An Improved Key Agreement Authentication Scheme Based on an Anonymous Password

Hsieh-Tsen Pan[1], Shu-Fen Chiou[2], Cheng-Ying Yang[3], and Min-Shiang Hwang[1, 4]
[1] Department of Computer Science & Information Engineering, Asia University, Taichung, Taiwan
[2] Department of Information Management, National Taichung University of Science and Technology, Taiwan
[3] Department of Computer Science, University of Taipei, Taipei, Taiwan
[4] Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan
Email: 102566004@gm.asia.edu.tw; fen057@gmail.com; cyang@utaipei.edu.tw; mshwang@asia.edu.tw

Abstract—**It is becoming much significant in the security of password-based authentication over the Internet. Recently, with a formal proof, the improved anonymous password-based authentication scheme was proposed by Wu, Chen, and Wang. Within the practical applications, the scheme provides better performance for security. The scheme has claimed the ability to withstand various known attacks, such as user anonymity, user and server impersonations, and so on. Unfortunately, there still exist some weaknesses in the scheme. This work shows that the scheme is not secure to those attacks, such as online password guessing and denial of service attacks. Finally, the improved scheme is proposed.**

Index Terms—**Password, smart card, formal proof, user authentication, key agreement**

I. Introduction

It becomes much significant in the security of password-based authentication over the Internet. For the remote user access control, the authentication schemes were proposed [1]-[4]. For the legal users, it provides an important scheme to protect privacy and confidentiality. Over the Internet, the authentication schemes were proposed with employing a smart card [5]-[19]. Among these schemes, for multi-servers, the authentications proposed by Chen *et al*. [5] and Feng *et al*. [6]. For biometric applications, the schemes were proposed by Annamalai *et al*. [7] and Tarek *et al*. [8]. Based on elliptic curve cryptosystems, the time efficient authentication have been proposed [9]-[11]. Besides, based on timestamps, Wijayanto *et al*. and Huang *et al*. proposed the schemes [17], [18]. With using RFID, some schemes have been presented [12], [13]. For generating the session key by applying passwords, the schemes were proposed [14]-[16]. Also, the other authentications were proposed [19], [20].

A secure authentication is needed for the access control system. Beginning with Li, Liu, and Wu in 2012, the remote authentication scheme was proposed to resist the attacks including spoofing, forgery, and password guessing attacks [21]. Additionally, for efficiency consideration, Yoon *et al.* proposed a remote control scheme [22]. However, the security was broken by the impersonated attack. Huang, Chang, and Yu proposed an authentication scheme with employing timestamp to withstand [18]. Similarly, to resist password guessing attacks and to improve the weaknesses in the scheme by Li *et al.*, Feng, Chao, and Hwang proposed an authentication [23]. Additionally, to resist the password guessing attack, t hey improved the insecurity in the remote control scheme by by Yoon *et al.* [24]. Moreover, for the smart card and password guessing attack, they developed a scheme to improve the weakness in the scheme proposed by Huang, Chang, and Yu [25].

On the other hand, the smart card could be used for the identification. For security enhancement, the usage of smart card is applied. In 2010, Kumar proposed a robust user authentication scheme based on a smart card [26]. That scheme was shown to be vulnerable to the off-line guessing password attack [27]. Hence, Yang *et al.* proposed a scheme with mutual authentication to enhance the security in the application of smart card [28]. Unfortunately, Cahyadi *et al.* found that scheme is vulnerable to the on-line guessing password attack and man-in-the-middle attacks [29]. Then, Chang and Lee proposed an efficient smart card-based user authentication scheme in 2013 [30]. However, Chiou *et al.* showed that scheme is vulnerable to the on-line guessing identity and password attacks, and the denial of service attack [31].

Generally, the password could be applied to the access control system for the security concern. Sood *et al.* proposed a practical inverse cookie-based virtual password authentication scheme in 2016 [32]. However, Pan *et al.* showed that scheme is vulnerable with some weaknesses for the on-line guessing password and the denial of service attacks [33]. With the consideration for multi-server environments, Amin proposed an efficient ID-based remote user authentication scheme in 2016. [34]. However, this scheme is vulnerable to resist the off-line identity guessing with the smart card stolen attack and off-line password guessing with the smart card stolen attack [35]. Then, Thandra *et al.* proposed an efficient user authentication scheme to improve the authentication [36]. Regrettably, for the denial of service, online and

Manuscript received September 9, 2019; revised November 25, 2019; accepted December 12, 2019.

Corresponding author: Min-Shiang Hwang (email: mshwang@asia.edu.tw)

©2020 Int. J. Elec. & Elecn. Eng. & Telcomm.
doi: 10.18178/ijeetc.9.3.199-205

offline password guessing, and impersonation attacks, this vulnerable scheme is found by Pan. [37].

For saving the computing resource, some authentications have been proposed. Moon *et al.* proposed an efficient and secure authentication scheme in 2017 [20]. However, Irawan and Hwang showed that some weaknesses in this proposed scheme [38]. Hou and Wang proposed an ECC-based user authentication scheme [9]. Similarly, Hwang *et al.* proved that that scheme could not withstand the guessing attack with the smart card [39]. For practical applications, an enhanced anonymous password-based authentication with the key agreement was proposed by Wu, Chen, and Wang [16]. It claimed that the scheme has the ability to withstand various known types of attacks including the user anonymity, the off-line password guessing, stolen verifier, insider, replay, user impersonation, and server impersonation attacks for the mutual authentication and the forward secrecy. However, there exist some weaknesses and the vulnerable system is frail to resist both the online password guessing with the smart card stolen attack and the denial of service attack.

In the following section, Wu *et al.*'s authentication scheme for remote users is described. The analysis of security weakness in Wu *et al.*'s scheme is given in Section III. To improve the frangibility in Wu's scheme, the proposed authentication scheme for remote users is shown in Section IV. The comparisons in security properties and efficiencies among the proposed scheme and others are given in Section V. The conclusion of this work is given in the final.

II. WU *ET AL.*'S AUTHENTICATION SCHEME

In this section, Wu *et al.*'s anonymous password-based authenticated key agreement scheme [16] is briefly reviewed. In Wu *et al.*'s authentication with the key agreement, user U_i, Smart Card, and Server S_i are included in the scheme. The scenario has four phases in the scheme. They are registration, login, authentication, and password change phases, respectively. For simplification, the notations used are listed in Table I.

TABLE I: NOTATIONS USED IN THE SCHEME

Notations	Description
U_i/U_k	A user i/k
S_i	A server i
E	An attacker
PW_i	The U_i's password
ID_i	The U_i's identity
x	A secret key generated by S_i
y	A public key generated by S_i
b	A random number generated by U_i
v	A random number generated by U_i
w	A random number generated by S_i
$h()$	A one-way hash function
$\|\|$	A concatenation
$\oplus$	A bitwise exclusive-or operation

A. Registration

Initially, each user U_i registers to server S_i to become legal to access the resources in the server. Server S_i issues a smart card to user U_i. Hence, the execution in this phase includes the following:

1) Firstly, user U_i randomly chooses a number b, the identity ID_i and the password PW_i.
2) User U_i sends $\{\mathrm{ID}_i, \mathrm{RPW}_i\}$ to server S_i, where $\mathrm{RPW}_i=h(b \,\|\, \mathrm{PW}_i)$.
3) After checking ID_i, if ID_i is validity, server S_i computes and sends a smart card which stores $\{C_2, C_3, C_4, C_5, h(\cdot), n, g, y\}$ to user U_i via a secure channel, where

$$C_1=h(\mathrm{ID}_i \,\|\, x)$$
$$C_2=C_1 \oplus \mathrm{RPW}_i$$
$$C_3=h(C_1 \,\|\, d)$$
$$C_4=h(C_1 \,\|\, \mathrm{RPW}_i) \oplus d$$
$$D=g^d \bmod n$$
$$C_5=h(C_1 \oplus \mathrm{ID}_i) \oplus h(x \,\|\, y \,\|\, D).$$

4) User U_i stores B in the smart card, where $B=b \oplus \mathrm{ID}_i \oplus \mathrm{PW}_i$. Now, the smart card includes $\{C_2, C_3, C_4, C_5, h(\cdot), n, g, y, B\}$.

B. Login

In the login phase, the user U_i is firstly connected to a terminal with the smart card and keys in ID_i' and PW_i'. This phase includes the following executions.

1) The smart card computes b, RPW_i', C_1, d, and C_3' according to the following equations,

$$b=B \oplus \mathrm{ID}_i \oplus \mathrm{PW}_i$$
$$\mathrm{PRW}_i=h(b \,\|\, \mathrm{PW}_i)$$
$$C_1=C_2 \oplus \mathrm{RPW}_i$$
$$d=C_4 \oplus h(C_1 \,\|\, \mathrm{RPW}_i)$$
$$C_3'=h(C_1 \,\|\, \mathrm{d})$$

2) Comparing C_3' with C_3 stored inside of the card, if $C_3' = C_3$, the smart card carries the calculation as

$$V=g^v \bmod n$$
$$D=g^d \bmod n$$
$$h(x \,\|\, y \,\|\, D)=C_5 \oplus h(C_1 \oplus ID_i)$$
$$\mathrm{CID}_i=\mathrm{ID}_i \oplus h(V \,\|\, h(x \,\|\, y \,\|\, D))$$
$$F_1=\mathrm{RPW}_i \oplus h(C_1 \,\|\, ID_i)$$
$$F_2=C_4 \oplus h(V \,\|\, C_1) \oplus h(x \,\|\, y \,\|\, D)$$
$$M_1=h(\mathrm{ID}_i \,\|\, \mathrm{RPW}_i \,\|\, V \,\|\, C_1 \,\|\, d).$$

3) User U_i sends the login request message $\{\mathrm{CID_i}, V, D, F_1, F_2, M_1\}$ to server S_i.

C. Authentication

After receiving the login request message $\{\mathrm{CID}_i, V, D, F_1, F_2, M_1\}$, for authentication, server S_i executes the procedure including:

1) Server S_i computes ID_i, C_1, RPW_i, C_4, d and M_1^* as follows:

$$\mathrm{ID}_i=\mathrm{CID}_i \oplus h(V \,\|\, h(x \,\|\, y \,\|\, D))$$
$$C_1=h(ID_i \,\|\, x)$$
$$\mathrm{RPW}_i=F_1 \oplus h(C_1 \,\|\, \mathrm{ID}_i)$$
$$C_4=F_2 \oplus h(V \,\|\, C_1) \oplus h(x \,\|\, y \,\|\, D)$$
$$d=C_4 \oplus h(C_1 \,\|\, RPW_i)$$

$$M_1^*=h(\mathrm{ID}_i \,||\, \mathrm{RPW}_i \,||\, V \,||\, C_1 \,||\, d).$$

2) Server S_i checks whether $M_1^*=M_1$. If the equation is held, server S_i computes and sends $\{M_2, W\}$ to the smart card as follows:

$$W=g^w \bmod n$$
$$\mathrm{SK}=V^w \bmod n$$
$$M_2=h(\mathrm{SK} \,||\, W \,||\, C_1 \,||\, \mathrm{RPW}_i \,||\, d).$$

3) After receives the message $\{M_2, W\}$ from server S_i, the session key SK' and M_2' are generated by the smart card according to

$$\mathrm{SK}'=W^v \bmod n$$
$$M_2'=h(\mathrm{SK}' \,||\, W \,||\, C_1 \,||\, \mathrm{RPW}_i \,||\, d).$$

4) The smart card checks whether $M_2=M_2'$. If the equation is held, the smart card computes and sends M_3 to server S_i.

$$M_3=h(M_2 \,||\, C_1 \,||\, \mathrm{SK}' \,||\, d).$$

5) Upon receiving M_3, server S_i computes $M_3^*=h(M_2 \,||\, C_1 \,||\, \mathrm{SK} \,||\, d)$ and checks whether $M_3^*=M_3$. If the equation is held, server S_i and user U_i finish the mutual authentication. Both of them share a same session key $\mathrm{SK}=g^{vw}$. Or, termination of the session is held.

III. Weakness Analysis

Cryptanalysis of Wu *et al.*'s authentication scheme [16] is given in this session. Wu *et al.* claimed that the proposed scheme has the ability to resist possible attacks including User anonymity, off-line password guessing, stolen verifier, insider, replay, user impersonation and server impersonation attacks for mutual authentication and forward secrecy. This work proves that the authentication scheme proposed by Wu *et al.* is vulnerable to online password guessing with the stolen smart card and denial of service attacks.

A. Online Password Guessing with the Stolen Smart Card

Wu *et al.* claimed that the attackers hardly guess the password PWi if the smart card is stolen. However, under the condition of smart card stolen, this work shows that the scheme is not strong to resist the online password guessing attack.

By employing the following login procedures, the attacker could guess password PWi. with user U_i's smart card.

1) The parameter b, RPW_i, C_1, d and C_3' are calculated by the smart card as follows:

$$B'=B \oplus ID_i \oplus PW_i'$$
$$\mathrm{PRW}_i'=h(b \,||\, PW_i')$$
$$C_1'=C_2 \oplus \mathrm{RPW}_i'$$
$$d=C_4 \oplus h(C_1' \,||\, \mathrm{RPW}_i')$$
$$C_3^*=h(C_1' \,||\, d')$$

2) Comparing C_3^* with C_3 stored inside of the card, if $C_3^*=C_3$, the smart card computes and sends a request message $\{\mathrm{CID}_i, V, D, F_1, F_2, M_1\}$ to server S_i. Otherwise, the connection is terminated.
3) The attacker monitors the transition between the terminal and server S_i. If the attacker intercepts the request message $\{\mathrm{CID}_i, V, D, F_1, F_2, M_1\}$, this means the attacker guesses the user U_i's password correctly, Otherwise it's incorrect. The attacker repeats Step 1 and Step 2 till guessing the correct password.

B. Denial of Service

Under a public channel, the attacker has the ability to intercept the transition. Thus, the attacker could receive a legal login message $\{\mathrm{CID}_i, V, D, F_1, F_2, M_1\}$ from user U_i. The denial of service would be held according to the following operations.

1) The attacker re-sends the previous login message $\{\mathrm{CID}_i, V, D, F_1, F_2, M_1\}$ sent by the legal user U_i's.
2) Receiving the login request message $\{\mathrm{CID}_i, V, D, F_1, F_2, M_1\}$ from the attacker, the server S_i computes ID_i, C_1, RPW_i, C_4, d and M_1^* as in Equation in Section II-*C*.
3) Server S_i checks whether $M_1^*=M_1$. If the equation is held, server Si computes and sends $\{M_2, W\}$ to the smart card as follows:

$$W=g^w \bmod n$$
$$\mathrm{SK}=V^w \bmod n$$
$$M_2=h(\mathrm{SK} \,||\, W \,||\, C_1 \,||\, \mathrm{RPW}_i \,||\, d),$$

where w is a random number.

4) The attacker ignores the receiving message $\{M_2, W\}$ and sends a random M_3' to server S_i.
5) Upon receiving M_3', server S_i computes $M_3''=h(M_2 \,||\, C_1 \,||\, \mathrm{SK} \,||\, d)$ and checks whether $M_3''=M_3$. If the equation is not held, server S_i terminates the session.

IV. Proposed Improved Scheme

Within Wu *et al.*'s authentication scheme, one weakness is that the attacker could repeat to conjecture the password if he holds the smart card. In order to overcome this defeat, for the rule of using a smart card, the number of inputting the incorrect password should be limited (i.e., 3 times). The other weakness within Wu *et al.*'s scheme is that the attacker could exhaust the CPU computing resource in the server. To improve this weakness, the server should cost a light computation to check the legality of users. To remedy these disadvantages, the proposed scheme modifies both login and authentication in Wu *et al.*'s scheme as the following phases.

A. Login

To access the resource in the server S_i, user U_i logins to the system. Initially, user U_i connects the smart card to the device (terminal), and then enters identity ID_i' and password PW_i'. At this phase, the smart card executes the following operations.

1) The parameter b' and RPW' are calculated according to

$$b'=B\oplus ID_i'\oplus PW_i'$$
$$RPW_i'=h(b' \,||\, PW_i')$$

2) Checking whether $PW_i'=PW_i$, where PW_i is retrieved from the smart card, if the equation is not held, the smart card counts on the incorrect password. If the number of inputting the incorrect password three times, the smart card will self-lock and stop all operations. If the number of inputting password less than three, the smart card asks the user to reenter the identity ID_i and password PW'. Then, the smart card repeats Steps 1 - 2.
3) According the following equations, the smart card computes C_1, d, and C_3'.

$$C_1=C_2\oplus RPW_i$$
$$d=C_4\oplus h(C_1 \,||\, RPW_i)$$
$$C_3'=h(C_1 \,||\, d)$$

4) Comparing C_3' with C_3 stored inside of the card, if $C_3'=C_3$, the following operations are executed.

$$V=g^v \bmod n$$
$$D=g^d \bmod n$$
$$h(x \,||\, y \,||\, D)=C_5\oplus h(C_1\oplus ID_i)$$
$$CID_i=(ID_iT_i)\oplus h(V \,||\, h(x \,||\, y \,||\, D))$$
$$F_1=RPW_i\oplus h(C_1 \,||\, ID_i)$$
$$F_2=C_4\oplus h(V \,||\, C_1)\oplus h(x \,||\, y \,||\, D)$$
$$M_1=h(ID_i \,||\, RPW_i \,||\, V \,||\, C_1 \,||\, d).$$

In the equation, T_i is a time stamp of the smart card, and v is a random number.

5) User U_i sends a login request message $\{CID_i, V, D, F_1, F_2, M_1, T_i\}$ to server S_i.

B. Authentication

Server S_i executes the authentication procedure if it receives the login request message $\{CID_i, V, D, F_1, F_2, M_1, T_i\}$ from user U_i. The procedure includes:

1) For the validity of time stamp, Server S_i checks T_i and computes ID_i and T_i as

$$ID_i \,||\, T_i'=CID_i\oplus h(V \,||\, h(x \,||\, y \,||\, D))$$

2) Checking whether $T_i'=T_i$, if the equation is held, server S_i continually executes the following steps. Or, the server terminates the session.
3) Server S_i computes C_i, RPW_i, C_4, d and M_1^* as follows:

$$C_1=h(ID_i \,||\, x)$$
$$RPW_i=F_1\oplus h(C_1 \,||\, ID_i)$$
$$C_4=F_2\oplus h(V \,||\, C_1)\oplus h(x \,||\, y \,||\, D)$$
$$d=C_4\oplus h(C_1 \,||\, RPW_i)$$
$$M_1^*=h(ID_i \,||\, RPW_i \,||\, V \,||\, C_1 \,||\, d).$$

4) Checking whether $M_1^*=M_1$, if the equation is held, server S_i computes and sends $\{M_2, W\}$ to the smart card as follows:

$$W=g^w \bmod n$$
$$SK=V^w \bmod n$$
$$M_2=h(SK \,||\, W \,||\, C_1 \,||\, RPW_i \,||\, d)$$

where w is a random number.

5) Once the smart card receives the message $\{M_2, W\}$, session key SK' and M_2' are generated with the following operations.

$$SK'=W^v \bmod n$$
$$M_2'=h(SK' \,||\, W \,||\, C_1 \,||\, RPW_i \,||\, d)$$

6) Checking whether $M_2=M_2'$, if the equation is held, the smart card replies with M_3 to server S_i, where

$$M_3=h(M_2 \,||\, C_1 \,||\, SK' \,||\, d)$$

7) Upon receiving M_3 , server S_i computes $M_3^*=h(M_2 \,||\, C_1 \,||\, SK \,||\, d)$ and checks $M_3^*=M_3$. If the equation is held, server S_i and user U_i finish the mutual authentication. The common session key $SK=g^{vw}$ is shared to server S_i and user U_i . Otherwise, the server terminates the session.

V. Comparisons

A. Comparisons in Security Properties

The security of the improved scheme is similar to that of Wu *et al.*'s scheme. However, the weaknesses, as described in Section III, in the proposed authentication scheme, it will be vanished. In this section, the work shows that the proposed scheme could withstand the attacks including both on-line password guessing with the smart card stolen and denial of service attacks.

One of the weaknesses of Wu *et al.*'s scheme is that the attacker could repeat to guess the password with the smart card. To improve the weakness of Wu *et al.*'s scheme, the smart card should limit the number of inputting an incorrect password. In the improved scheme, if the number of inputting password is more than three, the smart card will reject the login request. Hence, the online password guessing with the smart card stolen attacks will not be held in the proposed authentication scheme. The other weakness in Wu *et al.*'s scheme is that the attacker could replay and exhaust the server in CPU computation. To overcome the defeat, the server might cost a light computation to check the legality of users.

In Step 4 of the login phase of the improved scheme, the timestamp T_i is used against the replay attack:

$$CID_i=ID_i \,||\, T_i\oplus h(V \,||\, h(x \,||\, y \,||\, D))$$

In the authentication phase, with Steps 1-2, the server will reject the login request if the previous request message $\{CID_i, V, D, F_1, F_2, M_1, T_i\}$ is resent to server S_i. The server compares if $T_i'=T_i$ in the improved scheme. The server only costs an exclusive OR operation in the equation below:

$$\mathrm{ID}_i \,\|\, T_i' = \mathrm{CID}_i \oplus h(V \,\|\, h(x \,\|\, y \,\|\, D))$$

and a comparison operation is done in Step 2 of the authentication phase. Since the server costs a light computation to check the legality of users, the improved scheme could be against the denial of service attacks.

Table II presents the comparison among the proposed scheme and the others with security properties. In the table, we compare these schemes: Wu *et al.* [16], Zhang *et al.* [11], and Cao *et al.* [1] schemes, which were published within 3 years. The security properties include mutual authentication, forward security, user anonymity, resisting off-line password guessing attacks, resisting replay attacks, resisting man-in-the-middle attacks, resisting forgery attacks, resisting online password guessing with the smart card stolen attack, and resisting denial of service attacks. In Table II, "V" denotes that the scheme provides the security property. In opposite, "X" denotes the scheme fails the security property.

In 2018, Zhang *et al.* proposed an ECC-based (elliptic curves cryptosystem-based) user authentication scheme for anonymous users. Their scheme could achieve mutual authentication and forward security [11]. They also claimed that their scheme can withstand some attacks, such as forgery, offline password guessing, server impersonating, and reply attacks. However, in 2018, Hwang *et al.* showed that their scheme is vulnerable to forgery attacks, server impersonating attacks, and man-in-the-middle attacks [40].

TABLE II: COMPARISON IN SECURITY PROPERTIES

Security properties	Ref. [16]	Ref. [11]	Ref. [1]	Ours
Mutual authentication	V	X	V	V
Forward security	V	V	V	V
User anonymity	V	V	V	V
Resist off-line password guessing attack	V	V	V	V
Resist replay attack	V	V	V	V
Resist man-in-the-middle attack	V	V	V	V
Resist forgery attack	V	X	V	V
Resist online password guessing with smart card stolen attack	X	V	X	V
Resist denial of service attack	X	V	X	V

TABLE III: COMPARISON IN EFFICIENCIES

Efficiencies	Ref. [16]	Ref. [11]	Ref. [1]	Ours
Login phase	$8T_h+2T_{\exp}$	$3T_h+4T_{\text{ec-mul}}+1T_{\text{ec-add}}$	$4T_h$	$8T_h+2T_{\exp}$
Verification phase (for client)	$2T_h+1T_{\exp}$	$1T_h+2T_{\text{ec-mul}}$	$4T_h$	$2T_h+1T_{\exp}$
Verification phase (for server)	$10T_h+2T_{\exp}$	$3T_h+8T_{\text{ec-mul}}$	$6T_h$	$10T_h+2T_{\exp}$

In Section II, we have introduced Wu, Chen, and Wang's user authentication scheme [16]. Their scheme has user anonymity, mutual authentication, forwarding secrecy, and can resist off-line password guessing, stolen verifiers, insiders, and replaying attacks. However, we have shown that their scheme is frail to both online password guessing with the smart card stolen attack and the denial of service attack in Section III.

In 2019, Cao, Sun, and Cao proposed a remote user authentication scheme [1]. Their scheme has identity preservation, mutual authentication, forwarding secrecy properties, and resists the slow wrong password detection, password guessing, and other possible attacks in Table II. However, Hwang *et al.* showed that their scheme is vulnerable to the on-line password guessing attack with user's smart card and denial of service attacks [41].

B. *Comparisons in Efficiencies*

Table III presents the comparison among the proposed scheme and the others with efficiency in the login and the verification phases. In Table III, we define some denotations:

T_h: The time to execute a one-way Hash function operation;

$T_{\exp}$: The time to execute an exponential operation;

$T_{\text{ec-mul}}$: The time to execute a multiplication operation of elliptic curves;

$T_{\text{ec-add}}$: The time to execute an add operation of elliptic curves.

The time to execute an XOP ($\oplus$) operation can be ignored to compare with $T_{\exp}$ and T_h. The proposed user authentication scheme is an improved Wu *et al.*'s scheme [16]. The computation costs both of the proposed scheme and Wu *et al.*'s scheme $8T_h+2T_{\exp}$ in the login phase, including $1T_h$ for Step 1, $2T_h$ for Step 2, $5T_h$ and $2T_{\exp}$ for Step 4 of the login phase. The computation costs both of the proposed scheme and Wu *et al.*'s scheme $2T_h+1T_{\exp}$ and $10T_h+2T_{\exp}$ in the verification phases for clients and servers, respectively. The computation costs need $2T_h$ for Step 1, $6T_h$ for Step 3, $1T_h$ and $2T_{\exp}$ for Step 4, $1T_h$ for Step 7 of the verification phase for servers. The total computation costs the verification phase for servers $10T_h+2T_{\exp}$. The computation needs $1T_h$ and $1T_{\exp}$ for Step 5, $1T_h$ for Step 6 of the verification phase for clients. The total computation costs of the verification phase for the client are $2T_h+1T_{\exp}$.

The computation costs of Zhang *et al.* scheme [11] and Cao *et al.*'s scheme [1] are summarized in Table III. Obviously, the computation costs of Zhang *et al.*'s scheme are inefficient compared with that of the proposed scheme. Although the performances of Cao *et al.*'s scheme [1] and Wu *et al.*'s scheme are efficient than or equal to that of the proposed scheme, their schemes fails to both online password guessing with the smart card stolen attack and the denial of service attack.

VI. CONCLUSIONS

A brief review of Wu *et al.*'s anonymous password-based authenticated key agreement scheme and the security analysis is given in this article. Based on the condition of password attacks, this work shows that the authentication by Wu *et al.* could not resist both of the denial of service and online password guessing with smart card attacks. To overcome the weaknesses of Wu *et al.*'s scheme, this work proposes an improvement to conquer those weaknesses in Wu *et al.*'s scheme. With the detailed analysis, the proposed scheme could resist the defeats mentioned.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

All authors conducted the research; Hsieh-Tsen Pan and Shu-Fen Chiou wrote the paper; Cheng-Ying Yang and Min-Shiang Hwang analyzed and verified the scheme and security; all authors had approved the final version.

ACKNOWLEDGMENT

This work was partially supported by the Grants from Ministry of Science and Technology, Taiwan, under contracts, MOST 104-2221-E-468-004, MOST 107-2221-E-845 -001 -MY3 and MOST 107-2221-E-845 -002 -MY3.

REFERENCES

[1] S. Q. Cao, Q. Sun, and L. L. Cao, "Security analysis and enhancements of a remote user authentication scheme," *International Journal of Network Security*, vol. 21, pp. 661-669, July 2019.

[2] T. Y. Chang, W. P. Yang, and M. S. Hwang, "Simple authenticated key agreement and protected password change protocol," *Computers & Mathematics with Applications*, vol. 49, pp. 703-714, 2005.

[3] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, pp. 64-67, Jan. 2013.

[4] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, pp. 28-30, Jan. 2000.

[5] 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, pp. 1008-1032, Feb. 2013.

[6] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments," *International Journal of Network Security*, vol. 16, pp. 318-321, July 2014.

[7] P. Annamalai, K. Raju, and D. Ranganayakulu, "Soft biometrics traits for continuous authentication in online exam using ICA based facial recognition," *International Journal of Network Security*, vol. 20, pp. 423-432, May 2018.

[8] E. Tarek, O. Ouda, and A. Atwan, "Image-based multimodal biometric authentication using double random phase encoding," *International Journal of Network Security*, vol. 20, pp. 1163-1174, Nov. 2018.

[9] G. Hou and Z. Wang, "A robust and efficient remote authentication scheme from elliptic curve cryptosystem," *International Journal of Network Security*, vol. 19, pp. 904-911, Nov. 2017.

[10] L. Han, Q. Xie, and W. Liu, "An improved biometric based authentication scheme with user anonymity using elliptic curve cryptosystem," *International Journal of Network Security*, vol. 19, pp. 469-478, May 2017.

[11] X. Zhang, B. Wang, and W. Wang, "A new remote authentication scheme for anonymous users using elliptic curves cryptosystem," *International Journal of Network Security*, vol. 20, pp. 390-395, Mar. 2018.

[12] S. Y. Chiou, W. T. Ko, and E. H. Lu, "A secure ECC-based mobile RFID mutual authentication protocol and its application," *International Journal of Network Security*, vol. 20, pp. 396-402, Mar. 2018.

[13] C. H. Wei, M. S. Hwang, and A. Y. H. Chin, "A mutual authentication protocol for RFID," *IEEE IT Professional*, vol. 13, pp. 20-24, Mar. 2011.

[14] S. F. Chiou, H. T. Pan, E. F. Cahyadi, and M. S. Hwang, "Cryptanalysis of the mutual authentication and key agreement protocol with smart cards for wireless communications," *International Journal of Network Security*, vol. 21, pp. 100-104, Jan. 2019.

[15] C. Guo, C. C. Chang, and S. C. Chang, "A secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications," *International Journal of Network Security*, vol. 20, pp. 323-331, Mar. 2018.

[16] M. Wu, J. Chen, and R. Wang, "An enhanced anonymous password-based authenticated key agreement scheme with formal proof," *International Journal of Network Security*, vol. 19, pp. 785-793, Sept. 2017.

[17] H. Wijayanto and M. S. Hwang, "Improvement on timestamp-based user authentication scheme with smart card lost attack resistance," *International Journal of Network Security*, vol. 17, pp. 160-164, Mar. 2015.

[18] H. F. Huang, H. W. Chang, and P. K. Yu, "Enhancement of timestamp-based user authentication scheme with smart card," *International Journal of Network Security*, vol. 16, pp. 463-467, May 2014.

[19] Y. Liu, C. C. Chang, and S. C. Chang, "An efficient and secure smart card based password authentication scheme," *International Journal of Network Security*, vol. 19, pp. 1-10, Jan. 2017.

[20] J. Moon, D. Lee, J. Jung, and D. Won, "Improvement of efficient and secure smart card based password authentication scheme," *International Journal of Network Security*, vol. 19, pp. 1053-1061, Nov. 2017.

[21] J. Li, S. Liu, and S. Wu, "Cryptanalysis and improvement of a YS-like user authentication scheme," *International Journal of Digital Content Technology and Its Applications*, vol. 7, pp. 828-836, Jan. 2012.

[22] E. J. Yoon, S. H. Kim, and K. Y. Yoo, "A security enhanced remote user authentication scheme using smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 8, pp. 3661-3675, Sept. 2012.

[23] T. H. Feng, W. Y. Chao, and M. S. Hwang, "Cryptanalysis and improvement of the Li-Liu-Wu user authentication scheme," in *Proc. International Conference on Future Communication Technology and Engineering*, 2014, pp. 103-106.

[24] T. Y. Chen, C. H. Ling, and M. S. Hwang, "Weaknesses of the Yoon-Kim-Yoo remote user authentication scheme using smart cards," in *Proc. IEEE Workshop on Electronics, Computer and Applications*, 2014, pp. 771-774.

[25] T. H. Feng, C. H. Ling, and M. S. Hwang, "An improved timestamp-based user authentication scheme with smart card," in *Proc. 2nd Congress on Computer Science and Application*, 2014, pp. 111-117.

[26] M. Kumar, "An enhanced remote user authentication scheme with smart card," *International Journal of Network Security*, vol. 10, pp. 175-184, May 2010.

[27] M. S. Hwang, E. F. Cahyadi, Y. C. Chou, and C. Y. Yang, "Cryptanalysis of Kumar's remote user authentication scheme with smart cards," in *Proc. 14th International Conference on Computational Intelligence and Security*, Hangzhou, 2018, pp. 416-420.

[28] L. Yang, J. F. Ma, and Q. Jiang, "Mutual authentication scheme with smart cards and password under trusted computing," *International Journal of Network Security*, vol. 14, pp. 156-163, May 2012.

[29] E. F. Cahyadi, Y. C. Chou, C. Y. Yang, and M. S. Hwang, "An improved mutual authentication scheme with smart cards and

password under trusted computing," in *Proc. IOP Conference Series: Materials Science and Engineering*, Dec. 2018, vol. 466, pp. 012008.

[30] C. C. Chang and C. Y. Lee, "A smart card-based authentication scheme using user identity cryptography," *International Journal of Network Security*, vol. 16, pp. 139-147, Jan. 2013.

[31] S. F. Chiou, E. F. Cahyadi, C. Y. Yang, and M. S. Hwang, "An improved Chang-Lee's smart card-based authentication scheme," *Journal of Physics: Conference Series*, vol. 1237, pp. 042044, June 2019.

[32] S. K. Sood, A. K. Sarje, and K. Singh, "Inverse cookie-based virtual password authentication protocol," *International Journal of Network Security*, vol. 13, pp. 172-181, Mar. 2016.

[33] H. T. Pan, C. C. Wu, C. Y. Yang, and M. S. Hwang, "The weaknesses of the virtual password authentication protocol with cookie," in *Proc. IOP Conference Series: Materials Science and Engineering*, vol. 466, pp. 012009, Dec. 2018.

[34] R. Amin, "Cryptanalysis and efficient dynamic ID based remote user authentication scheme in multi-server environment using smart card," *International Journal of Network Security*, vol. 18, pp. 172-181, Jan. 2016.

[35] H. T. Pan, C. S. Pan, S. C. Tsaur, and M. S. Hwang, "Cryptanalysis of efficient dynamic ID based remote user authentication scheme in multi-server environment using smart card," in *Proc. 12th International Conference on Computational Intelligence and Security*, Jiangsu, 2016, pp. 590-593.

[36] P. K. Thandra, J. Rajan, and S. A. V. S. Murty, "Cryptanalysis of an efficient password authentication scheme," *International Journal of Network Security*, vol. 18, pp. 362-368, Mar. 2016.

[37] C. S. Pan, C. Y. Tsai, S. C. Tsaur, and M. S. Hwang, "Cryptanalysis of an efficient password authentication scheme," in *Proc. 3rd IEEE International Conference on Systems and Informatics*, Shaihai, 2016, pp. 732-737.

[38] B. Irawan and M. S. Hwang, "The weakness of Moon *et al.*'s password authentication scheme," *Journal of Physics: Conference Series*, vol. 1069, pp. 012070, Aug. 2018.

[39] M. S. Hwang, H. W. Yang, and C. Y. Yang, "An improved Hou-Wang's user authentication scheme," *Lecture Notes in Electrical Engineering*, vol. 514, pp. 295-301, 2019.

[40] M. S. Hwang, E. F. Cahyadi, C. Y. Yang, and S. F. Chiou, "An improvement of the remote authentication scheme for anonymous users using an elliptic curve cryptosystem," in *Proc. IEEE 4th International Conference on Computer and Communications*, Chengdu, China, 2018, pp. 1872-1877.

[41] M. S. Hwang, H. W. Yang, and C. Y. Yang, "Cryptanalysis of security analysis and enhancements of a remote user authentication scheme," in *Proc. 3rd annual International Conference on Cloud Technology and Communication Engineering*, Wuhan, China, 2019.

Copyright © 2020 by the authors. This is an open access article distributed under the Creative Commons Attribution License (CC BY-NC-ND 4.0), which permits use, distribution and reproduction in any medium, provided that the article is properly cited, the use is non-commercial and no modifications or adaptations are made.

Hsieh-Tsen Pan received B.Sc. degree in business administration from Soochow University Taipei, Taiwan in 1999; M.Sc. degree in information engineering, Asia University, Taichung, Taiwan 2015. He is currently pursuing his Ph.D. degree in information engineering, Asia University Taichung. From 2011 to 2014, he was the manager in enterprise service, Chunghwa Telecom South Branch, Taichung, Taiwan. From 2014 to 2017, he was the operation manager in Medium Division Taiwan Ricoh Co., Ltd., Taichung, Taiwan. From 2017 Sep 20 he has been with the Apple MDM Server Service VP in Get Technology Co. Ltd. Taipei Taiwan.

Shu-Fen Chiou received a B.B.A degree in Information Management from National Taichung Institute of Technology, Taichung, Taiwan, ROC, in 2004; She studied M.S. degree in Computer Science and Engineering from National Chung Hsing University for one year, and she started to pursue the Ph.D. degree. She received a Ph.D. from Computer Science and Engineering from National Chung Hsing University in 2012. She is currently an assistant professor of department of Information Management, National Taichung University of Science and Technology. Her current research interests include information security, network security, data hiding, text mining and big data analysis.

Cheng-Ying Yang received the M.S. degree in Electronic Engineering from Monmouth University, New Jersey, in 1991, and Ph.D. degree from the University of Toledo, Ohio, in 1999. He is a member of IEEE Satellite & Space Communication Society. Currently, he is employed as an Associate Professor at Department of Computer Science, University of Taipei, Taiwan. His research interests are performance analysis of digital communication systems, error control coding, signal processing and computer security.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988; and Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan in 1995. He was a professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2009. He was also a visiting professor with University of California (UC), Riverside and UC. Davis (USA) during 2009-2010. He was a distinguished professor of Department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.