International Journal of Security and Its Applications
Vol. 9, No. 5 (2015), pp. 255-268
http://dx.doi.org/10.14257/ijsia.2015.9.5.25

An Improved Anonymous Remote user Authentication Scheme with Key Agreement based on Dynamic Identity

Yajuan Shi[1], Han Shen[2], Yuanyuan Zhang[3] and Jianhua Chen[4]

[1,2,3,4]*School of Mathematic and Statistics, Wuhan University, Wuhan, Hubei, China*
[1]*shiyj_ecc@163.com,*[2]*Hjmshenhan_ecc@163.com,* [3]*circle0519@hotmail.com*

Abstract

To keep the pace with the development of internet technology, remote user authentication techniques become more and more important to protect user's privacy. Recently, Kumari, et al., presented an improved remote user authentication scheme with key agreement based on dynamic-identity using smart card. This scheme allows legal users to change the password at his will without the need to connect the server. They claimed that their scheme could resist smart card stolen or loss attack, user impersonation and server masquerading attack, and provide user anonymity and untraceability and so on. However, our research indicates that their scheme is completely unsafe. Furthermore, the scheme can't provide the proper mutual authentication. In this manuscript, we will propose a new scheme, which can withstand those attacks mentioned above and provide the perfect user anonymity and forward secrecy. Security analysis makes it clear that the improved scheme apparently is more secure and practical.

Keywords: *key agreement, dynamic-identity, user anonymity and untraceability, smart card*

1. Introduction

With the rapid development of network technology, remote user authentication has become an indispensable part of life to access to the worthy resources, which are provided by the host across the network by the remote systems. And before having the access to the services, people should be verified to be a legal user through the authentication of the remote system. Otherwise, an attacker could pretend to be a legal user to log in the system and get the resources. That is, only the legal user through the authentication of the remote system could have the access to the service, or an attacker could easily log in the system. As a result, researchers pay more attention on the secured issues and users' authentication.

The authentication techniques are essential to guarantee the users' legality. In 1981, Lamport [1] had come-up with a remote authentication based on password Table to authenticate the right of logging in the system. Later, many improved schemes are proposed on the security and efficiency [2-9]. However, those schemes need a Table of passwords or some values related to password stored by the server to complete the authentication. Once an adversary got the Table, the system would be partly or completely broken and users would suffer a lot.

To avoid the verified Table [8, 10, 11], researchers proposed some schemes based on static ID of users' identities which could widely leak the information of the legal users. But adversary may obtain the ID and other massages to disguise as a user to log into the remote systems. And many static ID-based remote user authentications can't provide users with the convenience of password change or verify the validity of the login requests without any verify Table. To overcome these risks and improve the efficiency and security, many applications and researches [12-21] based on dynamic ID have been done. And owing to the features of portability, low cost, cryptographic and computational

ISSN: 1738-9984 IJSIA

capacity, the smart cards are used in the scheme of authentication on a large scale.

In 2004, an authentication scheme based on a dynamic ID was proposed by Das, *et al.*, and they claimed that their scheme was secure to resist ID-theft, replay attacks and insider attack. However, Wang, *et al.*, [11] pointed out that the Das, *et al.*, scheme didn't achieve mutual authentication and dependence of password, and could not resist impersonate server attack. Therefore, they advanced a new scheme to strengthen the password authentication and provide mutual authentication in 2009. But many researches [22-25] made it clear that the improved scheme was vulnerable .In 2009, Chang, *et al.*, [22, 23] demonstrated that the scheme proposed by Wang wasn't efficient and secure because the attacker can be verified by the server and select an identity at his will. Then they provided a new scheme based on a smart card to complete the mutual authentication without any verified Table and they claimed that the scheme could provide untraceability and convenience of password update.

In 2013, Kumari, *et al.*, [26] proposed an improved user authentication scheme with key agreement, then they pointed out that the scheme of Chang, *et al.*, could not resist off-line password guessing attack, user impersonation attack, server masquerading attack, insider attack and so on. They showed that once smart card of any user was lost, the password of every legal user in the Chang, *et al.*, scheme system will be at stake. With the information of any smart card, the adversary could pretend to be any user in this system and get the service of the server successfully. What's more, there were several loopholes in password change phase and no verification mechanism existed in smart card. Besides, the scheme didn't provide any session key agreement. Then Kumari, *et al.*, presented an improved scheme and they claimed that the scheme could resist the smart card loss attack, impersonation attack, sever masquerading attack and provide forward secrecy, user anonymity and untraceability and so on.

In this article, however, we illustrate that Kumari, *et al.*, scheme is still vulnerable to the smart card stolen or loss attack, forge attack and even fail to provide the forward secrecy and so on. The rest organization of the article is arranged as follows: Section 2 reviews Kumari *et al.*, scheme. The cryptanalysis of Kumari, *et al.*, scheme is shown in Section 3. Section 4 gives the details of our new proposed scheme. Section 5 makes the security analysis of the proposed scheme. Section 6 compares the performance and efficient of new scheme. At last, the conclusion of this paper will be given in Section7.

2. Review of Kumari, *et al.*, Scheme

In this part, we review Kumari, *et al.*, scheme, which consists of four phases: the registration phase, the login phase, authentication phase and password change phase. The detail steps will be shown as follows. The notations used in the whole literature are indicated in Table 1.

Table 1. Notations

Notations			
U_i / U_e	A system user/an attacker E	$\|\|$	A concatenation operation
S_i	The remote server	SC	Smart card
ID_i, Pw_i, Pw_{new}	U_i's identity, password, new password	r_i	Unique random number assigned to U_i by S_i
CID_i	U_i 's dynamic identity	r	A random number selected by the smart card
T_1, T_2, T_3	Timestamps	$\oplus$	An XOR operation
$h(.)$	A secure one-way hash function	$x(y)$	A secret key(number) of server

2.1. Registration Phase

In this phase, we can know that if a user U_i would like to become a legal user of this system S_i, U_i should carry out the following steps.

1) The user U_i selects identity ID_i and password PW_i and chooses a random number n. Then U_i computes $R_i = h(n \| PW_i)$ and sends $\{ID_i, R_i\}$ to S_i via a secure channel.
2) After receiving $\{ID_i, R_i\}$, the server S_i chooses a random number r_i for each user U_i, which means that r_i is different for every user. x is the private key of S_i and y is a secrete number of S_i.
3) Then S_i computes $TN_i = h(ID_i \| x) \oplus R_i$, $TY_i = r_i \oplus h(ID_i \| x)$, $TD_i = h(ID_i \| r_i \| R_i)$ and $TE_i = r_i \oplus h(y \| x)$. Then S_i stores $\{TY_i, TD_i, TE_i, h\}$ into smart card and issues {smart card, TN_i} to the user U_i via a secure channel.
4) On receiving {smart card, TN_i} from the server S_i, the user U_i computes $A_i = (ID_i \| PW_i) \oplus n$, $TM_i = TN_i \oplus n$ and stores $\{A_i, TM_i\}$ into smart card.

The registration phase of Kumari *et al.*, scheme is showed in Figure 1.

Registration phase

User (U_i)		Server
Choose ID_i, PW_i, n Compute $R_i = h(n \| PW_i)$	ID_i, R_i →	Server private key : x Server's secret number: y Select a random number r_i Compute $TN_i = h(ID_i \| x) \oplus R_i$ $TY_i = r_i \oplus h(ID_i \| x)$ $TD_i = h(ID_i \| r_i \| R_i)$ $TE_i = r_i \oplus h(y \| x)$
Compute $A_i = (ID_i \| PW_i) \oplus n$ $TM_i = TN_i \oplus n$ Store A_i, TM_i into the smart card	← Issue the smart card and TN_i	Store $\{TY_i, TD_i, TE_i, h\}$ into the smart card

Figure 1. The Registration Phase of Kumari, *et al.*, Scheme

2.2. Login phase

When user U_i wants to get the service from S_i, he should perform the following steps.

1) The user U_i inputs identity ID_i and password PW_i, then the smart card SC computes $n = A_i \oplus (ID_i \| PW_i)$, $R_i = h(n \| PW_i)$, $h(ID_i \| x) = TM_i \oplus R_i \oplus n$, $r_i = TY_i \oplus h(ID_i \| x)$ and checks whether the equation $TD_i ? = h(ID_i \| r_i \| R_i)$ holds or not.
2) If not, SC will drop the session. If it repeats thrice then SC gets blocked and U_i is required to enter PUK to SC.
3) If holds, SC will compute $h(y \| x) = r_i \oplus TE_i$, $TN_i = TM_i \oplus n$ and gets the current time T_1.
4) SC computes $CID_i = ID_i \oplus h(N_i \| r_i \| T_1)$, $TN_i' = TN_i \oplus h(r_i \| T_1)$, $TB_i = TN_i \oplus R_i$, $TC_i = h(TN_i \| r_i \| TB_i \| T_1)$, $TF_i = r_i \oplus (h(y \| x) \| T_1)$ and sends $\{CID_i, TN_i', TC_i, TF_i, T_1\}$ to S_i via a public channel.

2.3. Authentication Phase

When S_i gets the message $\{CID_i, TN_i', TC_i, TF_i, T_1\}$ from U_i, S_i will play the detail steps as follows to finish the authentication phase and key agreement phase.

1) S_i gets the current time T_2 and checks whether T_1 is valid or not, which means

$T_2 - T_1 \le \Delta T$ .If T_1 isn't valid, S_i rejects all login requests and drops this phase.

2) If T_1 is valid, S_i continues to compute $r_i = TF_i \oplus (h(y \| x) \| T_1)$, $TN_i = TN_i' \oplus h(r_i \| T_1)$, $ID_i = CID_i \oplus (h(T_1 \| N_i \| r_i)$, $TB_i^* = h(ID_i \| x)$ and checks whether the equation $TC_i ? = h(TN_i \| r_i \| TB_i^* \| T_1)$ holds or not.
3) If holds, S_i gets the current time T_3 and computes $A = h(TB_i^* \| r_i \| T_3)$ .Then he sends $\{A, T_3\}$ to the user U_i .
4) After obtaining the $\{A, T_3\}$ from S_i, SC checks the validity of T_3 .If T_3 is valid, the smart card will check the equation $A ? = h(TB_i \| r_i \| T_3)$ .If holds, the user and server complete the mutual authentication. Otherwise, the session will be terminated by S_i .
5) Finally, the user U_i and the server S_i negotiate the session key. U_i computes the value of session key $SK = h(TB_i \| r_i \| T_1 \| T_3 \| h(y \| x))$ and the server S_i computes the value of session key $SK^* = h(TB_i^* \| r_i \| T_1 \| T_3 \| h(y \| x))$ respectively.

The login and authentication phases of Kumari *et al.*, scheme are summarized in Figure 2.

User (U_i)		Server
Input ID_i, PW_i Compute $n = A_i \oplus (ID_i \| PW_i)$ $R_i = h(n \| PW_i)$ $h(ID_i \| x) = TM_i \oplus R_i \oplus n$ $r_i = TY_i \oplus h(ID_i \| x)$ Check $TD_i ? = h(ID_i \| r_i \| R_i)$ Compute $h(y \| x) = r_i \oplus TE_i$ $TN_i = TM_i \oplus n$ gets the current time T_1 Compute $CID_i = ID_i \oplus h(N_i \| r_i \| T_1)$ $TN_i' = TN_i \oplus h(r_i \| T_1)$ $TB_i = TN_i \oplus R_i$ $TC_i = h(TN_i \| r_i \| TB_i \| T_1)$ $TF_i = r_i \oplus (h(y \| x) \| T_1)$	$\xrightarrow{\{CID_i, TN_i', TC_i, TF_i, T_1\}}$	gets the current time T_2 Check $T_2 - T_1 \le \Delta T$ Compute $r_i = TF_i \oplus (h(y \| x) \| T_1)$ $TN_i = TN_i' \oplus h(r_i \| T_1)$ $ID_i = CID_i \oplus h(TN_i \| r_i \| T_1)$ $TB_i^* = h(ID_i \| x)$ $TC_i ? = h(TN_i \| r_i \| TB_i^* \| T_1)$ gets the current time T_3 Compute $A = h(TB_i^* \| r_i \| T_3)$
Check T_3 $A ? = h(TB_i \| r_i \| T_3)$	$\xleftarrow{\{A, T_3\}}$	
Session key $SK = h(TB_i \| r_i \| T_1 \| T_3 \| h(y \| x))$	$\longleftrightarrow$	Session key $SK^* = h(TB_i^* \| r_i \| T_1 \| T_3 \| h(y \| x))$

Figure 2. The Login and Authentication Phases of Kumari, *et al.*, Scheme

2.4. Password Change Phase

If the user U_i wants to change his password in the system, he must take such steps as follows.

1) U_i inserts his smart card into the device and inputs his identity ID_i and password PW_i into the smart card.
2) Then SC computes $n = A_i \oplus (ID_i \| PW_i)$, $R_i = h(n \| PW_i)$, $h(ID_i \| x) = TM_i \oplus R_i \oplus n$, $r_i = TY_i \oplus h(ID_i \| x)$ and checks whether the equation $TD_i ? = h(ID_i \| r_i \| R_i)$ holds or not.
3) If holds, SC reminds the user of entering the new password PW_i^{new} and computes the

values of $R_i^{new} = h(n \| PW_i^{new})$, $A_i^{new} = h(ID_i \| PW_i^{new}) \oplus n$, $M_i^{new} = M_i \oplus R_i \oplus R_i^{new}$ and $TD_i^{new} = h(ID_i \| r_i \| R_i^{new})$.

4) Finally, SC replaces the old $\{A_i, TD_i, TM_i\}$ with $\{A_i^{new}, TD_i^{new}, TM_i^{new}\}$ respectively.

3. Cryptanalysis of Kumari, *et al.*, Scheme

Kumari, *et al.*, claimed that their proposed scheme can resist smart card loss attack, user impersonation, the server masquerading attack and so on. Besides, they could also provide user anonymity and untraceability. However, we find that their system actually fails to resist attacks mentioned above and can't provide user anonymity and untraceability. The detail steps of those attacks will be shown as follows.

3.1. Smart Card Stolen or Loss Attack

1) The attacker E obtains $\{A_e, TM_e, TY_e, TD_e, TE_e\}$ from his own smart card [27, 28] and then computes $n_e = A_e \oplus (ID_e \| Pw_e)$, $R_e = h(n_e \| Pw_e)$, $h(ID_e \| x) = TM_e \oplus R_e \oplus n_e$, $r_e = h(ID_e \| x) \oplus TY_e$, $h(y \| x) = r_e \oplus TE_e$, so attacker E can obtain the system value of $h(y \| x)$.
2) When the legal user U_i logins the system and sends login request message $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1\}$.Then attacker E can intercept the login request massage $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1\}$ and computes $r_i = TF_i \oplus (h(y \| x) \| T_1)$, $TN_i = TN_i^{'} \oplus h(r_i \| T_1)$, $ID_i = CID_i \oplus h(TN_i \| r_i \| T_1)$ and $TE_i = r_i \oplus h(y \| x)$,which $h(y \| x)$ is computed from step (1).
3) Then we can know $\mathrm{H}: \{ID_i, r_i, TN_i, TE_i, h(y \| x)\}$ of every legal user U_i from those computations. No matter what password is, $\{ID_i, r_i, TE_i, h(y \| x)\}$ are unchanged for each U_i and TN_i is fixed before U_i 's passwords changed.
4) When U_i 's smart card was stolen or lost, the attacker E obtains the information $\{A_i, TM_i, TY_i, TD_i, TE_i\}$ and the attackers searches TE_i in $\mathrm{H}: \{ID_i, r_i, TN_i, TE_i, h(y \| x)\}$. Then the attackers can get $\{ID_i, r_i, TN_i\}$ of users.
5) The attackers computes $n_i = TM_i \oplus TN_i$, $(ID_i \| Pw_i) = A_i \oplus n_i$ and the attackers obtains ID_i from step(3),then attacker can get Pw_i from $(ID_i \| Pw_i) = A_i \oplus n_i$.

3.2. User Impersonation

If user U_i ' smart card was stolen or lost, from section 3.1, the attacker E can obtain Pw_i , n_i , TM_i , $R_i = h(n_i \| PW_i)$ and then computes $h(ID_i \| x) = TM_i \oplus R_i \oplus n_i$ .As we know, for each user U_i ,the value of $h(ID_i \| x)$ is unchanged, so after user U_i get a new smart card with the same ID_i, the attacker can also obtain $\{ID_i, r_i, TE_i, h(y \| x), TN_i\}$ by intercepting previous message $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1\}$ and pretends to be user U_i to login the system without the new smart card, the detail steps are shown as follows.

1) The attacker computes $CID_i^* = ID_i \oplus h(TN_i \| r_i \| T_1)$, $TN_i^* = TN_i \oplus h(r_i \| T_1)$, $TB_i = h(ID_i \| x)$, $TC_i^* = h(TN_i \| r_i \| TB_i \| T_1)$ and $TF_i^* = r_i \oplus (h(y \| x) \| T_1)$,which $h(ID_i \| x)$ is already known. Then attacker sends $\{CID_i^*, TN_i^*, TC_i^*, TF_i^*, T_1\}$ to S_i .

2) When S_i receives the message $\{CID_i^*, TN_i^*, TC_i^*, TF_i^*, T_1\}$ from the attacker, S_i gets the current time T_2 and checks whether T_1 is valid, which means $T_2 - T_1 \le \Delta T$ .If T_1 isn't valid, S_i rejects all login requests and drops this phase.
3) If T_1 is valid, S_i computes the values of $r_i = TF_i^* \oplus (h(y \| x) \| T_1)$, $TN_i = TN_i^* \oplus h(r_i \| T_1)$, $ID_i = CID_i^* \oplus h(TN_i \| r_i \| T_1)$, $TB_i^* = h(ID_i \| x)$ and checks whether the equation $TC_i^* ? = h(TN_i \| r_i \| TB_i^* \| T_1)$ holds or not.
4) As we already know, $TC_i^* = h(TN_i \| r_i \| TB_i \| T_1)$ and the equation $TB_i = h(ID_i \| x) = TB_i^*$ holds, and then we can get $TC_i^* = h(TN_i \| r_i \| TB_i^* \| T_1)$. S_i gets the current time T_3 and computes $A = h(TB_i^* \| r_i \| T_3)$,and then S_i sends $\{A, T_3\}$ to SC. And the attacker E has successfully login the system as a legal user and the session key is $SK^{**} = h(TB_i \| r_i \| T_1 \| T_3 \| h(y \| x))$.

3.3. Server Masquerading Attack

The attacker gets $\{h(ID_i \| x), h(y \| x)\}$ by using the method mentioned above in section 3.1 and 3.2.

1) When the user U_i sends the login request message $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1\}$ in the public channel, the attacker can eavesdrop the login message and computes the values of $r_i = TF_i \oplus (h(y \| x) \| T_1)$, $TN_i = TN_i^{'} \oplus h(r_i \| T_1)$, $ID_i = CID_i \oplus h(TN_i \| r_i \| T_1)$ and $TB_i^* = h(ID_i \| x)$,which $h(ID_i \| x)$ is already known from section 3.2.
2) The attacker gets the current time T_3 and computes $A = h(TB_i^* \| r_i \| T_3)$ .Then he sends $\{A, T_3\}$ to SC.
3) When U_i receives the message from the attacker, he checks T_3 and verify the equation $A ? = h(TB_i \| r_i \| T_3)$ .As we know $TB_i = h(ID_i \| x) = TB_i^*$, then the equation will hold.
4) Finally, the user and the attacker complete the authentication, and the user computes the session key $SK = h(TB_i \| r_i \| T_1 \| T_3 \| h(y \| x))$ and the server computes the session key $SK^* = h(TB_i^* \| r_i \| T_1 \| T_3 \| h(y \| x))$ respectively.

3.4. User's Identity is Traceable

1) The attacker E obtains $\{A_e, TM_e, TY_e, TD_e, TE_e\}$ from his own smart card and then he computes $n_e = A_e \oplus (ID_e \| Pw_e)$, $R_e = h(n_e \| Pw_e)$, $h(ID_e \| x) = TM_e \oplus R_e \oplus n_e$, $r_e = h(ID_e \| x) \oplus TY_e$, $h(y \| x) = r_e \oplus TE_e$,so attacker E can easily get the system value of $h(y \| x)$.
2) When the legal user U_i logins the system and sends login request message $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1\}$ to the server, then attacker E can intercept the login request massage$\{CID_i, TN_i^{'}, TC_i, TF_i, T_1\}$and computes $r_i = TF_i \oplus (h(y \| x) \| T_1)$, $TN_i = TN_i^{'} \oplus h(r_i \| T_1)$, $ID_i = CID_i \oplus h(TN_i \| r_i \| T_1)$ .Then he can continue to compute $TE_i = r_i \oplus h(y \| x)$,which $h(y \| x)$ is computed from step (1).
3) Then we know $\mathrm{H}: \{ID_i, r_i, TN_i, TE_i, h(y \| x)\}$ of each user U_i . No matter what

password is, $\{ID_i, r_i, TE_i, h(y \| x)\}$ are unchanged for each U_i .So the attacker can get every user U_i 's identity ID_i in the system.

3.5. Lack of the Forward Secrecy

From section 3.1 and 3.2, the attacker E can obtain the values of $\{ID_i, r_i, TE_i, h(y \| x), TN_i\}$ and gets $\{h(ID_i \| x), h(y \| x)\}$ .If attacker E had intercepted the message $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1\}$ and $\{A, T_3\}$ every time, he could get previous session key by computing the value of $SK^{**} = h(h(ID_i \| x) \| r_i \| T_1 \| T_3 \| h(y \| x))$.

4. The Proposed Scheme

In this part, we proposed a new scheme to resist those attacks, which consists of four phases: the registration phase, the login phase, authentication phase and password change phase. The detail steps will be shown as follows.

4.1. Registration Phase

In this phase, we can know that if a user U_i would like to become a legal user of this system S_i , U_i should carry out the following steps.

Registration phase

User (U_i)		Server
Choose ID_i , PW_i , n Compute $R_i = h(n \| PW_i)$	$\xrightarrow{ID_i, R_i}$	Server private key : x Server's secret number: y Select a random number r_i Compute $TN_i = h(h(ID_i) \| x) \oplus R_i$ $TY_i = r_i \oplus h(h(ID_i) \| x) \oplus R_i$ $TD_i = h(ID_i \| r_i \| R_i)$ $TE_i = r_i \oplus h(y \| x)$
Compute $A_i = h(ID_i \| PW_i) \oplus n$ $TM_i = TN_i \oplus n$ Store A_i, TM_i into the smart card	$\xleftarrow{\text{Issue the smart card and } TN_i}$	Store $\{TY_i, TD_i, TE_i, h\}$ into the smart card

Figure 3. The Proposed Scheme of Registration Phase

1) U_i chooses identity ID_i and password PW_i , and then selects a random number n .he computes $R_i = h(n \| PW_i)$ and sends $\{ID_i, R_i\}$ to S_i via a secure channel.
2) After receiving $\{ID_i, R_i\}$, S_i chooses a random number r_i for each user U_i , which means that r_i is different for every user. x is the private key of S_i and y is a secret number of S_i .
3) Then S_i computes the values of $TN_i = h(h(ID_i) \| x) \oplus R_i$, $TY_i = r_i \oplus h(h(ID_i) \| x) \oplus R_i$, $TD_i = h(ID_i \| r_i \| R_i)$ and $TE_i = r_i \oplus h(y \| x)$ .Then he stores $\{TY_i, TD_i, TE_i, h\}$ into smart card and issues{smart card , TN_i } to the user U_i via a secure channel.
4) On receiving{smart card, TN_i } from S_i ,the user U_i computes $A_i = h(ID_i \| PW_i) \oplus n$, $TM_i = TN_i \oplus n$ and stores $\{A_i, TM_i\}$ into smart card.

4.2. Login Phase

When user U_i wants to get the service from S_i, he should perform the following steps.

1) U_i inputs identity ID_i and password PW_i. Then the smart card SC computes the values of $n = A_i \oplus h(ID_i \| PW_i)$, $R_i = h(n \| PW_i)$ and $h(h(ID_i) \| x) = TM_i \oplus R_i \oplus n$, $r_i = TY_i \oplus h(h(ID_i) \| x) \oplus R_i$.
2) SC checks whether the equation $TD_i ? = h(ID_i \| r_i \| R_i)$ holds or not. If not, SC drops the session. If holds, SC computes $h(y \| x) = r_i \oplus TE_i$, $TN_i = TM_i \oplus n$ and gets the current time T_1.
3) SC computes $CID_i = h(ID_i) \oplus h(N_i \| r_i \| T_1)$, $TN_i^{'} = TN_i \oplus h(r_i \| T_1)$, $TB_i = TN_i \oplus R_i$ and chooses a random number r. Then SC can compute $Q_i = h(h(ID_i) \| r)$, $DS_i = TB_i \oplus Q_i$, $TC_i = h(TN_i \| r_i \| Q_i \| T_1)$, $TF_i = r_i \oplus (h(y \| x) \| T_1)$ and sends $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1, DS_i\}$ to S_i via a public channel.

Login phase and authentication phase

User (U_i)		Server
Input ID_i, PW_i		
Compute $n = A_i \oplus h(ID_i \| PW_i)$		
$R_i = h(n \| PW_i)$		
$TB_i = h(h(ID_i) \| x) = TM_i \oplus R_i \oplus n$		
$r_i = TY_i \oplus h(h(ID_i) \| x) \oplus R_i$		
Check $TD_i ? = h(ID_i \| r_i \| R_i)$		
Compute $h(y \| x) = r_i \oplus TE_i$		
$TN_i = TM_i \oplus n$		gets the current time T_2
gets the current time T_1		Check $T_2 - T_1 \le \Delta T$
Compute $CID_i = h(ID_i) \oplus h(N_i \| r_i \| T_1)$		Compute $r_i = TF_i \oplus (h(y \| x) \| T_1)$
$TN_i^{'} = TN_i \oplus h(r_i \| T_1)$		$TN_i = TN_i^{'} \oplus h(r_i \| T_1)$
$TB_i = TN_i \oplus R_i$		$h(ID_i) = CID_i \oplus h(TN_i \| r_i \| T_1)$
Generate a random nuber r	$\{CID_i, TN_i^{'}, TC_i, TF_i, T_1, DS_i\}$ $\longrightarrow$	$TB_i^* = h(h(ID_i) \| x)$
Compute $Q_i = h(h(ID_i) \| r)$		$Q_i^* = TB_i^* \oplus DS_i$
$DS_i = TB_i \oplus Q_i$		$TC_i ? = h(TN_i \| r_i \| Q_i^* \| T_1)$
$TC_i = h(TN_i \| r_i \| Q_i \| T_1)$		gets the current time T_3
$TF_i = r_i \oplus (h(y \| x) \| T_1)$		Compute $A = h(TB_i^* \| r_i \| T_3)$
Check T_3	$\{A, T_3\}$ $\longleftarrow$	
$A ? = h(TB_i \| r_i \| T_3)$		
Session key	$\longleftrightarrow$	Session key
$SK = h(TB_i \| r_i \| T_1 \| T_3 \| h(y \| x) \| Q_i)$		$SK^* = h(TB_i^* \| r_i \| T_1 \| T_3 \| h(y \| x) \| Q_i^*)$

Figure 4. The Proposed Scheme of Login and Authentication Phase

4.3. Authentication Phase

When S_i gets the message $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1, DS_i\}$ from U_i, S_i will play the detail steps as follows to finish the authentication phase and key agreement phase.

1) S_i gets the current time T_2 and checks whether T_1 is valid, which means $T_2 - T_1 \le \Delta T$. If T_1 isn't valid, S_i rejects all login requests and drops this phase.
2) If T_1 is valid, S_i continues to compute $r_i = TF_i \oplus (h(y \| x) \| T_1)$, $TN_i = TN_i^{'} \oplus h(r_i \| T_1)$, $h(ID_i) = CID_i \oplus h(TN_i \| r_i \| T_1)$, $TB_i^* = h(h(ID_i) \| x)$, $Q_i^* = TB_i^* \oplus DS_i$, and checks

whether the equation $TC_i ? = h(TN_i \| r_i \| Q_i^* \| T_1)$ holds or not.

3) If holds, S_i gets the current time T_3 and computes $A = h(TB_i^* \| r_i \| T_3)$ .Finally he sends $\{A, T_3\}$ to the user U_i .
4) After obtaining the $\{A, T_3\}$ from S_i, SC checks the validity of T_3 .If T_3 is valid, checks weather the equation $A ? = h(TB_i \| r_i \| T_3)$ holds or not further. If holds, the user and server complete the mutual authentication. Otherwise, the session will be terminated by S_i .
5) Finally, the user U_i and the server S_i negotiate the session key. The user U_i computes the session key $SK = h(TB_i \| r_i \| T_1 \| T_3 \| h(y \| x) \| Q_i)$ and the server computes the session key $SK^* = h(TB_i^* \| r_i \| T_1 \| T_3 \| h(y \| x) \| Q_i^*)$ respectively.

In the end, users can use the session key to encrypt or decrypt their massages for secret communication safely through a secure channel. Besides, the login and authentication phases of our proposed scheme are summarized in Figure 4.

4.4. Password Change Phase

If the user U_i wants to change his password in the system, he must take such steps as follows. And the proposed scheme of password change phase is summarized in Figure 5.

Password change phase

Input ID_i, PW_i to smart card
Compute $n = A_i \oplus h(ID_i \| PW_i)$
$R_i = h(n \| PW_i)$
$h(h(ID_i) \| x) = TM_i \oplus R_i \oplus n$
$r_i = TY_i \oplus h(ID_i \| x) \oplus R_i$
Check $TD_i ? = h(ID_i \| r_i \| R_i)$
enter the new password PW_i^{new}
Compute $R_i^{new} = h(n \| PW_i^{new})$
$A_i^{new} = h(ID_i \| PW_i^{new}) \oplus n$
$M_i^{new} = M_i \oplus R_i \oplus R_i^{new}$
$TY_i^{new} = TY_i \oplus R_i \oplus R_i^{new}$
$TD_i^{new} = h(ID_i \| r_i \| R_i^{new})$
Replace $\{A_i, TD_i, TM_i, TY_i\}$ with $\{A_i^{new}, TD_i^{new}, TM_i^{new}, TY_i^{new}\}$

Figure 5. The Proposed Scheme of Password Change Phase

1) Inserts his smart card into the device, and then inputs his identity ID_i and password PW_i into the smart card. Then SC computes the values of $n = A_i \oplus h(ID_i \| PW_i)$, $R_i = h(n \| PW_i)$, $h(h(ID_i) \| x) = TM_i \oplus R_i \oplus n$, $r_i = TY_i \oplus h(ID_i \| x) \oplus R_i$ and checks whether the equation $TD_i ? = h(ID_i \| r_i \| R_i)$ holds or not.
2) If holds, SC reminds the user of entering the new password PW_i^{new} .Then SC computes $R_i^{new} = h(n \| PW_i^{new})$, $A_i^{new} = h(ID_i \| PW_i^{new}) \oplus n$, $M_i^{new} = M_i \oplus R_i \oplus R_i^{new}$, $TY_i^{new} = TY_i \oplus R_i \oplus R_i^{new}$, $TD_i^{new} = h(ID_i \| r_i \| R_i^{new})$ and replaces the old $\{A_i, TD_i, TM_i, TY_i\}$ with $\{A_i^{new}, TD_i^{new}, TM_i^{new}, TY_i^{new}\}$ respectively.

5. Security Analysis of the Proposed Scheme

In this section, we will show that our scheme can overcome the drawbacks analyzed above and further can resist some other attacks. The details are shown in the following.

5.1. Users' Anonymity and Untraceability

We will show that any attacker can trace the identity ID_i of a user in the proposed scheme.

1) The attacker E obtains $\{A_e, TM_e, TY_e, TD_e, TE_e\}$ from his own smart card and then computes $n_e = A_e \oplus h(ID_e \| Pw_e)$, $R_e = h(n_e \| Pw_e)$, $h(h(ID_e) \| x) = TM_e \oplus R_e \oplus n_e$, $r_e = h(h(ID_e) \| x) \oplus TY_e \oplus R_e$, $h(y \| x) = r_e \oplus TE_e$, so attacker E can obtain the system value of $h(y \| x)$.
2) When the legal user U_i logins the system and sends login request message $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1\}$, the attacker E intercepts the massage $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1\}$ and continues to compute the values of $r_i = TF_i \oplus (h(y \| x) \| T_1)$, $TN_i = TN_i^{'} \oplus h(r_i \| T_1)$, $h(ID_i) = CID_i \oplus h(TN_i \| r_i \| T_1)$. So the attacker just can get $h(ID_i)$ instead of ID_i of a user in this system. Namely, this scheme can provide users' anonymity and untraceability.

5.2. Off-line Password Guessing Attack

Off-line password guessing attack means the attacker can use user's smart card to get the user's password off-line. In this scheme, the attacker stole a user's smart card. From the section 3.1, the attacker can get $\{n_i\}$ and computes $A_i \oplus n_i = h(ID_i \| PW_i)$. From the $h(ID_i \| PW_i)$, he can't guess the correct password without knowing ID_i.

5.3. Smart Card Stolen or Loss Attack

Suppose the attacker E obtains the smart card of any user, we will show that E can't get any useful information out of those extracted values. From section 5.1 and 5.2, we can know the values of $\{h(ID_i), TN_i, r_i, n_i\}$ from the attacks but not $\{ID_i, PW_i\}$, so the attackers can't compute $TB_i = h(h(ID_i) \| x)$ from the entities he has already known. Then he can't obtain the correct value of $DS_i = TB_i \oplus Q_i$ without correct value of TB_i. When the server receives the mock massage $\{CID_i, TN_i^{'}, TC_i^{**}, TF_i, T_1, DS_i^{**}\}$ from the attacker, the server will reject the login request because the equation $TC_i^{**} ?= TC_i^{*}$ won't hold with different TB_i. Therefore, the scheme can resist the smart card stolen or loss attack.

5.4. Resist Server Masquerading and user Impersonation Attack

If the attacker E wants to impersonate a legal user of the system, the attacker E needs to compute a correct login request $\{CID_i, TN_i^{'}, TC_i, TF_i, T_1, DS_i\}$. However, based on the analysis of section 5.3, the attacker can't pass the authentication equation of $TC_i^{**} = TC_i^{*}$ successfully without TB_i^{*}. So the scheme can resist the user impersonation attack. In order to masquerade server, the attacker should compute the valid value of $A = h(TB_i^{*} \| r_i \| T_3)$, but he can't get the private key x or TB_i. Therefore, the scheme can resist server masquerading attack.

5.5. Provides Forward Secrecy

Forward secrecy is a very important part of ensuring the security of users' information.

In the proposed scheme, the session key $SK = h(h(ID_i \| x) \| r_i \| T_1 \| T_3 \| h(y \| x) \| h(h(ID_i) \| r))$ is based on $\{ h(ID_i \| x), r_i, h(y \| x), h(h(ID_i) \| r) \}$, which means the adversary must know the value of $h(h(ID_i) \| r)$. Suppose the adversary can obtain $\{ h(ID_i \| x), r_i, h(y \| x), h(ID_i) \}$, but he still won't get the number r, which is generated randomly in every round. Therefore, attacker can't compute the previous session keys properly.

5.6. Resist Replay Attack

The improved scheme uses the current timestamps to resist the relay attack. Namely, upon receiving the login request message $\{ CID_i, TN_i^{'}, TC_i, TF_i, T_1, DS_i \}$ from users, the server checks the validity of T_1 immediately. Similarly, the user receives the response message $\{ A, T_3 \}$ from the server and then verifies the legality of T_3 firstly. If the timestamps was out of deadline, the server or users will reject those request messages. So, the scheme can resist replay attack.

5.7. Insider Attack

In the improved scheme, users transmit a nonce R_i instead of the plaintext password. To protect the password from insider attack, user U_i uses a random number n and submits the value of $R_i = h(n \| PW_i)$ .But insiders don't know both of $\{ n, PW_i \}$, this is, it is less likely to guess the two value in polynomial time. Therefore, the attacker doesn't have the chance to guess the probable password and test his guess right. Namely, this scheme can provide full resistance of insider attack.

5.8. Provides Mutual Authentication

In the proposed scheme, the server verifies the legal user by the method of checking the validity of equation $TC_i ? = h(TN_i \| r_i \| Q_i^* \| T_1)$ .On the contrary, the user verifies the equation $A ? = h(TB_i \| r_i \| T_3)$ to authenticate the server. By the way, based on the analysis of section 5.4, no one can pretend to be a legal user or server to deceive others. So, the scheme can provide proper mutual authentication.

5.9. Provides Session Key

In the improved scheme, the user U_i computes $SK = h(TB_i \| r_i \| T_1 \| T_3 \| h(y \| x) \| Q_i)$ and the server computes the session key $SK^* = h(TB_i^* \| r_i \| T_1 \| T_3 \| h(y \| x) \| Q_i^*)$ respectively at the end of every session, which is based on the fact that the equation $SK = h(h(ID_i \| x) \| r_i \| T_1 \| T_3 \| h(y \| x) \| h(h(ID_i) \| r))$ holds. Then the user can transmit any information he wants to the server and the server can also provide any service he can to the legal users confidentially. Based on the rigorous analysis of section 5.5, the scheme can provide forward secrecy. That is, the scheme can provide reasonably and secure session key.

6. Performance and Efficient Comparison

In this section, we will compare the proposed scheme with Kumari, *et al.*, Chang, *et al.*, and Chou, *et al.*, [29] on the aspects of performance and efficiency. The first Table will exhibit us that ours can resist all attacks mentioned in the Table 2.

The third Table will show the efficiency of those four schemes. In each scheme, there

are four parts, which compose of the registration phase, the login phase, authentication phase and the total computational complexity. Notations used in the Table 1 will be described as follows:

$t_{\oplus}$: The complexity of one-way hash function operation

$t_{h(.)}$:The complexity of XOR operation

t_{ce} : The complexity of checking an equation

From the Table 2, we can know that our proposed scheme is obviously more efficient than other four schemes in the login and authentication phase on the foundation of safety. What's more, our scheme can change password without the need to connecting the server and taking no consideration of internet's condition. Besides, registration operation only needs to be carried out one time for every legal user, but the login and authentication phase is more likely to take place one more times in a short time. Thus, ours is more convenient and practical than other three schemes.

Table 2. The Efficiency Comparison

	Chou *et al.*,	Chang *et al.*,	Kumari *et al.*,	Ours
registration phase	$5t_{\oplus}+8t_{h(.)}$	$t_{\oplus}+t_{h(.)}$	$5t_{\oplus}+5t_{h(.)}$	$6t_{\oplus}+8t_{h(.)}$
login phase	$3t_{\oplus}+6t_{h(.)}$	$3t_{\oplus}+4t_{h(.)}$	$10t_{\oplus}+8t_{h(.)}+t_{ce}$	$11t_{\oplus}+12t_{h(.)}+t_{ce}$
authentication phase	$14t_{\oplus}+20t_{h(.)}+3t_{ce}$	$6t_{\oplus}+10t_{h(.)}+2t_{ce}$	$3t_{\oplus}+7t_{h(.)}+2t_{ce}$	$4t_{\oplus}+8_{h(.)}+2t_{ce}$
total of login and authentication	$17t_{\oplus}+26t_{h(.)}+3t_{ce}$	$8t_{\oplus}+14t_{h(.)}+2t_{ce}$	$13t_{\oplus}+15t_{h(.)}+3t_{ce}$	$15t_{\oplus}+20t_{h(.)}+3t_{ce}$
Password change	$6t_{\oplus}+14t_{h(.)}+t_{ce}$	$8t_{\oplus}+12t_{h(.)}+2t_{ce}$	$6t_{\oplus}+6t_{h(.)}+t_{ce}$	$10t_{\oplus}+7t_{h(.)}+t_{ce}$
total complexity	$28t_{\oplus}+48t_{h(.)}+4t_{ce}$	$18t_{\oplus}+27t_{h(.)}+4t_{ce}$	$24t_{\oplus}+26t_{h(.)}+4t_{ce}$	$31t_{\oplus}+35t_{h(.)}+4t_{ce}$

In Table 3, we will display the security properties referring to security analysis among those four schemes.

Table 3. The Performance Comparison

	Chou, *et al.*,	Chang, *et al.*,	Kumari, *et al.*,	Ours
Users' anonymity and untraceability.	No	No	No	Yes
Off-line password guessing attack	No	No	Yes	Yes
Insider attack	No	No	Yes	Yes
Smart card stolen or loss attack	No	No	No	Yes
server masquerading attack	Yes	No	No	Yes
user impersonation attack	No	No	No	Yes
Provides forward secrecy	Yes	N/A	No	Yes
replay attack	Yes	Yes	Yes	Yes
proper mutual authentication	No	No	No	Yes
Provides session key	Yes	Yes	Yes	Yes
Provides secure session key	No	N/A	No	Yes
Total of No	6	7+2(N/A)	7	0

From the Table 3, our proposed scheme is more secure than other three schemes, which are similar with each other among the login and authentication phases. And ours can resist

all attacks mentioned above, but each of other three schemes has its own drawbacks.

7. Conclusions

In this study, we have reviewed the Kumari, *et al.*, scheme with basic secure analysis, which described an improved remote user authentication scheme with key agreement. Their scheme is more vulnerable to smart card stolen or loss attack, user impersonation and server masquerading attack. Besides, user's identity is traceable in their scheme and their scheme lacks of the forward secrecy. Then, we propose an improved scheme to resist those attacks and analyze the security of our scheme. After that, the advantages of our scheme have been shown by contrast of the performance and efficiency with other three schemes. It shows that our proposed scheme is more secure and applicable to practice.

References

[1] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, vol. 24, no. 11, **(1981)**, pp. 770-772.
[2] C. C. Chang and T. C. Wu, "Remote password authentication with smartcards", IEE Proceedings-E Computers and Digital Techniques, vol. 138, no. 3, **(1993)**, pp. 165-168.
[3] M. S. Hwang and L. H. Li, "New remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 46, no. 1,**(2000)**, pp. 28-30.
[4] Y. L. Tang, M. S. Hwang and C. C. Lee, "A simple remote user authentication scheme", Mathematical and Computer Modeling, vol. 36, Issues 1-2, **(2002)**, pp. 103–107.
[5] H. Y. Chien, J. K. Jan and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card", Computers and Security, vol. 21, no. 4, **(2002)**, pp. 372-375.
[6] C. L. Hsu, "Security of Chien, *et al.*, "Remote user authentication scheme using smart cards", Computer Standards and Interfaces, vol. 26, no. 3 , **(2004)**, pp. 167-169.
[7] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 1, **(2004)**, pp. 204-207.
[8] Y. F. Chang and C. C. Chang, "Authentication schemes with no verification Table", Applied Mathematics and Computation, vol. 167, no. 2, **(2005)**, pp. 820–832.
[9] H. C. Hsiang and W. K. Shih, "Weakness and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smartcards", Computer Communications, vol. 32, no. 4, **(2009)**, pp. 649-652.
[10] M. L. Das, A. Saxena and V. P. Gulati, "A Dynamic ID-based Remote User Authentication Scheme", IEEE Transactions on Consumer 630 Electronics, vol. 50, no. 2, **(2004)**, pp. 639-931.
[11] Y. Y. Wang, J. Y. Liu, F. X. Xiao and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," Computer Communications, vol. 32, no. 4, **(2009)**, pp. 583–585.
[12] R. Madhusudhan and R. C. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: A review", Journal of network and computer applications, vol. 35, no. 4, **(2012)**, pp. 1235-1248.
[13] C. C. Lee, T. H. Lin and R.X. Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards", Expert systems with applications, vol. 38. no. 11, **(2011)**, pp. 13863-13870.
[14] C. G. Ma, D. Wang and S. D. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards", International journal of communication systems, vol. 27, no. 10, **(2014)**, pp. 2215-2227.
[15] L. Xiong, J. W. Niu, Y. Liu, J. Liao and W. Liang, "Robust dynamic ID-based remote user authentication scheme using smart cards", International journal of ad hoc and ubiquitous computing, vol. 17, no. 4, **(2014)**, pp. 254-264.
[16] W. F. Tong, G. D. Li and L. X. Lei, "Cryptanalysis of a New Dynamic ID-based User Authentication Scheme to Resist Smart-Card-Theft Attack", Applied Mathematics & Information Sciences, vol. 8, no. 4, **(2014)**, pp. 1855-1858.
[17] M. K. Khan, S. Kumari, X. M.Wang and R. Kumar, "Security Issues of Chen *et al.*, dynamic ID-based authentication scheme", 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing (DASC), **(2014)** August 24-27, Dalian, China.
[18] J. Sand and W. B. Hsieh, "Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards", IET information security, vol. 8, no. 2, **(2014)**, pp. 104-113.
[19] X. Xu, Z. P. Jin, H. Zhang and P. Zhu, "A dynamic ID-based authentication scheme based on ECC for telecare medicine Information systems", Applied mechanics and materials, vol. 457-458, **(2014)**, pp. 861-866.

[20] R. Martinez-Pelaez, F. Rico-Novella, J. Forne and P. Velarde-Alvarado, "Security Improvement of Two Dynamic ID-based Authentication Schemes by Sood-Sarje-Singh", Journal of applied research and technology, vol. 11, **(2013)**, pp. 755-763.
[21] D. Z. Sun and Z. F. Cao, "On the Privacy of Khan *et al.*, Dynamic ID-Based Remote Authentication Scheme with User Anonymity", Cryptologia, vol. 37, no. 4, **(2013)**, pp. 345-355.
[22] Y. F. Chang and H. C. Chang, "Security of dynamic ID-based remote user authentication scheme," 2009 Fifth International Joint Conference on INC, IMS and IDC, **(2009)**, pp. 2108–2110.
[23] Y. F. Chang, W. L. Tai and H. C. Chang, "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update", International journal of communication systems, vol. 27, no. 11, **(2013)**, pp. 3430-3440.
[24] W. F. Tong and L. X. Lei, "An improved dynamic ID-based remote user authentication with key agreement scheme", Computers & Electrical engineering, vol. 38, no. 2, **(2012)**, pp. 381-387.
[25] E. J. Yoon and K. Y. Yoo, "On the Security of an Efficient and Secure Dynamic ID-Based Remote User Authentication Scheme", IEICE transaction on information and systems, vol. E95D, no. 6, **(2012)**, pp. 1684-1686.
[26] S. Kumari, M. K. Khan and X. Li, "An improved remote user authentication scheme with key agreement", Computers and Electrical Engineering, vol. 40, no. 6, **(2014)**, pp. 1997–2012.
[27] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Trans Comp, vol. 51, no. 5, **(2002)**, pp. 541-52.
[28] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis", Proceedings of advances in cryptology CRYPTO'99, **(1999)**, pp. 388–97.
[29] J. S. Chou, C. H. Huang, Y. S. Huang and Y. Chen, "Efficient two-pass anonymous identity authentication using smart card", IACR Cryptology ePrint Archive, 2013.402th, **(2013)**.

Authors

Yajuan Shi, is working as a MS candidate in applied mathematics in Wuhan University now. Her research interests include cryptographic protocol ,network security and cryptography.

Han Shen, received his BS degree in basic mathematics from Wuhan University, China, in 2011. After that, he received MS degree in applied mathematics in Wuhan University. Now, he is working as a PhD candidate in applied mathematics. His research interests include side channel attack and signature scheme.

Yuanyuan Zhang, received her MS degree in applied mathematics from Wuhan University, China, in 2012. Now, she is working as a PhD candidate in applied mathematics in Wuhan University. Her research interests include cloud computing security and cryptographic protocol.

Jianhua Chen, received his BS degree in applied mathematics from Harbin Institute of Technology, Harbin, China, in 1983 and received his MS and PhD degree in applied mathematics from Wuhan University, Wuhan, China, in 1989 and 1994, respectively. Currently, he is a professor of Wuhan University. His current research interests include number theory, information security, and network security.

