. System Sci*, vol.72, no. 6, pp. 978-1001, 2006.
[10] Mohan R, Partheeban N, Secure multimodal mobile authentication using one time password, *Informational Journal of Recent Technology and Engineering*, no.1,pp.17-25,2012..
[11] Y. Huang, Z. Huang, H. R. Zhao, X. J. Lai, A new one-time password method, *Informational Conference on Electronic Engineering and Computer Science*, no.1, pp.32-37,2013.
[12] F. Xu, X. Lv, Q. Zhou Q, Liu X, Self-updating one-time password authentication protocol for ad hoc network, *Transactions on Internet and Information Systems*, no.8,pp.256-265,2014.
[13] H. F. Zhu, One-time identitypassword authenticated key agreement scheme based on biometrics, *Security Comm. Networks*, 2015.
[14] L. H. Li, I. 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, pp. 1498-1504, 2001.
[15] 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, pp. 13-22, 2003.
[16] J. L. Tsai, Efficient multi-server authentication scheme based on one-way hash function without verification table, *Comput Secur*, vol. 27, no. 34, pp.115-121, 2008.
[17] S. P. Ravi, C. D. Jaidhar, T. Shashikala, Robust Smart Card Authentication Scheme for Multi-server Architecture, *Information Processing Letters*, vol. 72, Issue 1, pp. 729-745, 2013.
[18] L, Kocarev, and S. Lian, Chaos-Based Cryptography: Theory, Algorithms and Applications, pp. 53-54, 2011.
[19] S. P. Ravi, C. D. Jaidhar, and T. Shashikala, Robust Smart Card Authentication Scheme for Multi-server Architecture, *Wireless Pers Commun*, vol. 72, pp. 729-745, 2013.
[20] X. Wang, and J. Zhao, An improved key agreement protocol based on chaos, *Commun. Nonlinear Sci. Numer. Simul*, vol. 15, pp. 4052-4057, 2010.
[21] L. Zhang, Cryptanalysis of the public key encryption based on multiple chaotic systems, *Chaos Solitons Fractals*, vol. 37, no. 3, pp. 669-674, 2008.
[22] 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, *J Supercomput*, vol. 66, no. 2 , pp. 1008-1032, 2013.
[23] J. L. Tsai, Efficient multi-server authentication scheme based on one-way hash function without verification table, *Comput Secur*, vol. 27, no. 34, pp. 115-121, 2008.
[24] Y. P. Liao, S. S. Wang, A secure dynamic ID based remote user authentication scheme for multiserver environment, *Comput Stand Interfaces*, vol. 31, no. 1, pp. 24-29, 2009.
[25] H. C. Hsiang, W. K. Shih, Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment, *Comput Stand Interfaces*, vol. 31, no. 6, pp. 1118-1123, 2009.
[26] M. Burrows, M. Abadi, R. Needham, A logic of authentication, *ACM Trans. Comput. Syst*, no. 8, pp. 18-36, 1990.