ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2012, Vol. 41, No. 1

A SECURE PASSWORD-BASED REMOTE USER AUTHENTICATION SCHEME WITHOUT SMART CARDS

Bae-Ling Chen[1], Wen-Chung Kuo[2*], Lih-Chyau Wuu[3]

[1] *Graduate School of Engineering Science and Technology*
National Yunlin University of Science and Technology
No. 123, Section 3, University Road, Douliu, Yunlin 64002, Taiwan
e-mail: chenbl@yuntech.edu.tw

[2]*Department of Computer Science and Information Engineering*
National Yunlin University of Science and Technology
No. 123, Section 3, University Road, Douliu, Yunlin 64002, Taiwan
e-mail: simonkuo@yuntech.edu.tw

[3]*Institute of Computer Science and Information Engineering*
National Yunlin University of Science and Technology
No. 123, Section 3, University Road, Douliu, Yunlin 64002, Taiwan
e-mail: wuulc@yuntech.edu.tw

crossref http://dx.doi.org/10.5755/j01.itc.41.1.975

Abstract. There are many remote user authentication schemes proposed in literature for preventing unauthorized parties from accessing resources in an insecure environment. Due to inherent tamper-resistance, most of them are based on smart card authentication schemes. Unfortunately, the cost of cards and readers makes these schemes costly. In the real world, common storage devices, such as universal serial bus (USB) thumb drives, portable HDDs, mobile phones, Laptop or Desktop PCs, are widely used, and they are much cheaper or more convenient for storing user authentication information. However, since these devices do not provide tamper-resistance, it is a challenge to design a secure authentication scheme using these kinds of memory devices. In this paper, we will propose a secure password-based remote user authentication and key agreement scheme without using smart cards. According to our analysis, the proposed scheme guarantees mutual authentication and also resists off-line dictionary, replay, forgery, and impersonation attacks. Compared to related scheme, the proposed scheme's computation cost is lower and the total message length is shorter. Therefore, our scheme is suitable even for applications in limited power computing environments.

Keywords: password-based; remote access; tamper-resistant; mutual authentication; impersonation attack.

1. Introduction

With the increasing number of systems that provide services over open networks, remote authentication is critical for preventing unauthorized parties from accessing remote system resources. Smart cards are the most commonly used mechanism in password-based remote user authentication schemes. Smart card-based authentication schemes [5] provide strong authentication and reduce the risk of server side verification tables being tampered with using Lamport's authentication scheme [9]. In order to improve security and efficiency, many authentication schemes have been proposed [1, 4-7, 10-11, 14-15, 17-18] in the last decade.

Smart cards are usually adopted to store the personal secret information such as authentication information. Though smart card-based authentication schemes come with a tamper-resistant property, when a smart card is lost, the card holder needs to worry about the damage arising from the loss of the smart card. Especially since there is research showing smart card content being extracted by off-line passive power analysis [8]. Using tamper-resistant devices does not guarantee that an authentication scheme is secure against all risks. In addition, the cost of the necessary

[*] Corresponding author

infrastructure for smart card-based schemes, such as the cards and readers add substantially to the cost. In the real world, common storage devices, such as USB thumb drives, portable HDDs, mobile phones, and Laptop or Desktop PCs, are much cheaper or more convenient for storing user authentication information issued from the system server. However, since these common storage devices come without tamper-resistance, it is a big challenge to design a secure authentication scheme using these memory devices.

In 2009, Rhee *et al.* [12] analyzed the security of two remote authentication schemes proposed by Fan *et al.* [4] and Khan and Zhang [7], respectively. Rhee *et al.* showed that the two schemes are vulnerable to impersonation attacks when the tamper-resistant property is eliminated from smart-card-based schemes; in other words, if any user in those two schemes is using insecure storage instead of using a tamper-resistant device such as a smart card, the user authentication procedure is insecure against impersonation attacks. In order to mitigate this weakness and enhance security when using insecure storage device, Rhee *et al.* proposed a remote user authentication scheme (RKL-scheme for short) based on ElGamal's public key cryptosystem [3]. They stated that their scheme provides mutual authentication with no verification table at the cost of only two messages for login and authentication protocols. They also claimed that their scheme is resistant against impersonation and off-line dictionary attacks. However, Tan [16] performed a security analysis of RKL-scheme later in 2009 and pointed out that the RKL-scheme is insecure against impersonation and man-in-the-middle attacks.

So RKL-scheme is insecure because we find that there are much redundant information and they lack identification-related information in terms of their login request. In this paper, we will propose a novel secure password-based remote user authentication and key agreement scheme using common storage devices such as USB drives. The proposed scheme is based on the difficulty of cracking the computational Diffie-Hellman Problem (CDHP for short) [2, 13]. According to our security analysis, the proposed scheme cannot only withstand off-line dictionary and well-known on-line attacks, but also provides mutual authentication. Compared with the RKL-scheme, the proposed scheme's computation cost is lower and the total message length is also shorter. Therefore, our scheme is efficient and more suitable for applications in power-limited computing environments.

The structure of this paper is organized as follows. Section 2 describes the preliminaries. In Section 3, we propose our secure password-based remote user authentication and key agreement scheme without using smart cards, and present the security analysis of the proposed scheme in Section 4. Our conclusions are given in Section 5.

2. Preliminaries

2.1. Notations

The notations used throughout this paper are as follows.

- ID_i user U_i's identity
- PW_i user U_i's password
- x server S's secret key
- p, q two large prime numbers that satisfy p=2q+1
- H secure one-way hash function
- T timestamp
- ΔT maximum transmission delay
- Z_q ring of integers modulo q
- Z_q* multiplicative group of Z_q
- $\|$ concatenation operation

2.2. Computational Diffie-Hellman Problem (CDHP) [2, 13]

Consider a multiplicative group G and an element $g \in G$ having order p. The CDH problem states that, given g^a mod p and g^b mod p for randomly-chosen a, b, it is computationally intractable to compute the value g^{ab} mod p. Note that this problem is closely related to the difficulty of computing the discrete logarithm problem (DLP for short) over a cyclic group.

2.3. Security of Common Storage Devices

USB drives are ease to use memory devices. There are commercially available products coming with fingerprint locks or protected by AES-256 encryption. We incorporate these kinds of products in our scheme to strengthen the tamper-resistant property. Checking fingerprints provides a better security on unauthorized access. Encrypting files also provides considerable protection against tamper attacks or stolen items.

2.4. Goals

(I) The proposed scheme should provide a mechanism to prevent data tampering even though the scheme comes without using tamper-resistant devices.

(II) The proposed scheme should protect stored data against off-line dictionary attack.

(III) The proposed scheme should withstand well-known on-line attacks, such as replay attack, forgery attack, and user/server impersonation attack.

3. Proposed Scheme

We propose our novel secure password-based remote user authentication and key agreement scheme without using smart cards in this section, as shown in Figure1. The proposed scheme consists of three phases: registration, login, and authentication, and one activity: password change.

3.1. Registration Phase

In this phase, server S selects large prime numbers p and q that satisfy $p = 2q + 1$, its secret key $x \in Z_q^*$, and a one-way hash function H. User U_i applies his identity ID_i and password PW_i to S, obtains the authentication information from S and stores the information on his local memory device.

Step R1. U_i chooses his identity ID_i and password PW_i and sends them to S via a secure channel.

Step R2. Upon receiving the registration information, S computes $Y_i = H(ID_i)^{x + PWi}$ mod p.

Step R3. S sends the authentication information $\{Y_i, H, p, q\}$ back to U_i via the secure channel.

Step R4. Upon receiving the authentication information, U_i stores it locally on his memory device, i.e., his USB drive.

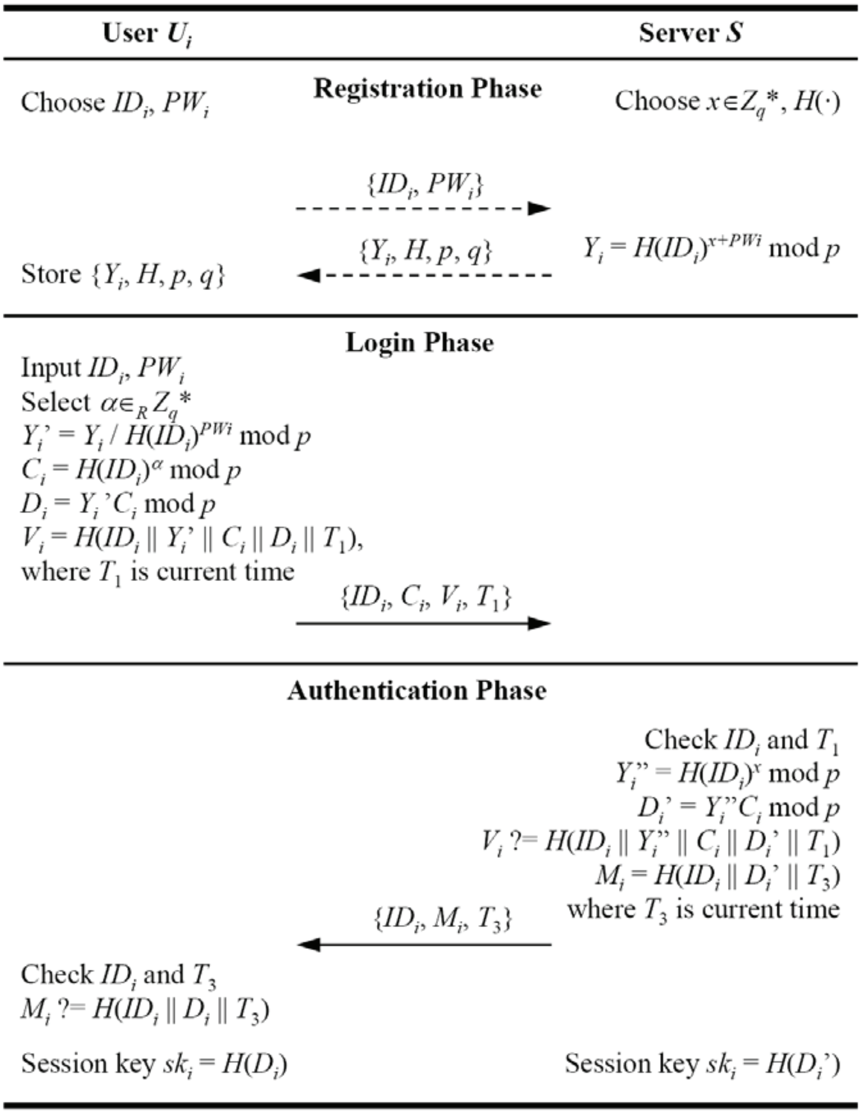
User U_i
Server S
Registration Phase
Choose ID_i, PW_i
Choose $x \in Z_q^*$, $H(\cdot)$
$\{ID_i, PW_i\}$
$\{Y_i, H, p, q\}$
$Y_i = H(ID_i)^{x+PWi} \bmod p$
Store $\{Y_i, H, p, q\}$
Login Phase
Input ID_i, PW_i
Select $\alpha \in_R Z_q^*$
$Y_i' = Y_i / H(ID_i)^{PWi} \bmod p$
$C_i = H(ID_i)^{\alpha} \bmod p$
$D_i = Y_i' C_i \bmod p$
$V_i = H(ID_i \| Y_i' \| C_i \| D_i \| T_1)$,
where T_1 is current time
$\{ID_i, C_i, V_i, T_1\}$
Authentication Phase
Check ID_i and T_1
$Y_i'' = H(ID_i)^x \bmod p$
$D_i' = Y_i'' C_i \bmod p$
$V_i ?= H(ID_i \| Y_i'' \| C_i \| D_i' \| T_1)$
$M_i = H(ID_i \| D_i' \| T_3)$
where T_3 is current time
$\{ID_i, M_i, T_3\}$
Check ID_i and T_3
$M_i ?= H(ID_i \| D_i \| T_3)$
Session key $sk_i = H(D_i)$
Session key $sk_i = H(D_i')$

Figure 1. The proposed scheme

3.2. Login Phase

This phase is invoked whenever user U_i wants to access system resources provided by server S. To log into the system, U_i retrieves the authentication information stored on his USB stick, calculates the proper information, and submits his login request to S. In our scheme, the authentication information issued from the server is stored on a device without tamper-resistance. It is possible that the information may be altered by careless or malicious means. In such case, to ensure the correctness of the authentication information, we setup a timeout threshold; any user must go back to the registration phase and re-obtain his authentication information if he does not receive the server's reply after the threshold time.

Step L1. U_i chooses a random numbers $\alpha \in Z_q^*$ and computes $Y_i' = Y_i / H(ID_i)^{PWi} \bmod p$, $C_i = H(ID_i)^{\alpha} \bmod p$, $D_i = Y_i' C_i \bmod p$, and $V_i = H(ID_i \| Y_i' \| C_i \| D_i \| T_1)$, where T_1 is the current time of U_i.

Step L2. U_i sends his login request $\{ID_i, C_i, V_i, T_1\}$ to S.

Step L3. If U_i does not receive S's reply before timeout, U_i must go back to the registration phase and re-obtain his authentication information.

3.3. Authentication Phase

Upon receiving the login request from user U_i, server S checks the request and replies the mutual authentication message if U_i is legitimate. After mutual authentication completed, U_i and S establish a secure channel by their shared session key *sk*.

Step A1. S checks that ID_i is valid and $(T_2 - T_1) < \Delta T$, where T_2 is the time which ID_i arrives to the server S. If either does not hold, S drops the request and terminates the session.

Step A2. S computes $Y_i'' = H(ID_i)^x \bmod p$ and $D_i' = Y_i'' C_i \bmod p$ and then verifies V_i with $H(ID_i \| Y_i'' \| C_i \| D_i' \| T_1)$. If they are not equal, S rejects the login request and stops the session; otherwise, S authenticates U_i and the login request is accepted.

Step A3. S computes $M_i = H(ID_i \| D_i' \| T_3)$, where T_3 is the current time of S, and replies with response $\{M_i, T_3\}$ back to U_i.

Step A4. Upon receiving the message, U_i checks if T_3 is valid and M_i is equal to $H(ID_i \| D_i \| T_3)$. If they hold, S is authenticated and mutual authentication between U_i and S is achieved; otherwise, S is not authenticated. U_i ends the session and goes back to the login phase.

Step A5. After the mutual authentication finished, U_i and S compute the symmetric session key $sk = H(D_i)_{\text{user-side}} = H(D_i')_{\text{server-side}}$ and use the key to launch a secure communication channel.

3.4. Password Change Activity

In the case where user U_i wants to change his identity ID_i and password PW_i, he can choose his new identity ID_i* and password PW_i*, go back to the registration phase, and re-obtain his new authentication information from server S.

4. Security and Performance Analysis

In this section, we present the security analysis of the proposed scheme.

4.1. Security of Server *S*'s Secret Key {*x*}

In the proposed scheme, only the service providing server S knows the secret key x. An adversary A may monitor the network traffic and collect U_i's login request $\{ID_i, C_i, V_i, T_1\}$ and S's response $\{M_i, T_3\}$. However, A cannot recover x from C_i since $C_i = H(ID_i)^{\alpha} \bmod p$ does not contain any knowledge of x. Besides, V_i and M_i are two digests. Since H is a secure one-way hash function, there is no way for A to regain x based on these two messages. Therefore, it is impossible for A to get the server's secret key x based on eavesdropped communication flows. Assume A steals U_i's authentication information $\{Y_i, H, p, q\}$, and tries to retrieve x from $Y_i = H(ID_i)^{x + PWi} \bmod p$. Since there is no any redundancy inside the authentication information that can be used as a checking verifier, it is impossible for A to guess x successfully. For a malicious user U_a, he can extract Y_a from his own authentication information $\{Y_a, H, p, q\}$ and try to retrieve Y_a'. To calculate x from $Y_a' = H(ID_a)^x \bmod p$, he needs to break the difficult problem of DLP [2]. Currently, it is believed that there is no polynomial time algorithm that can solve DLP.

4.2. Security of User *U*$_i$'s Password {*PW*$_i$ }

In the proposed scheme, there is no password table or verifier derived from PW_i stored on the server side after the registration phase. There is no way for an adversary A to retrieve U_i's password PW_i based on the eavesdropped communication flows, such as U_i's login request message $\{ID_i, C_i, V_i, T_1\}$ and S's response $\{M_i, T_3\}$, since these communication flows do not contain any information of U_i's password PW_i. Assume A steals U_i's authentication information $\{Y_i, H, p, q\}$, and tries to retrieve PW_i from $Y_i = H(ID_i)^{x + PWi} \bmod p$. Since there is no redundancy inside the authentication information that can be used as a verifier, it is impossible for A to guess PW_i successfully.

4.3. Security of Authentication Information {*Y*$_i$, *H*, *p*, *q*}

The only secret in the authentication information is Y_i. Assume that U_i's authentication information is stolen by an adversary A. By the above discussions in Sections 4.1 and 4.2, we know that A can guess neither the server S's secret key x nor the user U_i's password PW_i. Therefore, without correct x or PW_i, it is impossible that A can successfully calculate U_i's secret information $Y_i' = H(ID_i)^x \bmod p$. A may also monitor network traffic and collect U_i's login request $\{ID_i, C_i, V_i, T_1\}$ and S's response $\{M_i, T_3\}$, and try to recover Y_i'. However, H is a secure one-way hash function; there is no way for A to retrieve x or PW_i based on V_i and M_i. Moreover, A cannot recover Y_i' from $C_i = H(ID_i)^{\alpha} \bmod p$ either since C_i does not contain any useful knowledge of x or PW_i.

4.4. Off-line Dictionary Attacks

Assume that U_i's authentication information $\{Y_i, H, p, q\}$ is stolen by an adversary A, and A has also eavesdropped U_i's communication flows $\{ID_i, C_i, V_i, T_1\}$ and $\{M_i, T_3\}$. By the discussion in Section 4.1 of the security of S's secret $\{x\}$, we prove that it is very difficult that A can successfully recover the server's secret key x from the user's authentication information or eavesdropped communication flows. According to the security of U_i's password $\{PW_i\}$ discussed in Section 4.2, it is no way that A can retrieve the user's password PW_i from user's authentication information or eavesdropped communication flows. Also, from the discussion in Section 4.3, we see that it is impossible that A can successfully retrieve U_i's secret information Y_i' from Y_i. Therefore, our scheme is secure against off-line dictionary attacks.

4.5. On-line Attacks

We analyze the security of our scheme when it is attacking by: replay, forgery, and user/server impersonation attacks.

4.5.1. Replay Attacks

Assume that an adversary A pretends to be user U_i or server S by replaying the eavesdropped communication flows, such as U_i's login request message $\{ID_i, C_i, V_i, T_1\}$ or S's response $\{M_i, T_3\}$. For U_i's login request $\{ID_i, C_i, V_i, T_1\}$, S can easily detect a replay attack by checking the timestamp T_1. For S's response $\{M_i, T_3\}$, U_i can easily detect a replay attack by checking the timestamp T_3. Therefore, the attacker cannot circumvent the timestamp checking and complete the authentication phase. Note that, the man-in-the middle attack is a particular case of replay attack. It can also be detected by checking the timestamp.

4.5.2. Forgery Attacks

An adversary A may try to modify T_1 in Step L2 or T_3 in Step A4 to achieve a forgery attack. This will not work unless he also modifies $V_i = H(ID_i \| Y_i' \| C_i \| D_i \| T_1)$ in Step L1 or $M_i = H(ID_i \| D_i' \| T_3)$ in Step A3 with their corresponding values. However, it is difficult to compute the two digests V_i and M_i correctly without user U_i's password PW_i or server S's secret key x. Unless A can compute the two digests V_i or M_i, both S and U_i can easily calculate the corresponding hash value and compare with the received V_i or M_i, respectively.

4.5.3. User Impersonation Attacks

If an adversary A wants to forge the login request $\{ID_i, C_i, V_i, T_1\}$ and impersonate user U_i to fool server S, A needs to compute $Y_i' = H(ID_i)^x \bmod p$. However, from the previous discussion in Section 4.3, A cannot calculate the correct values of D_i and V_i without Y_i'. Therefore, the proposed scheme is secure against user impersonation attacks.

4.5.4. Server Impersonation Attacks

Assume that there is an adversary A that intends to masquerade as server S and deceive user U_i. A needs to generate a valid response $\{M_i, T_3\}$, where $M_i = H(ID_i \| D_i' \| T_3)$. However, from the discussion in Section 4.1, we proved that A cannot recover the server's secret key x from the eavesdropped communication flows and authentication information. Therefore, A cannot correctly compute D_i' and generate the forged mutual authentication message without x. Hence, the proposed scheme is secure against server impersonation attacks.

4.6. Mutual Authentication

The proposed scheme provides a mechanism that allows the user and server to verify each other. From the discussion in Section 4.2, we can recognize that only the legitimate user with the correct password can pass through the server's verification. In addition, from the discussion in Section 4.1, we also can distinguish that only the correct server with correct secret key can be qualified by the user. Therefore, the scheme achieves mutual authentication between a valid user and the server.

4.7. Secure Channel

After mutual authentication completed, both U_i and S can calculate their symmetric session key sk and establish a secure channel for subsequent communications. Note that if current session key is compromised by an attacker, the secrecy of previously established session keys is not affected. In the proposed scheme, the session key $sk = H(D_i) = H(D_i')$, where $D_i = H(ID_i)^{x+\alpha} \bmod p = D_i$'. Even if the system session key x is compromised, the attacker cannot calculate any previous sk without the random value α chosen every login session by U_i.

4.8. Efficiency

We evaluated the performance of the proposed scheme with related schemes. Tables 1 and 2 show the computation overhead and communication cost of RKL-scheme [12] and the proposed scheme.

Table 1. Computation overhead

Phase / Scheme	RKL-scheme	Ours
Registration		
User side	–	–
Server side	$2t_e + t_m + t_h$	$t_e + t_h$
Authentication		
User side	$3t_e + 2t_m + 3t_h$	$2t_e + 2t_m + 3t_h$
Server side	$3t_e + t_m + 2t_h$	$t_e + t_m + 2t_h$

- t_e is the time complexity of exponentiation operation.
- t_m is the time complexity of multiplication/division operation.
- t_h is the time complexity of hashing operation.

From Table 1, we can calculate the total computation overhead of RKL-scheme and ours to be $8t_e + 4t_m + 6t_h$ and $4t_e + 3t_m + 6t_h$, respectively. It can be seen that the proposed scheme can save four exponentiation and one multiplication operations compared to RKL-scheme.

From Table 2, the communication costs of RKL-scheme and the proposed scheme are 8 terms and 6 terms. We can reasonably assume that the lengths of the identity and the timestamp are 64 bits, the length of the prime number p is 128 bits, and the one-way hash function is SHA-1 with 160 bits throughout. The communication cost at the user side between RKL-scheme and the proposed scheme is 640(=64+128+128+128+128+64) bits and 416(=64+128+160+64) bits, respectively. It is demonstrated that the proposed scheme's communication cost is shorter than RKL-scheme's.

Table 2. Message length

Scheme	Contain	Terms
RKL-scheme		
Login request	$\{ID_i, Y_{i,2}, C_1, C_2, C_3, T\}$	6
Mutual acknowledgement	$\{C_4, T"\}$	2
Ours		
Login request	$\{ID_i, C_i, V_i, T_1\}$	4
Mutual acknowledgement	$\{M_i, T_2\}$	2

According to our analysis on both computation overhead and communication cost, our scheme is efficient and more suitable for applications in power-limited computing environments.

4.9. Functionality

The functionality of the proposed scheme is compared with RKL-scheme when users use insecure devices instead of smart cards to store authentication information. We summarize the comparisons in Table 3.

Table 3. Functionality comparison

Functionality / Scheme	RKL-scheme	Ours
Resists stolen-authentication-information attacks	No	Yes
Resists insider attacks	No	Yes
Resists off-line dictionary attacks	No	Yes
Resists replay attacks	No	Yes
Resists man-in-the-middle attacks	No	Yes
Resists forgery attacks	No	Yes
Resists user impersonation attacks	No	Yes
Resists server impersonation attacks	No	Yes
Achieves mutual authentication	No	Yes
Establishes secure channel	No	Yes

- Tan [16] has shown that RKL-scheme is insecure against impersonation and man-in-the-middle attacks.

5. Conclusions

In this paper, we have proposed a novel secure password-based remote user authentication scheme which solves the user impersonation attack problem by adding a blind factor into the authentication information stored on a user's local memory device. The proposed scheme is based on the difficulty of cracking CDHP. We demonstrated that the proposed scheme cannot only withstand off-line dictionary and well-known on-line attacks, but also provides mutual authentication. It shows that the proposed scheme achieves our goals. In other words, the proposed scheme retains all the advantages of RKL-scheme while being robust against user/server impersonation attacks, and also provides more security properties at the same time. Compared with RKL-scheme, the proposed scheme's computation cost is lower and the message length is shorter. Therefore, our scheme is efficient and more suitable for applications in power-limited computing environments.

Acknowledgment

This research was supported by NSC 100-2221-E-150-068.

References

[1] **H. Y. Chien, J. K. Jan, Y. M. Tseng.** "An efficient and practical solution to remote authentication: smart card," Computers and Security 21(4) (2002) 372–375.

[2] **W. Diffie, M. E. Hellman.** New Directions in Cryptography, IEEE Transactions on Information Theory IT-22 (6) (1976) 644–654.

[3] **T. ElGamal.** A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31 (4) (1985) 469–472.

[4] **C. I. Fan, Y. C. Chan, Z. K. Zhang.** Robust remote authentication scheme with smart cards, Computers & Security 24 (8) (2005) 619–628.

[5] **M. S. Hwang, L. H. Li.** A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (1) (2000) 28–30.

[6] **W. S. Juang.** Efficient password authenticated key agreement using smart cards, Computers & Security 23 (2) (2004) 167–173.

[7] **M. K. Khan, J. S. Zhang.** Improving the security of a flexible biometrics remote user authentication scheme, Computer Standards & Interfaces 29 (1) (2007) 82–85.

[8] **P. Kocher, J. Jaffe, B. Jun.** Differential power analysis. In: *Advances in Cryptology*, CRYPTO'99 (1999) 388–397.

[9] **L. Lamport.** Password authentication with insecure communication, Communications of the ACM 24 (1981) 770–772.

[10] **C. T. Li, C. C. Lee.** A robust remote user authentication scheme using smart card, Information Technology and Control 40 (2011) 236–245.

[11] **J. Y. Liu, A. M. Zhou, M. X. Gao.** A new mutual authentication scheme based on nonce and smart cards, Computer Communications 31 (10) (2008) 2205–2209.

[12] **H. S. Rhee, J. O. Kwon, D. H. Lee.** A remote user authentication scheme without using smart cards, Computer Standards & Interfaces 31 (1) (2009) 6–13.

[13] **D. R. Stinson.** Cryptography: Theory and Practice, Third Edition, CRC/C&H, 2005.

[14] **H. M. Sun.** An efficient remote use authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (4) (2000) 958–961.

[15] **D. Z. Sun, J. P. Huai, J. Z. Sun, J. X. Li.** Cryptanalysis of a mutual authentication scheme based on nonce and smart cards, Computer Communications 32 (6) (2009) 1015–1017.

[16] **Z. Tan.** Security analysis of two password authentication schemes, Mobile Business, International Conference on, 296–300, 2009 Eighth International Conference on Mobile Business, 2009.

[17] **X. M. Wang, W. F. Zhang, J. S. Zhang, M. K. Khan.** Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards, Computer Standards & Interfaces 29 (5) (2007) 507–512.

[18] **C. C. Yang, R. C. Wang**. Cryptanalysis of a user friendly remote authentication scheme with smart cards, Computers and Security 23 (5) (2004) 425–427.

Received December 2011.