# ROBUST DYNAMIC ID-BASED REMOTE MUTUAL AUTHENTICATION SCHEME

**Toan-Thinh TRUONG, Minh-Triet TRAN, Anh-Duc DUONG**

*Faculty of Information Technology, University of Science, VNU-HCM*

Received September 30, 2011

## ABSTRACT

Dynamic ID based authentication scheme is more and more important in insecure wireless environment and system. Two of kinds of attack that authentication schemes must resist are stealing identity and reflection attack which is a potential way of attacking a challenge- response authentication system using the same protocol in both directions. It must be guaranteed to prevent attackers from reusing information from authentication phase and the scheme of Yoon and Yoo satisfies those requirements. However, their scheme can not resist insider and impersonation attack by using lost or stolen smart card. In this paper, we demonstrate that Yoon and Yoo's scheme is still vulnerable to those attacks. Then, we present an improvement to their scheme in order to isolate such problems.

*Keywords.* Authentication, Password, Dynamic ID, Smart card, Impersonation.

## 1. INTRODUCTION

Communication in network environment is more and more popular. In such insecure environments, especially wireless networks, remote authentication schemes play an important role in communicating between parties. There are many approaches, but one of remarkable solutions is biometrics-based method [1, 2, 3, 4]. Furthermore, many schemes also use elliptic curve to increase security of protocols [5, 6, 7]. However, all these schemes use operations which cost too much such as biometric-algorithm, scalar multiply point or addition point [8]. So, authentication scheme which is based on passwords is considered simple, efficient, and convenient way allowing a legal user to login to remote server securely. There are many papers proposing various ideas to improve password authentication schemes for safe login of legal users [9, 10, 11, 12, 13]. Nevertheless, all these schemes employ static login ID, which is easy for adversaries to steal some information about a user's login message. One solution to ID-theft is to generate different ID of users for each login [14, 15, 16].

In 2005, Liao et al. [15] proposed a dynamic ID-based remote user authentication scheme using smart cards. In this scheme, Liao et al achieved fixing problems existing in Das et al [14] with low cost successfully. Moreover, their scheme also inherits advantages from Das et al [14].

In 2006, E. J. Yoon and K. Y. Yoo [16], however, showed that Liao et al.'s scheme has three security weaknesses as follow: It can not protect against reflection attack. In addition, it can not protect against insider attack. Finally, it cannot protect against impersonation attack by using lost or stolen smart card. E. J. Yoon and K. Y. Yoo proposed a slight modification of Liao et al.'s scheme. They claimed that their proposed scheme not only inherits Liao et al.'s advantages but it also enhances Liao et al.'s security by removing the security weaknesses. In 2010, Tsai et al. [17] pointed weak points of Yoon's scheme. However, their solution employs modular exponentiation which costs too much. Furthermore, timestamp based on two-way authentication can not achieve explicit key confirmation [18, 19].

With above analyses, we will re-prove Yoon's scheme is still vulnerable to a privileged insider's attack and impersonation attacks by using lost or stolen smart card with different solution. Our main ideas are using a random value for each user instead of providing the same key for all and three-way challenge-response handshake technique to resist replay attack better [19]. Then, we present an improvement to the scheme to resist problems existing in Yoon's scheme.

This paper is organized as follows: section 2 quickly reviews and discusses weaknesses of E. J. Yoon and K. Y. Yoo's improving the dynamic ID-based remote authentication scheme. Our proposed scheme is presented in section 3, while section 4 discusses the security and efficiency of the proposed scheme. Our conclusions are presented in section 5.

## 2. REVIEW AND CRYPTANALYSIS OF EUN-JUN YOON AND KEE-YOUNG YOO'S SCHEME

In this section, we review Yoon and Yoo's Improving the dynamic ID-based remote mutual authentication scheme[16] and show that their authentication scheme is vulnerable to insider attack, and impersonation attack with lost or stolen smart card. Before continuing to the main part, we reuse some of the notations used in Yoon and Yoo's paper:

- $U$: The user
- $PW$: The password of $U$
- $S$: The remote system
- $x$: The secret key of $S$
- $y$: The secret number of $S$ stored in each user's smart card
- $T$: A time-stamp
- $h(.)$: A one-way hash function
- $\oplus$ : Bit-wise XOR operation

- $\|$ : Concatenation

### 2.1. Review of Eun-Jun Yoon and Kee-Young Yoo’s scheme

Yoon and Yoo’s scheme includes two phases: a registration phase and an authentication phase. Figure 1 shows Yoon and Yoo’s authentication scheme. The scheme works as follows:

**Registration Phase:** When a new user *U* wants to register with the remote system *S*, he/she performs this phase only once. *S* will issue a smart card to *U* after this phase is done. The steps are as follows:

1. *U* freely chooses a password *PW* and computes $h(PW\|R)$, where *R* is randomly chosen nonce by *U*. He/she submits his/her identity *ID* and $h(PW\|R)$ to *S* through a secure channel.
2. *S* then computes $N=h(PW\|R)\oplus h(ID\|x)$ and $K=h(PW\|R)\oplus h(N\|y)$.
3. *S* stores $(N,y,K,h(.))$ into a smart card and then sends the smart card to *U* through a secure channel.
4. *U* enters *R* into his/her smart card.

In their registration phase, we see that there are two advantages: another user can choose password *PW* and identity *ID* freely. Furthermore, user also can hide his/her password from server by sending a hash value $h(PW\|R)$ instead of only *PW* and at this point, our scheme proposed later completely inherits them. However, due to preparation for our authentication scheme, we only modify our registration phase a little bit by adding a random value *e* for each user’s registration.

**Authentication Phase:** In this phase, when *U* wants to login *S*, *S* can authenticate *U*. The steps of this phase are as follows:

1. *U* inserts his/her smart card into the card reader of a terminal, and keys in his/her *PW* Then, the smart card computes $h(PW\|R)$ and extracts $h(N\|y)$ by computing $K\oplus h(PW\|R)$. The smart card computes $h(N\|y)$ by using stored *N* and *y*, and compares it with extracted hash value $h(N\|y)$. If it is equal, the smart card computes a dynamic *ID* as $CID=h(PW\|R)\oplus h(N\|y\|T)$, $B=h(CID\|h(PW\|R))$, $C=h(T\|N\|B\|y)$, where *T* is a time-stamp.
2. *U* sends $(CID,N,C,T)$ to *S*.
3. Upon receiving the login request at the time *T’*, *S* verifies if whether $(T'-T)\le\Delta T$. If it holds, *S* accepts the login request of *U*, where $\Delta T$ is an expected valid time interval. Then, *S* computes $h(PW\|R)=CID\oplus h(N\|y\|T)$, $B=h(CID\|h(PW\|R))$, and

checks if $C = h(T \| N \| B \| y)$. If it holds, *S* allows *U* to login to the system. Otherwise, *S* rejects it. Then *S* computes $D = h(T^{*} \| B \| y)$, where $T^{*}$ is a time-stamp.

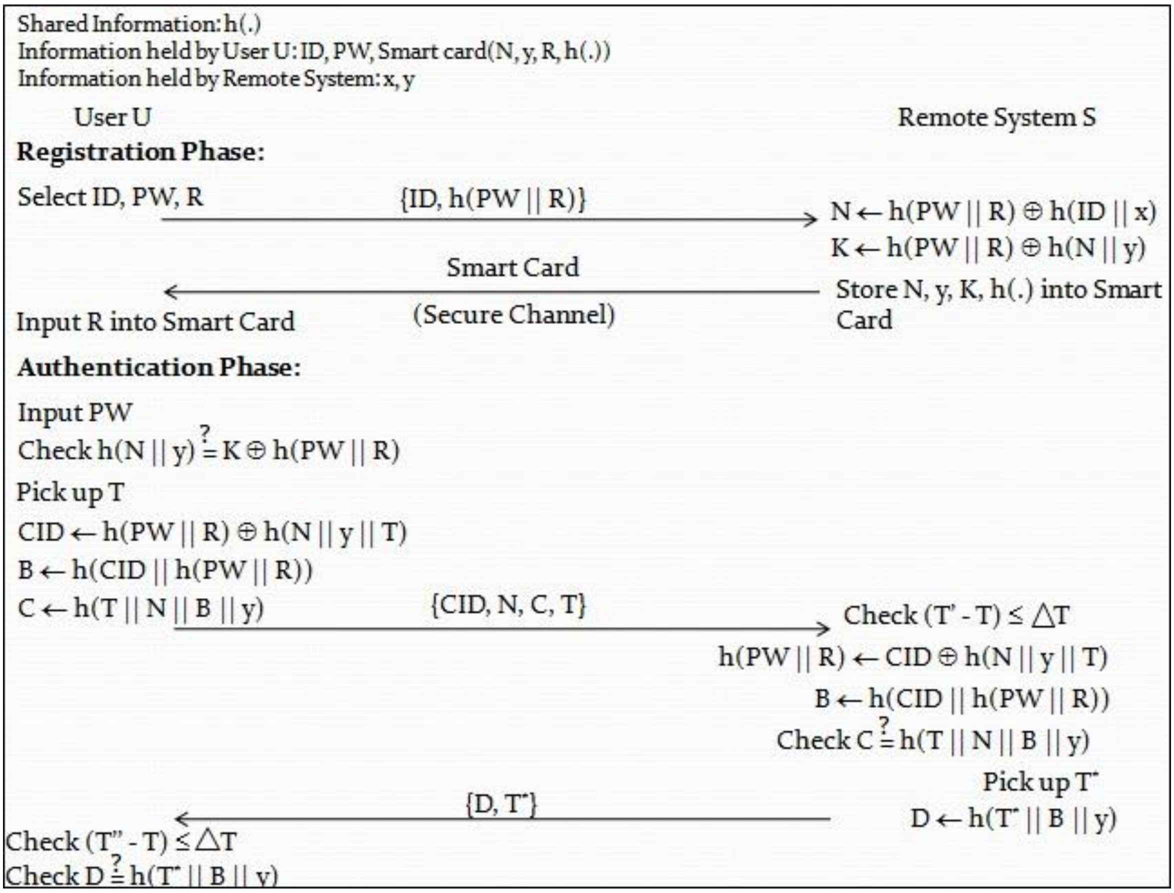

*Figure 1.* Yoon And Yoo Authetication Scheme

4. *S* sends $(D,\ T^{*})$ to *U*.
5. Upon receiving the reply message at the time *T"*, *U* verifies whether $(T" - T^{*}) \leq \Delta T$, where $\Delta T$ is an expected valid time interval. If it holds, *U* computes $h(T^{*} \| B \| y)$ and compares it with the received *D*. If it holds, *U* can be sure that she/he is communicating with the actual *S*.

Due to using the same key *y* provided by server *S*, adversaries easily uses their key *y* to know $h(PW \| R)$ of any legal users by decrypting *CID* which belongs to package *(CID, N, C, T*) transmitted from another user. With $h(PW \| R)$, adversaries can do anything which is analysed in below section to harm user and server.

### 2.2. Cryptanalysis of Yoon and Yoo's Scheme

In this section, we show that Yoon and Yoo's authentication scheme is vulnerable to insider attack, and impersonation attack with lost or stolen smart card.

**Insider Attack:** In paper [16], we see that any legal user can fake *S*. If an attacker is a legal user, he/she will have *y*. So, when other users send *(CID, N, C, T)*, he/she can catch this package. Then, he or she can compute $h(PW\|R) = CID \oplus h(N\|y\|T)$, $B = h(CID\|h(PW\|R))$. With *B*, he/she continues to compute $D = h(T^{*}\|B\|y)$, where timestamp $T^{*}$ is generated by his/herself. Clearly, package $(D, T^{*})$ is legal and it can cheat any legal user that user is communicating with *S*.

**Impersonation Attack by Using Lost or Stolen Smart Card:** In paper the authors mention that this protocol can resist lost or stolen smart card. It is not true because we can demonstrate that if anyone is stolen information of smart card, that user will be impersonated. For example, attacker has $(N, y, K, h(.))$ of *U*. He/she will have by performing $K \oplus h(N\|y)$. With $h(PW\|R)$, the attacker can compute $CID = h(PW\|R) \oplus h(N\|y\|T)$, $B = h(CID\|h(PW\|R))$ and $C = h(T\|N\|B\|y)$. Finally, attacker sends *(CID, N, C, T)* and he/she impersonates *U* successfully.

## 3. PROPOSED SCHEME

In this section, we propose an enhancement to Yoon and Yoo's scheme that removes the security problems described in the previous section. Our improved scheme not only inherits the advantages of their scheme, it also enhances the security of their scheme. Our scheme is also divided into the two phases of registration and authentication. To resist such attacks, the proposed phases perform as follows:

### 3.1. Registration phase

Before we continue to present, we list three requirements for a registration phase: secrecy for information transmitted between user and server, the true password of user should not shown to anyone even the server, and difference between keys provided for each time of registration by server. Easily, we see that Yoon and Yoo's scheme achieved first two requirements but not the last. So, we will recover this point to accomplish a good registration phase.

When a new user *U* wants to register with the remote system *S*, he/she performs this phase only one time. *S* will issue a smart card to *U* after this phase is finished. Figure 2 illustrates the steps of this phase.

1. *U* freely chooses *ID* and password *PW*. Then *U* computes $h(PW\|R)$, where *R* is randomly chosen nonce by *U*. *U* submits *U*'s identity *ID* and $h(PW\|R)$ to *S* through a secure channel.

2. Afterward, server *S* continues to compute $N = h(PW \| R) \oplus h(ID) \oplus h(x \| e)$, $L = h(h(PW \| R) \oplus h(N \| h(y \| e)))$ and $E = h(PW \| R) \oplus h(ID) \oplus h(y \| e)$, where *e* is randomly chosen nonce by *S*.
3. *S* stores (*N*, *L*, *E*, *e*) into a smart card and then sends the smart card to *U* through a secure channel.
4. *U* enters *R* into his/her smart card.

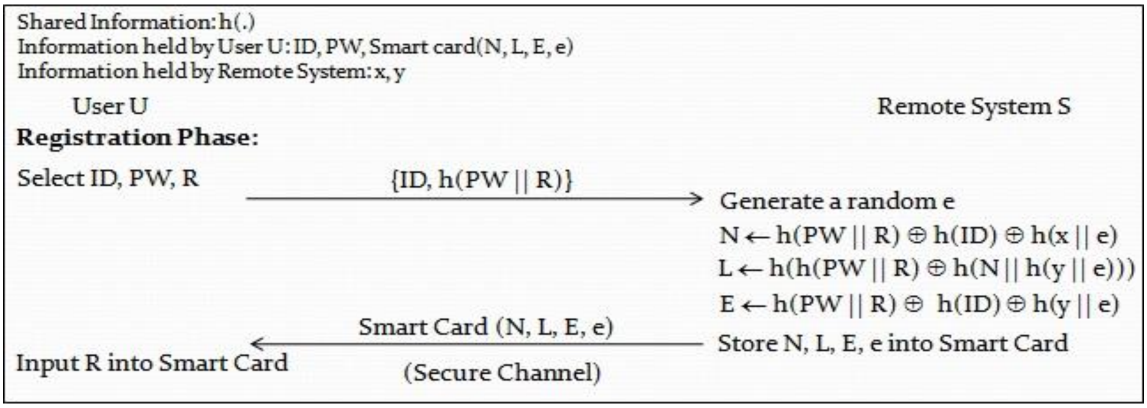
Shared Information: h(.)
Information held by User U: ID, PW, Smart card(N, L, E, e)
Information held by Remote System: x, y
User U
Remote System S
Registration Phase:
Select ID, PW, R
{ID, h(PW || R)}
Generate a random e
N ← h(PW || R) ⊕ h(ID) ⊕ h(x || e)
L ← h(h(PW || R) ⊕ h(N || h(y || e)))
E ← h(PW || R) ⊕ h(ID) ⊕ h(y || e)
Smart Card (N, L, E, e)
Store N, L, E, e into Smart Card
Input R into Smart Card
(Secure Channel)

*Figure 2.* Proposed Registration Phase

In our registration phase, we see that the main difference is a random value e generated by server *S*. With this value, *S* can provide each user with two keys $h(x \| e)$ and $h(y \| e)$, which is not the same at different time.

### 3.2. Authentication Phase

Similarly, we also propose three requirements that help authentication be more secure: user must use a random value to challenge server, server must use a random value to challenge user. And user and server share a secret session key. In Yoon and Yoo's scheme, only user uses time-stamp instead of random value to challenge server but not vice versa and no session key is generate after authenticating successfully. Our phase will fix these weak points. In this phase, when *U* wants to login *S*, *S* can authenticate *U*. Figure 3 illustrates the steps of this phase.

1. *U* inserts *U*'s smart card into the card reader of a terminal, and types in *U*'s *PW* and *ID*. Then the smart card computes $H_1 = h(PW \| R)$ and $H_2 = h(ID)$. Then smart card computes $h(y \| e) = E \oplus H_1 \oplus H_2$. Then smart card continues to compute $L^* = h(H_1 \oplus h(N \| h(y \| e)))$ and compares $L^*$ to *L* stored in smart card. If it is equal, the smart card computes a dynamic *ID* as $CID = H_2 \oplus h(N \| h(y \| e) \| T_1)$, where $T_1$ is a random value chosen by *U*, $B = h(CID \| H_1)$ and $C = h(T_1 \| N \| B \| h(y \| e))$.
2. *U* sends (*CID*, *N*, $T_1$, *C*, *e*) to *S*.

3. On receiving the login request, *S* computes $h(ID) = CID \oplus h(N \| h(y \| e) \| T_1)$, $h(PW \| R) = h(x \| e) \oplus N \oplus h(ID)$. Then *S* computes $B^* = h(CID \| h(PW \| R))$ and $C^* = h(T_1 \| N \| B^* \| h(y \| e))$. Finally *S* checks if $C^* = C$. If it holds, *S* allows *U* to login the system. Otherwise, *S* rejects it. Then *S* computes $D = h(T_2 \| B^* \| h(x \| e))$, where $T_2$ is a random value chosen by *S*.
4. *S* sends *(D, $T_2$ )* to *U*.
5. On receiving the login request, *U* computes $h(x \| e) = N \oplus H_1 \oplus H_2$ and $D^* = h(T_2 \| B \| h(x \| e))$. Then *U* verifies whether $D^* = D$. If it holds, *U* computes hash value $M_1 = h(H_1 \| H_2 \| B \| T_2)$ and session key $SK = h(H_1 \| H_2 \| B \| T_2 \| T_1)$. Then *U* sends $M_1$ to *S*.
6. On receiving $M_1$, *S* computes $M^* = h(h(PW \| R) \| h(ID) \| B^* \| T_2)$ and checks if $M_1 = M^*$. If it is not equal, *S* terminates the session. Otherwise, *S* computes session key $SK = h(h(PW \| R) \| h(ID) \| B^* \| T_2 \| T_1)$.

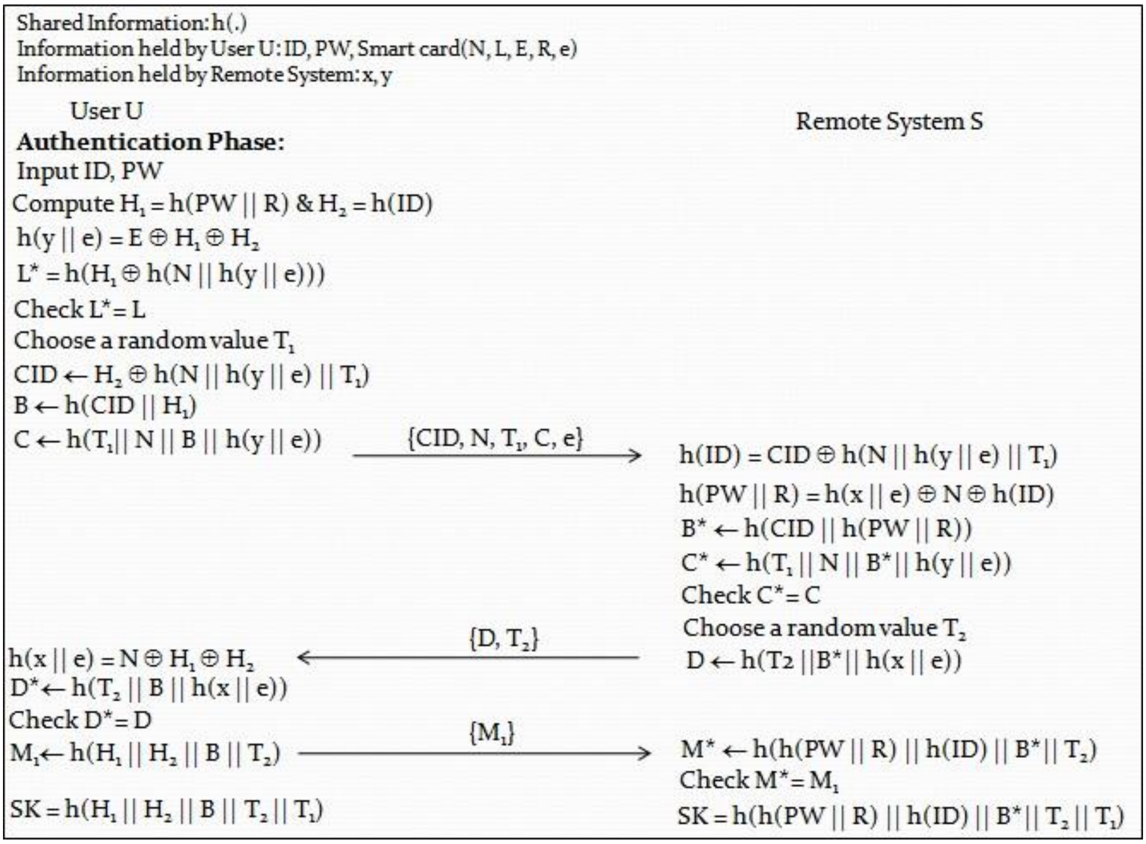
Shared Information: h(.)
Information held by User U: ID, PW, Smart card(N, L, E, R, e)
Information held by Remote System: x, y
User U
Remote System S
Authentication Phase:
Input ID, PW
Compute H₁ = h(PW || R) & H₂ = h(ID)
h(y || e) = E ⊕ H₁ ⊕ H₂
L* = h(H₁ ⊕ h(N || h(y || e)))
Check L* = L
Choose a random value T₁
CID ← H₂ ⊕ h(N || h(y || e) || T₁)
B ← h(CID || H₁)
C ← h(T₁|| N || B || h(y || e))
{CID, N, T₁, C, e}
h(ID) = CID ⊕ h(N || h(y || e) || T₁)
h(PW || R) = h(x || e) ⊕ N ⊕ h(ID)
B* ← h(CID || h(PW || R))
C* ← h(T₁ || N || B* || h(y || e))
Check C* = C
Choose a random value T₂
D ← h(T2 ||B* || h(x || e))
{D, T₂}
h(x || e) = N ⊕ H₁ ⊕ H₂
D* ← h(T₂ || B || h(x || e))
Check D* = D
{M₁}
M₁ ← h(H₁ || H₂ || B || T₂)
M* ← h(h(PW || R) || h(ID) || B* || T₂)
Check M* = M₁
SK = h(H₁ || H₂ || B || T₂ || T₁)
SK = h(h(PW || R) || h(ID) || B* || T₂ || T₁)

*Figure 3.* Proposed authentication phase

Because of using a random value is better time-stamp value [19], we use random values on two user and server sides in our authentication phase to make phase more fair and secure. Moreover, after this phase, user and server share a session key *SK* to encrypt data later.

## 4. SECURITY AND EFFICIENCY ANALYSIS

In this section, we review weak points and strong points of our scheme and analyze it on two aspects: security and efficiency. Our scheme includes two phases, registration and authentication phases.

- Registration phase: User *U* sends $(ID, h(PW \| R))$ to server *S* and *U* receives (*N, L, E, e*). Finally, *U* enters *R* into smart card. The advantage of this phase is user will receive smart card with different information at different time, and the drawback is *PW* chosen by *U*. That *PW* may be a weak password [20], which has a value of low entropy and can be guessed in polynomial time.
- Authentication phase: At first, *U* challenges *S* by sending (*CID*, *N*, $T_1$, C, *e)* to *S*. Then, *S* re-challenges by sending (*D*, $T_2$) to U. And finally, *U* confirm *S* by sending $M_1$ to *S*. After authenticating successfully, *S* and *U* share the same session key *SK*. The advantage of this our phase is all information depend on master key *x* and y, a strong key [20] of *S*, which has a value of high entropy and can not be guessed in polynomial time. And the drawback of this our phase is using more hash operation than previous ones.

### 4.1. Security Analysis

In this section, we present security analyses. Table 1 lists the functionality comparisons between our improved scheme and others. It can be seen that functionality comparisons of our improved scheme is more secure against various attacks.

**Insider attacks:** Unlike Yoon and Yoo's authentication scheme, any legal user can fake *S*. Our scheme bases *x* and *y* that only belong to *S*. So, attacker can not fake *S* to cheat other users. For example, if attacker *A* wants to fake S, *A* must compute *D*. So, *A* must have *B* of user and *x* of *S* to achieve *D*. Clearly, *A* has no way to compute *D* to fake *S* to cheat user. So, our scheme resists insider attacks.

**Impersonation attacks with a lost or stolen smart card:** With information in smart card, attacker cannot compute $h(y \| e)$ to fake user. If attacker *A* wants to have $h(y \| e)$, *A* must have *ID* and *PW* to compute $h(PW \| R) \oplus h(ID) \oplus E$ to get $h(y \| e)$. It is obvious that *A* has no way to have *ID* and *PW* of user. So, our scheme resists impersonation attacks with a lost or stolen smart card.

**Replay attacks:** If attacker uses old login message *(CID, N,* $T_1$, *C, e*) to cheat *S*, he/she will fail at step 5 due to not having B, $h(PW \| R)$ and *h(ID)* to compute $M_1$ to cheat *S*. So, our scheme resists replay attacks.

**Known-key attacks:** Known-key attacks mean that compromise of a past session key cannot derive any further session key. In our scheme, the session key *SK* is associated with *B*, *h(ID)* and $h(PW\| R)$, which are unknown to the adversary. Even though the past session key *SK* is disclosed, the attacker cannot know *B*, *h(ID)* and $h(PW\| R)$. Thus, the attacker can not obtain any further session key.

**Achieving mutual authentication and session key agreement:** In our scheme, firstly the user authenticates the server and then server authenticates the user with three-way challenge-response handshake technique. After mutual authentication, the user and server share the common session key to encrypt messages later. In our scheme, server sends ($D$, $T_2$) to user after receiving ($CID$, $N$, $T_1$, $C$, $e$) from user. Then user authenticates server by checking the condition $D^* = D$. Afterward, user sends $M_1$ to server and server authenticates user by checking $M^* = M_1$. Therefore, the mutual authentication and session key agreement are performed securely in our scheme.

**Password guessing attacks:** Like Yoon and Yoo’s scheme, our scheme bases *PW* and *R*. Even attacker can guess *PW* of *U*, she/he can not login *S* without random *R*. So our scheme can resist guessing attacks. In addtion to attacks above, our scheme also achieves three properties that belong to previous schemes, user’s anonymity, reflection attack and no verification table.

*Table 1.* The functionality comparison between our scheme and the others

| | *Liao et al [15]* | *Yoon and Yoo [16]* | *Ours* |
|---|---|---|---|
| Insider attack | No | No | Yes |
| Impersonation attack | No | No | Yes |
| Known-key attack | No | No | Yes |
| Mutual authentication | No | Yes | Yes |
| Session key exchange | No | No | Yes |
| User anonymity | Yes | Yes | Yes |
| Replay attack | No | Yes | Yes |
| No verification table | Yes | Yes | Yes |
| Reflection attack | No | Yes | Yes |

### 4.2. Efficiency Analysis

To compare efficiency between our scheme and the two previous ones proposed by Liao et al and Yoon and Yoo, we reuse approach used in those previous schemes to analyze computational complexity. That is, we calculate the number of one-way hash function execution.

Let $T_h$ be the time to compute one-way hash function.

In Liao et al's scheme, $U$ needs 1 × $T_h$ for $h(PW)$ and $S$ needs 1 × $T_h$ for $N$ in registration phase. In authentication phase, $U$ needs 2 × $T_h$ for $CID$, 1 × $T_h$ for B, and 1 × $T_h$ for $C$. $U$ checks $D$ that needs 1 × $T_h$. In the same phase, $S$ computes $CID \oplus h(N \oplus y \oplus T)$ that needs 1 × $T_h$, computes $B$ needs 1 × $T_h$, computes $h(T \oplus N \oplus B \oplus y)$ that needs 1 × $T_h$, and computes $h(T^* \oplus N \oplus B \oplus y)$ needs 1 × $T_h$.

In Yoon and Yoo's scheme, $U$ computes $h(PW \| R)$ that needs 1 × $T_h$ and $S$ computes $N$ and $K$ that need 2 × $T_h$ in registration phase. In authentication phase of Yoon and Yoo's scheme, $U$ computes $h(N \| y)$ that needs 1 × $T_h$, $h(PW \| R)$ needs 1 × $T_h$, $CID$ needs 1 × $T_h$, computes $B$ that needs 1 × $T_h$, and computes $C$ that needs 1 × $T_h$. $U$ checks $D$ needs 1 × $T_h$. In the same phase, $S$ computes $h(N \| y \| T)$ that needs 1 × $T_h$, $B$ needs 1 × $T_h$, computes $h(T \| N \| B \| y)$ that needs 1 × $T_h$, and computes $h(T^* \| B \| y)$ that needs 1 × $T_h$.

In our scheme, $U$ computes $h(PW \| R)$ that needs 1 × $T_h$ and $S$ computes $N$, $L$ and $E$ that need 5 × $T_h$ in registration phase. In authentication phase of our scheme, $U$ computes $h(y \| e)$ that needs 2 × $T_h$, $L^*$ that needs 2 × $T_h$, $CID$ that needs 1 × $T_h$, $B$ that needs 1 × $T_h$ and $C$ that needs 1 × $T_h$. $U$ checks $D$ needs 1 × $T_h$ and computes $M_1$ that needs 1 × $T_h$. In the same phase, $S$ computes $h(ID)$ that needs 2 × $T_h$, $h(PW \| R)$ that needs 1 × $T_h$, $B$ that needs 1 × $T_h$ and $C^*$ that needs 1 × $T_h$. $S$ computes $D$ that needs 1 × $T_h$ and checks $M_1$ that needs 1 × $T_h$.

We can see that the number of hash operation in our registration phase needs more three times than Yoon and Yoo's. However, registration phase is performed one time for each user. And our authentication scheme needs more six times than Yoon and Yoo's. Nevertheless, this increase is necessary to enhance security stronger than previous schemes.

*Table 2.* A comparision of computation costs

| *Computational type* | *Liao et al[15]* | *Yoon and Yoo[16]* | *Ours* |
|---|---|---|---|
| Registration Phase | 2 × $T_h$ | 3 × $T_h$ | 6 × $T_h$ |
| Authentication Phase | 9 × $T_h$ | 10 × $T_h$ | 16 × $T_h$ |

## 5. CONCLUSIONS

In this paper, we review dynamic ID-based remote mutual authentication scheme of Yoon and Yoo. Although their scheme is secure against reflection attack, we see that their scheme is vulnerable to insider, impersonation by using stolen smart card attacks. So, we propose an improved scheme to eliminate such problems. Compared with related schemes, the proposed scheme has the following main advantages; (1) User can choose the password freely. (2) It provides secure user anonymity. (3) It does not hold the password verification table for users. (4)

It provides mutual authentication and session key agreement. As a result, the proposed scheme is able to provide greater security and be practical in wireless communication systems.

In the future, however, we will study a remote mutual authentication scheme on elliptic curve cryptosystem (ECC) using smart card to enhance security more and apply to more applications in electronic transactions.

## REFERENCES

1. C. H. Lin and Y. Y. Lai - A flexible biometrics remote user authentication scheme, Computer Standards & Interfaces **27** (1) (2004) 19-23.
2. C. T. Li and M. S. Hwang - An efficient biometrics-based remote user authentication scheme using smart cards, Journal of Network & Computer Applications **33** (1) (2010) 1-5.
3. X. Li, J. Niu, J. Ma, W. Wang, and C. L. Liu - Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards, J. Network & Computer Applications **34** (1) (2011) 73-79.
4. M. K. Khan and J. Zhang - Improving the security of ‘a flexible biometrics remote user authentication scheme’, Computer Standards & Interfaces **29** (1) (2007) 82-85.
5. J. H. Yang and C. C. Chang - An id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Computers & Security **28** (3 – 4) (2009) 138-143.
6. E. J. Yoon and K. Y. Yoo - Robust id-based remote mutual authentication with key agreement scheme for mobile devices on ecc, in *CSE* (2) (2009) 633-640.
7. S. T. Wu, J. H. Chiu, and B. C. Chieu - ID-based remote authentication with smart cards on open distributed system from elliptic curve cryptography, BT 2005 IEEE International Conference on Electro Information Technology, May 22, 2005 - May 25, 2005. Inst. of Elec. and Elec. Eng. Computer Society, 2005.
8. T. H. Chen, Y. C. Chen, W. K. Shih, and H. W. Wei - An efficient anonymous authentication protocol for mobile pay-tv, **34** (2011) 1131-1137.
9. L. H. Li, I. C. Lin, and M. S. Hwang - A remote password authentication scheme for multi-server architecture using neural networks, IEEE Transactions on Neural Network **12** (6) (2001) 1498-1504.
10. J. J. Shen, C. W. Lin, and M. S. Hwang - A modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics **49** (2) (2003) 414-416.
11. L. Lamport - Password authentication with insecure communication, Communications of the ACM **24** (1981) 770-772.
12. M. S. Hwang, C. C. Lee, and Y. L. Tang - A simple remote user authentication scheme,

Mathematical & Computer Modeling **36** (2002) 103-107.

13. C. C. Lee, M. S. Hwang, & W. P. Yang - Flexible remote user authentication scheme using smart cards, IEEE Transactions on Neural Network **36** (3) (2002) 46-52.
14. M. L. Das, A. Saxena, and V. P. Gulati - A dynamic id-based remote user authentication scheme, IEEE Transactions on Consumer Electronics **50** (2) (2004) 629-631.
15. I. E. Liao, C. C. Lee, and M. S. Hwang - Security enhancement for a dynamic id-based remote user authentication scheme, International Conference on Next Generation Web Services Practices **6** (2) (2005) 517-522.
16. E. J. Yoon and K. Y. Yoo - Improving the dynamic id-based remote mutual authentication scheme, First International Workshop on Information Security **4277** (2006) 499-507.
17. J. L. Tsai, T. C. Wu, and K. Y. Tsai - New dynamic id authentication scheme using smart cards, Int. J. Communication Systems **23** (12) (2010) 1449-1462.
18. D. He, J. Chen, and J. Hu - Weakness of two id-based remote mutual authentication with key agreement protocols for mobile devices, IACR Cryptology ePrint Archive (2010) 606.
19. S. H. Islam and G. P. Biswas - A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Journal of Systems & Software **84** (11) (2011) 1892-1898.
20. A. Menezes, P. Oorschot, and S. Vanstone - Handbook of applied cryptograph, 1997.

*Corresponding author:*

Toan-Thinh TRUONG

Faculty of Information Technology, University of Science, VNU_HCM

Email: *ttthinh@sdcontent.org*