An Improved Key Agreement Authentication Scheme Based on an Anonymous Password

Hsieh-Tsen Pan\textsuperscript{1}, Shu-Fen Chiou\textsuperscript{2}, Cheng-Ying Yang\textsuperscript{3}, and Min-Shiang Hwang\textsuperscript{1,4}

\textsuperscript{1} Department of Computer Science & Information Engineering, Asia University, Taichung, Taiwan
\textsuperscript{2} Department of Information Management, National Taichung University of Science and Technology, Taiwan
\textsuperscript{3} Department of Computer Science, University of Taipei, Taipei, Taiwan
\textsuperscript{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, they 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
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 the 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 serve 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>
<thead>
<tr>
<th>Table I: Notations Used in the Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notations</td>
</tr>
<tr>
<td>$U_i$</td>
</tr>
<tr>
<td>$S_i$</td>
</tr>
<tr>
<td>$E$</td>
</tr>
<tr>
<td>PW$i$</td>
</tr>
<tr>
<td>ID$i$</td>
</tr>
<tr>
<td>$x$</td>
</tr>
<tr>
<td>$y$</td>
</tr>
<tr>
<td>$b$</td>
</tr>
<tr>
<td>$v$</td>
</tr>
<tr>
<td>$w$</td>
</tr>
<tr>
<td>$h(x)$</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+</td>
</tr>
</tbody>
</table>

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 $\{ID_i$, RPW$$_i$\}$ to server $S_i$, where RPW$$_i$$=h(b \parallel PW_i)$.
3) After checking ID$$_i$, if ID$$_i$ is validity, server $S_i$ computes and sends a smart card which stores $\{C_2$, $C_3$, $C_4$, $h(C)$, $n$, $g$, $y$\} to user $U_i$ via a secure channel, where

   $C_1$$=h(ID_i \parallel x)$
   $C_2$$=C_1 \oplus$ RPW$$_i$
   $C_3$$=h(C_1 \parallel d)$
   $C_4$$=h(C_1 \parallel$ RPW$$_i$$) \oplus d$
   $D=g^d \bmod n$
   $C_7$$=h(C_1 \parallel$ ID$$_i$$) \oplus h(x \parallel y \parallel D)$.

4) User $U_i$ stores $B$ in the smart card, where $B=b \parallel ID_i \parallel$ PW$$_i$. Now, the smart card includes $\{C_2$, $C_3$, $C_4$, $h(C)$, $n$, $g$, $y$, $B$\}.

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$'$, $C_1$, $d$, and $C_3$ according to the following equations,

   $b=b \parallel$ ID$$_i \parallel$ PW$$_i$.
   $\text{PRW}_i=h(b \parallel$ PW$$_i$).
   $C_1=C_2 \oplus$ RPW$$_i$.
   $d=C_4 \oplus h(C_1 \parallel$ RPW$$_i$).
   $C_3=h(C_1 \parallel d)$.

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

   $V \leftarrow g^x \bmod n$
   $D \leftarrow g^y \bmod n$
   $h(x \parallel y \parallel D) \leftarrow h(C_2 \oplus$ ID$$_i$).
   $\text{CID}_i=ID_i \parallel h(V \parallel h(x \parallel y \parallel D))$
   $F_1=\text{RPW}_i \oplus h(C_1 \parallel$ ID$$_i$).
   $F_2=C_4 \oplus h(V \parallel$ $C_1$) \oplus h(x \parallel y \parallel D)$
   $M_1=h(ID_i \parallel$ RPW$$_i \parallel V \parallel C_1 \parallel d)$.

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

C. Authentication

After receiving the login request message $\{\text{CID}_i$, $V$, $D$, $F_1$, $F_2$, $M_1$\}, 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:

   $\text{ID}_i=\text{CID}_i \parallel h(V \parallel h(x \parallel y \parallel D))$
   $C_1=h(ID_i \parallel x)$
   $\text{RPW}_i=F_1 \parallel h(C_1 \parallel$ ID$$_i$).
   $C_4=F_2 \parallel h(C) \parallel h(x \parallel y \parallel D)$
   $d=C_4 \parallel h(C_1 \parallel$ RPW$$_i$).

©2020 Int. J. Elec. & Elecn. Eng. & Telecomm. 200
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:
\[
\begin{align*}
W &= g^w \mod n \\
SK &= r^n \mod n \\
M_2 &= h(SK || W || C_1 || RPW_i || d).
\end{align*}
\]

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
\[
\begin{align*}
SK &= W^r \mod n \\
M_2 &= h(SK || W || C_1 || RPW_i || d).
\end{align*}
\]

4) The smart card checks whether \(M_2 = M_2^*\). If the equation is held, the smart card computes and sends \(M_1\) to server \(S_i\).
\[
M_1 = h(M_2 || C_1 || SK || d).
\]

5) Upon receiving \(M_1\), server \(S_i\) computes \(M_2 = h(M_2 || C_1 || SK || d)\) and checks whether \(M_2 = M_2^*\). If the equation is held, server \(S_i\) and user \(U_i\) finish the mutual authentication. Both of them share a same session key \(SK = g^w\). 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 \(PW_i\) 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 \(PW_i\) with user \(U_i\)’s smart card.

1) The parameter \(b, RPW_i, C_1, d\) and \(C'_i\) are calculated by the smart card as follows:
\[
\begin{align*}
B &= B \oplus ID_i \oplus PW_i \\
PRW'_i &= h(b \parallel PW_i) \\
C'_i &= C_2 \oplus RPW_i \\
d &= C_4 \oplus h(C'_1 \parallel RPW_i) \\
C'_i &= h(C'_1 \parallel d)
\end{align*}
\]

2) Comparing \(C'_i\) with \(C_3\) stored inside of the card, if \(C'_i = C_3\), the smart card computes and sends a request message \(\{ID_i, V, D, F_1, F_2, M_1\}\) 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 \(\{ID_i, V, D, F_1, F_2, M_1\}\), 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 \(\{CID_i, V, D, F_1, F_2, M_1\}\) 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 \(\{CID_i, V, D, F_1, F_2, M_1\}\) sent by the legal user \(U_i\)’s.

2) Receiving the login request message \(\{CID_i, V, D, F_1, F_2, M_1\}\) 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 \(S_i\) computes and sends \(\{M_2, W\}\) to the smart card as follows:
\[
\begin{align*}
W &= g^w \mod n \\
SK &= r^n \mod n \\
M_2 &= h(SK || W || C_1 || RPW_i || d),
\end{align*}
\]

where \(w\) is a random number.

4) The attacker ignores the receiving message \(\{M_2, W\}\) and sends a random \(M_2\) to server \(S_i\).

5) Upon receiving \(M_2\), server \(S_i\) computes \(M'_2 = h(M_2 || C_1 || SK || d)\) and checks whether \(M'_2 = M_2\). 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 \(U_i\) logs in 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:
   
   \[ b' = B \oplus ID_i \oplus PW_i \]
   \[ \text{RPW}' = h(b' \parallel PW_i) \]

2) Checking whether PW' = 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 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 and password PW'. Then, the smart card repeats Steps 1 - 2.

3) According the following equations, the smart card computes $C_1, d$, and $C_3$:
   
   \[ C_1 = C_2 \oplus \text{RPW}_i \]
   \[ d = C_4 \oplus h(C_1 \parallel \text{RPW}_i) \]
   \[ C_3 = h(C_1 \parallel d) \]

4) Comparing $C_3$ with $C_3$ stored inside of the card, if $C_3$ = $C_3$, the following operations are executed.
   
   \[ V = g^{x} \mod n \]
   \[ D = g^{d} \mod n \]
   \[ h(x \parallel y \parallel D) = C_3 \oplus h(C_1 \oplus ID_i) \]
   \[ \text{CID}' = (ID_i) \oplus h(V \parallel h(x \parallel y \parallel D)) \]
   \[ F_1 = \text{RPW}_i \oplus h(C_1 \parallel ID_i) \]
   \[ F_2 = C_4 \oplus h(V \parallel C_1 \parallel y \parallel D) \]
   \[ M_1 = h(ID_i \parallel \text{RPW}_i \parallel V \parallel C_1 \parallel d) \]

   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 $\{\text{CID}_i, V, D, F_1, F_2, M_1, T_i\}$ to server $S_i$.

**B. Authentication**

Server $S_i$ executes the authentication procedure if it receives the login request message $\{\text{CID}_i, V, D, F_1, F_2, M_1, T_i\}$ 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:
   
   \[ ID_i \parallel T'_i = \text{CID}_i \oplus h(V \parallel h(x \parallel y \parallel D)) \]

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 $C_1$, RPW, $C_4$, $d$, and $M_1$ as follows:
   
   \[ C_1 = h(ID_i \parallel x) \]
   \[ \text{RPW}_i = F_1 \oplus h(C_1 \parallel ID_i) \]
   \[ C_2 = F_2 \oplus h(V \parallel C_1) \oplus h(x \parallel y \parallel D) \]
   \[ d = C_4 \oplus h(C_1 \parallel \text{RPW}_i) \]
   \[ M_1 = h(ID_i \parallel \text{RPW}_i \parallel V \parallel C_1 \parallel d) \]

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:
   
   \[ W = g^{w} \mod n \]
   \[ SK = v^{w} \mod n \]
   \[ M_2 = h(SK \parallel W \parallel C_1 \parallel \text{RPW}_i \parallel d) \]

   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.
   
   \[ SK' = W^* \mod n \]
   \[ M_2' = h(SK' \parallel W \parallel C_1 \parallel \text{RPW}_i \parallel d) \]

6) Checking whether $M_2' = M_2$, if the equation is held, the smart card replies with $M_3$ to server $S_i$, where
   
   \[ M_3 = h(M_2 \parallel C_1 \parallel SK' \parallel d) \]

7) Upon receiving $M_3$, server $S_i$ computes $M_3' = h(M_2 \parallel C_1 \parallel SK \parallel d)$ 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 = $g^{w}$ 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 defect, 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:

\[ \text{CID}_i \parallel T_i \parallel h(V \parallel h(x \parallel y \parallel D)) \]

In the authentication phase, with Steps 1-2, the server will reject the login request if the previous request message $\{\text{CID}_i, V, D, F_1, F_2, M_1, T_i\}$ 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:
\[ ID_i || T'_i = \text{CID}_i \oplus h(V \parallel h(x \parallel y \parallel D)) \]

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual authentication</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Forward security</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>User anonymity</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Resist off-line password guessing attack</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Resist replay attack</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Resist man-in-the-middle attack</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Resist forgery attack</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Resist online password guessing with smart card stolen attack</td>
<td>X</td>
<td>V</td>
<td>X</td>
<td>V</td>
</tr>
<tr>
<td>Resist denial of service attack</td>
<td>X</td>
<td>V</td>
<td>X</td>
<td>V</td>
</tr>
</tbody>
</table>

Table III: COMPARISON IN EFFICIENCIES

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Login phase</td>
<td>8T_h+2Texp</td>
<td>3T_h+4T_{ec-ml}+1T_{ec-ml}</td>
<td>4T_h</td>
<td>8T_h+2Texp</td>
</tr>
<tr>
<td>Verification phase (for client)</td>
<td>2T_h+1Texp</td>
<td>1T_h+2T_{ec-ml}</td>
<td>4T_h</td>
<td>2T_h+1Texp</td>
</tr>
<tr>
<td>Verification phase (for server)</td>
<td>10T_h+2Texp</td>
<td>3T_h+8T_{ec-ml}</td>
<td>6T_h</td>
<td>10T_h+2Texp</td>
</tr>
</tbody>
</table>

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;
- \( T_{ec-ml} \): The time to execute a multiplication operation of elliptic curves;
- \( T_{ec-add} \): 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 \( 2T_h+17T_{exp} \) 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 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


