**ISBN** 978-981-11-7861-0
**Proceedings of 2018 the 8th International Workshop on Computer Science and Engineering (WCSE 2018)**
*Bangkok, 28-30 June, 2018, pp. 605-609*
doi: 10.18178/wcse.2018.06.101

# A Dynamic Identity Mutual Authentication Scheme Based on Smart Card

Dengya Wan [1], Lei Wang [2] and Daren Zha [1+]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[1] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
[2] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

**Abstract.** In 2013, Chang YF et al. proposed an untraceable dynamic-identity-based remote user authentication scheme. This scheme can achieve mutual authentication and a verification table is no needed. Then, Li X et al. demonstrated that Chang YF et al.'s scheme suffers from offline password guessing attack and stolen smart card attack, and it is inefficient in wrong password verification. In this paper, an enhanced scheme is presented for improving the security. It protects the private key $x$ of the server by the discrete logarithm and resists attacks by calculating the user $ID_i$ and the random number. Moreover, the password change phase is more efficient.

**Keywords:** authentication, security, smart card, password.

## 1. Introduction

With the rapid development of the Internet, the relationship between people's lives and the network is getting closer and closer. Therefore, more attention has been paid to the security of the Internet. Identity authentication is one of the methods to solve the security problems, which authenticates the identity of users in a public environment in order to he/she can access the resources of the server. Among the identity authentication methods, the password authentication is one of the simplest and the most convenient authentication mechanisms to verify the legitimacy of the users. However, these schemes based on password have to maintain a verification table [1, 2, 4, 5]. This will increase the probability of being attacked. To avoid these problems, some password authentication schemes that don't need password tables have been proposed. In 2004, Das et al.[3] proposed a remote user authentication scheme based on dynamic identity identification. They claimed that the scheme can resist a series of attacks, such as password guessing attack, reply attack, insider attack, forgery attack and so on. But Chien HY [6], Liao IE [7], Ku WC [8] et al. pointed out that Das et al.'s scheme was insecure because it could not achieve anonymity, resist guessing attacks and resist the insider attacks, which made it work like an open channel.

To enhance the security, some authentication schemes based on smart card have been proposed. Also, comparing with the password authentication, these schemes are convenient and have secure computation [9, 10, 11, 12, 13, 14]. In 2013, Chang YF et al .[15] proposed a untraceable dynamic-identity-based remote user authentication scheme. In the next year, Li X et al. [16] pointed out that Chang YF et al.'s scheme could not resist stolen smart card attack, insider attack, offline password guessing attack, impersonation attack and so on. Aiming at some of the security weaknesses proposed by Li X et al., our work is to achieve a more secure and efficient scheme based on the Chang YF et al.'s scheme.

+ Corresponding author. Tel.: + 01082546335; fax: + 01082546335.
*E-mail address*: zhadaren@iie.ac.cn.

## 2. Review Chang YF et al.'s Scheme

### 2.1. Registration phase

(1) The user is free to choose his own identity $ID_i$ and the password $PW_i$, and then send them to the server $S$ through a secure channel.
(2) After receiving the registration request, the server $S$ calculates $N_i = h(ID_i||x) \oplus h(PW_i)$.
(3) $S$ selects a smart card for the user $U_i$ and stores the parameters $\{N_i, y, h(\cdot)\}$ into the smart card.
(4) $S$ sends the smart card to the user $U_i$ securely.

### 2.2. Login phase

(1) The smart card generates the current timestamp $T$ and calculates $CID_i = ID_i \oplus h(N_i||y||T)$, $N_i' = N_i \oplus h(y||T)$, $B = N_i \oplus h(PW_i) = h(ID_i||x)$, $C = h(N_i||y||B||T)$.
(2) The smart card sends the login information $\{CID_i, N_i', C, T\}$ to the server $S$ through the common channel.

### 2.3. Authentication phase

(1) $S$ check whether $(T' - T) \leq \Delta T$ and there is the same information $\{CID_i, N_i', C, T'\}$ between $T - \Delta T$ and $T + \Delta T$. If it is not satisfied, $S$ will discard information $\{CID_i, N_i', C, T'\}$ and end the authentication phase.
(2) $S$ computes $N_i^* = N_i' \oplus h(||y||T)$, $ID_i^* = CID_i \oplus h(N_i^*||y||T)$, $B^* = h(ID_i^*||x)$, $C^* = h(N_i^*||y||B^*||T)$.
(3) $S$ checks whether $C^*$ is equal to the received C. If they are equal, $U_i$ is authenticated by $S$ successfully. Then $S$ computes $a = h(B^*||y||T'')$, where $T''$ is the current timestamp. Otherwise, $S$ rejects the login request for $U_i$ and records the value of $ID_i$. If the login request from $ID_i$ has failed three times, $S$ will ignore the login of user $U_i$ for a period time.
(4) $S$ sends $\{a, T''\}$ to the smart card via the common channel.
(5) After receiving $\{a, T''\}$, the smart card first checks the freshness of $T''$. If $T''$ is fresh in an expected time interval, the smart card computes $a^* = h(B||y||T'')$ and compares whether $a^*$ is equal to $a$. If they are equal, the server $S$ is authenticated by the user $U_i$.

### 2.4. Password change phase

(1) The user $U_i$ inserts the smart card into the terminal device and enters the $ID_i$ and $PWi$, and then the smart card sends the password change request.
(2) The smart card computes $CID_i = ID_i \oplus h(N_i||y||T)$, $N_i' = N_i \oplus h(y||T)$, $B = N_i \oplus h(PW_i) = h(ID_i||x)$, $C = h(N_i||y||B||T)$, where $T$ is the current timestamp.
(3) The smart card sends $\{CID_i, N_i', C, T\}$ and password change request to the server $S$ via the common channel.
(4) After receiving the information $\{CID_i, N_i', C, T\}$ and password change request from the smart card, $S$ checks whether $(T' - T) \leq \Delta T$ and whether there is the same parameters information $\{CID_i, N_i', C, T'\}$ and password change request between $T - \Delta T$ and $T + \Delta T$. If it is not satisfied, $S$ will discard information $\{CID_i, N_i', C, T'\}$ and terminate the authentication phase.
(5) The server $S$ computes $N_i^* = N_i' \oplus h(||y||T)$, $ID_i^* = CID_i \oplus h(N_i^*||y||T)$, $B^* = h(ID_i^*||x)$, $C^* = h(N_i^*||y||B^*||T)$.
(6) $S$ checks whether $C^*$ is equal to the received $C$. If they are equal, $U_i$ is authenticated by $S$ successfully. Then $S$ computes $a = h(B^*||y||m||T'')$, where $T''$ is the current timestamp and $m$ is the reply to the password change request. Otherwise, $S$ rejects the login request for $U_i$ and records the value of $ID_i^*$. If the login request from Idi has failed three times, S will ignore the login of user $U_i$ for a period time.
(7) $S$ sends $\{a, m, T''\}$ to the smart card via a common channel.
(8) After receiving $\{a, m, T''\}$, the smart card first checks the freshness of $T''$. If $T''$ is fresh in an expected time interval, the smart card computes $a^* = h(B||y||m||T'')$ and compares whether $a^*$ is equal to $a$. If they are equal, the server $S$ is authenticated by the user $U_i$.
(9) If the password change request is verified, the smart card will ask the user $U_i$ to enter the new password $PW_i^{new}$ twice to ensure that the password is correct. If the entered password is inconsistent, the user will be asked to enter the new password again. If the inputted passwords are the same, the smart card computes $N_i^* = N_i \oplus h(PW_i) \oplus h(PW_i^{new})$ and replaces $N_i^*$ with $N_i$.

## 3. Security Analysis of Chang YF et al.'s Scheme

Li X et al. [16] pointed out that Chang YF [15] et al.'s scheme can not achieve untraceability and suffers from offline password guessing attack and stolen smart card attack. Besides, it is inefficient in wrong password verification.

### 3.1. Untraceability

The attacker $U_a$ obtains the information $\{y, h(\cdot)\}$ stored in the smart card by the side channel attack through his own smart card. And $U_a$ can eavesdrop the user's login information $\{CID_i, N_i', C, T\}$. Then $U_a$ can compute $N_i' = N_i \oplus h(y||T)$, $ID_i = CID_i \oplus h(N_i||y||T)$, so the attacker can get the user $U_i$'s real $ID_i$, which leads to the traceability.

### 3.2. Offline Password Guessing Attack

As can be seen from Section 3.1, the attacker $U_a$ can eavesdrop the information $\{CID_i, N_i', C, T\}$ and obtain $\{N_i, ID_i\}$. $U_a$ can guess $PW_i^*$ from the dictionary and compute $B^* = N_i \oplus h(PW_i^*)$, $C^* = h(N_i||y||B^*||T)$. Then Ua checks whether $C^*$ is equal to $C$. If they are equal, $U_a$ finds the correct password PW. Otherwise, $U_a$ will repeat the process until find the correct password. Therefore, the scheme can not resist offline password guessing attacks.

### 3.3. Stolen Smart Card Attack

Suppose that $U_a$ can eavesdrop on login information $\{CID_i, N_i', C, T\}$ and extract the parameters $\{N_i, y, h(\cdot)\}$ from the stolen smart card. $U_a$ can compute $ID_i = CID_i \oplus h(N_i||y||T)$. According to Section 3.2, $U_a$ can guess the correct password of the legal user $U_i$. It means that the attacker can access the server by using the stolen smart card. Therefore, it can not resist smart card stolen attack.

### 3.4. Inefficient in Wrong Password Verification and Password Change

Chang YF et al.'s scheme verifies the password in the authentication phase. Similarly, in the password change phase, if the user enters the wrong password, the server will stop the change until it finds that $C^*$ is not equal to $C$, which is not only unreasonable but also wastes unnecessary communication costs. The password update phase can be designed at the smart card terminal, which will be more efficient.

## 4. Improved Scheme

### 4.1. Registration Phase

(1) The user $U_i$ chooses identity $ID_i$, password $PW_i$ and a random number $k$, then the smart card computes $h(ID_i \oplus k)$ and sends $h(ID_i \oplus k)$ to the server S through a secure channel.

(2) After receiving the registration request, $S$ selects a cyclic group G whose order is $p$ and generator is $g$ and computes $A = g^x \bmod p$, $M_i = h(ID_i \oplus k) \oplus h(PW_i || A)$, $N_i = h(ID_i \oplus k) || x \oplus h(PW_i || A)$, $P_i = h(ID_i \oplus k) || h(PW_i || A)$. Then the server $S$ will store $(ID_i \oplus k \oplus x)$ in itself locally.

(3) The server $S$ chooses a smart card and stores the parameters $\{M_i, N_i, P_i, y, h(\cdot), A\}$ in the smart card.

(4) The server $S$ issues the smart card to the user $U_i$ securely.

### 4.2. Login Phase

(1) The smart card first computes $h(ID_i \oplus k) = M_i \oplus h(PW_i || A)$, $P_i^* = h(ID_i \oplus k) || h(PW_i || A)$, and then compares $P_i$ with $P_i^*$. If $P_i^* = P_i$, the login phase continues. Otherwise, the login phase terminates.

(2) The smart card generates the current timestamp $T$ and random number $n$, and computes $B = N_i \oplus h(PW_i || A)$, $CID_i = h(ID_i \oplus k) || h(B || y || T || n)$, $C = h(CID_i || B || y || T) || n$, $Q_i = n \oplus B$.

(3) The smart card sends the login message $\{CID_i, Q_i, C, T\}$ to the server $S$ through a common channel.

### 4.3. Authentication Phase

(1) The server $S$ first checks the freshness of the timestamp $(T' - T) \leq \Delta T$. If it is satisfied, the server will extract the information $(ID_i \oplus k \oplus x)$ stored in itself and get $(ID_i^* \oplus k)$. Otherwise, the server S will end the authentication phase.

(2) The server $S$ computes $B^* = h(ID_i^* \oplus k) || x$, $n^* = Q_i \oplus B^*$, $CID_i^* = h(ID_i^* \oplus k) || h(B^* || y || T || n^*)$, $C^* = h(CID_i^* || B^* || y || T) || n^*$.

(3) *S* checks that whether $C^*$ is equal to $C$. If they are equal, the user $U_i$ is successfully authenticated by S. The server *S* computes $a = h(B^* || y || T'')$, where $T''$ is the current timestamp.
(4) The server *S* sends the information $\{a, T''\}$ to the smart card.
(5) The smart card first checks the freshness of the timestamp $(T'' - T') \leq \Delta T$. If it is satisfied, the smart card will compute $a^* = h(B || y || T'')$ and then compare $a^*$ with $a$. If $a^*$ is equal to $a$, the server *S* has been authenticated by the user $U_i$ successfully. Otherwise, the authentication phase will terminate directly.

### 4.4. Password Change Phase

(1) The user $U_i$ inserts the smart card into the terminal device and enters the $ID_i$ and $PW_i$.
(2) The smart card computes $h(ID_i \oplus k) = M_i \oplus h(PW_i || A)$, $P_i^* = h(ID_i \oplus k) || h(PW_i || A)$ and compares $P_i$ with $P_i^*$. If $P_i^* = P_i$, it sends password change request to the server *S*.
(3) After the server *S* receives the password change request, the user $U_i$ enters the changed password $PW_i^{new}$. *S* chooses a big prime number $p$ and generator $g$ randomly, and then computes $A = g^x \bmod p$ $M_i = h(ID_i \oplus k) \oplus h(PW_i^{new} || A)$, $N_i = h(ID_i \oplus k) || x \oplus h(PW_i^{new} || A)$, $P_i = h(ID_i \oplus k) || h(PW_i^{new} || A)$
(4) The server *S* stores the parameters $\{M_i, N_i, P_i, y, h(\cdot), A\}$ in the smart card.
(5) The server *S* issues the smart card to the user securely.

After the password has been changed, the smart card can check whether $P_i^* = P_i$ and computes the value $B, CID, C$ when the user $U_i$ wants to access the server the next time because $P_i$ has been update.

## 5. The Security Analysis of the Improved Scheme

### 5.1. Untraceability

As can be seen from the process of the scheme, the identity information of the user is stored in $(ID_i \oplus k \oplus x)$. But the information of *x* is from *A* and it is impossible that the attacker $U_a$ gets *x* from *A* because of the discrete logarithm problem and random number *k*. So the attacker $U_a$ cannot get the user $U_i$'s identity, which achieves the untraceability.

### 5.2. Offline Password Guessing Attack

Suppose that the attacker $U_a$ can guess the password $PW_i^*$ from the dictionary and get the parameters $\{M_i, N_i, P_i, y, h(\cdot), A\}$ by side channel attack and eavesdrop the login information $\{CID_i, Q_i, C, T\}$. The attacker still cannot verify the correctness of the password $PW_i^*$. Even though the attacker $U_a$ can compute $B^* = N_i \oplus h(PW_i^* || A)$, he cannot guess the random number *n* generated by the smart card. The reason is that *n* is related to *x* whose value cannot be solved because of the discrete logarithm problem. So $U_a$ cannot get the values of $CID_i^* = h(ID_i \oplus k) || h(B^* || y || T || n)$, $C^* = h(CID_i || B^* || y || T) || n$ so that he is unable to compare $C$ with $C^*$ to verify the correctness of $PW_i^*$. Therefore, the scheme can resist offline password guessing attack.

### 5.3. Efficient Password Verification

Li X et.al argued that the scheme proposed by Chang YF et.al is efficient when the user wants to change his password and the smart card checks whether the password is correct. Because whether you verify passwords or change passwords, you have to verify that whether $C$ and $C^*$ are equal, wasting time. The improved scheme can verify the correctness of the password in the smart card according to $P_i$ and $P_i^*$. And as can be seen from password change phase, the process of changing password does not need to compare $C$ and $C^*$, which makes it more efficient to verify the password and change the password.

## 6. Conclusion

This paper proposes a dynamic identity authentication scheme to enhance the security of Chang YF [15] et al.'s scheme. It achieves untraceability and resists offline password guessing attack. Moreover, the wrong password verification and password change is more efficient because the phase occurs in the smart card rather than in the server.

## 7. Acknowledgements

This work was partially supported by Strategy Cooperation Project AQ-1702, AQ-17014 and National Natural Science Foundation of China No. U163620068.

# 8. References

[1] C. K. Chan, and L. M. Cheng, Cryptanalysis of a remote user authentication scheme using smart cards. *IEEE Trans. on Consumer Electron*., vol. 46, no. 4, pp. 992-993, Nov. 2000.

[2] IEEE P1363.2 Draft D12, Standard Specifications for Password-Based Public Key Cryptographic Techniques, *IEEE P1363 working group*, 2003.

[3] Das ML, Saxena A, Gulati VP. A dynamic ID-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics* 2004; 50(2):629–631.

[4] Hwang MS, Li LH. A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics 2000*; 46(1):28–30.

[5] C. C. Lee, L. H. Li, and M. S. Hwang, A remote user authentication scheme using hash functions. *ACM Operating Systems Review*, vol.36, no.4, pp.23-29, 2002.

[6] Chien HY, Chen CH. A remote authentication scheme preserving user anonymity. *International Conference on AINA'*05, Vol. 2, 2005; 245–248.

[7] Liao IE, Lee CC, Hwang MS. Security enhancement for a dynamic ID-based remote user authentication scheme. *Proceedings of the International Conference on Next Generation Web Services Practices*, NWeSP' 05, Seoul, Korea, 2005; 437–440

[8] Ku WC, Chen SM. Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics* 2004; 50(1):204–207.

[9] C. C. Lee, M. S. Hwang, and W. P. Yang. A flexible remote user authentication scheme using smart cards. *ACM Operating Systems Review*, vol.36, no.3, pp.46-52, July 2002.

[10] Ramasamy R and Muniyandi A P. An Efficient Password Authentication Scheme for Smart Card. *IJ Network Security*, vol.14, no.3, pp. 180-186,2012.

[11] J. J. Shen, C. W. Lin, and M. S. Hwang. A modified remote user authentication scheme using smart cards. *IEEE Trans. on Consumer Electron.*, vol.49, no.2, pp.414-416, May 2003.

[12] Hwang MS, Li LH. A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics* 2000; 46(1):28–30.

[13] Wang YY, Liu JY, Xiao FX, DanJ. A more efficient and secure dynamic ID-based remote user authentication scheme. *Computer Communications* 2009; 32(4):583–585.

[14] Yeh KH, Su CH, Lo NW, Li YJ, Huan YX. Two robust remote user authentication protocols using smart cards. *Journal of Systems and Software* 2010; 83(12):2556–2565.

[15] Chang YF, Tai WL, Chang HC. Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update. *International Journal of Communication Systems* 2013; in press. DOI: 10.1002/dac.2552.

[16] Li X, Niu J, Liao J and Liang W. Cryptanalysis of a dynamic identity‐based remote user authentication scheme with verifiable password update. *International Journal of Communication Systems*,vol.28, no.2, pp. 374-382,2014.