Secure Password-based Remote User Authentication Scheme against Smart Card Security Breach

Ding Wang*†, Chun-Guang Ma*, Qi-Ming Zhang*, Sendong Zhao
* College of Computer Science and Technology, Harbin Engineering University
145 Nantong Street, Harbin City 150001, China
Email: wangdingg@mail.nankai.edu.cn
† Automobile Management Institute of PLA, Bengbu City 233011, China

***Abstract*—It is a challenge for password authentication protocols using non-tamper resistant smart cards to achieve user anonymity, forward secrecy, immunity to various attacks and high performance at the same time. In 2011, Li and Lee showed that both Hsiang-Shih's password-based remote user authentication schemes are vulnerable to various attacks if the smart card is non-tamper resistant. Consequently, an improved scheme was developed to preclude the identified weaknesses and claimed that it is secure against smart card loss attacks. In this paper, however, we will show that Li-Lee's scheme still cannot withstand offline password guessing attack under the non-tamper resistance assumption of the smart card. In addition, their scheme is also vulnerable to denial of service attack and fails to provide user anonymity and forward secrecy. As our main contribution, a robust scheme is presented to cope with the aforementioned defects, while keeping the merits of different password authentication schemes using smart cards. The analysis demonstrates that our scheme meets all the proposed criteria and eliminates several hard security threats that are difficult to be tackled at the same time in previous scholarship.**

***Index Terms*—cryptanalysis, authentication protocol, network security, smart card, non-tamper resistant, user anonymity.**

I. INTRODUCTION

Password-based authentication is widely used for systems that control remote access to computer networks. In order to address some of the security and management problems that occur in traditional password authentication protocols, research in recent decades has focused on smart card based password authentication. Since Chang and Wu [1] introduced the first remote user authentication scheme using smart cards in 1993, there have been many smart card based authentication schemes proposed [2-7]. In most of the previous authentication schemes, the smart card is assumed to be tamper-resistant, i.e., the secret information stored in the smart card cannot be revealed. However, recent research results have shown that the secret data stored in the smart card could be extracted by some means, such as monitoring the power consumption [8,9] or analyzing the leaked information [10]. Therefore, such schemes based on the tamper resistance assumption of the smart card are vulnerable to some types of attacks, such as user impersonation attacks, server masquerading attacks, and offline password guessing attacks, etc., once an adversary has obtained the secret information stored in a user's smart card and/or just some intermediate computational results in the smart card.

Another common feature of the published schemes is that the user's identity is transmitted in plaintext over insecure networks during the authentication process, which may leak the identity of the logging user once the login messages were eavesdropped, and thus user privacy is not preserved. The leakage of the user identity may also cause an unauthorized entity to track the user's login history and current location [5,7], as well as user's life styles and preferences. In many cases, it is of utmost importance to provide anonymity so that the adversary cannot trace user activity. Therefore, user anonymity is an important feature that a practical authentication scheme should achieve.

As noted by Blake-Wilson et al. [11], forward secrecy is an admired security feature for authentication protocols with session keys establishment. Particularly, forward secrecy is a property concerned with limiting the effects of eventual failure of the entire system. It indicates that, even if the long-term private keys of one or more entities are compromised, the secrecy of previous session keys established by honest entities should not be affected and thus the previous sessions shall remain secure [12,22]. Hence, a sound authentication scheme should achieve this important property.

As mentioned in Refs. [3,7,13-15] and the above description, the following criteria are important for smart card based remote user authentication schemes in terms of friendliness, security and efficiency: (C1) the server needs not to maintain a security-sensitive verification table; (C2) the password is memorable, and can be chosen freely by the user; (C3) the password cannot be derived by the privileged administrator of the server; (C4) the scheme is free from smart card loss attack, i.e., unauthorized users should not be able to easily change the password of the

Manuscript received June 1, 2012; revised July 1, 2012; accepted July 15, 2012. This is a substantially expanded and full version of a paper [29] that has been presented in DBSec 2012.
Wang Ding is the corresponding author

doi: 10.4304/jnw.8.1.148-155

smart card, or guess the password of the user by using password guessing attacks, or impersonate the user to login to the system, even if the smart card is obtained and/or secret data in the smart card is revealed; (C5) the scheme can resist various kinds of sophisticated (conventional) attacks, such as offline password guessing attack, replay attack, parallel session attack, denial of service attack, stolen verifier attack, user/server impersonation attack; (C6) the client and the server can establish a common session key during the authentication process; (C7) the scheme provides the property of timely wrong password detection, i.e. the user will be timely notified if he inputs wrong password by mistake in login phase; (C8) the scheme is not prone to the problems of clock synchronization and time-delay; (C9) the user can change the password locally without any interaction with the authentication server; (C10) the scheme can achieve mutual authentication; (C11) the scheme preserves user anonymity to avoid partial information leakage; (C12) the scheme provides the property of forward secrecy.

In 2004, Yoon et al. [16] proposed an advanced remote user authentication scheme using smart cards, their scheme possesses the merits of providing mutual authentication, no verification table, freely choosing password, involving only a few hashing operations, and so forth. Later on, Hsiang and Shih [17] showed that, in addition to parallel session attack, Yoon et al.'s scheme is vulnerable to offline password guessing attack, user impersonation attack if the smart card is non-tamper resistant. Consequently, an improvement over enhance Yoon et al.'s scheme is presented. In 2011, Li and Lee [18] identified that Hsiang-Shih's scheme still cannot withstand various attacks if the secret data stored in smart is revealed and further proposed an enhanced remote authentication scheme. They claimed their scheme is secure and can overcome all the identified security flaws of Hsiang-Shih's scheme even if the smart card is non-tamper resistant.

In this work, however, we will demonstrate that Li-Lee's scheme cannot withstand denial of service attack and is still vulnerable to offline password guessing attack under their assumption. In addition, their scheme does not provide the feature of forward secrecy and user anonymity. To conquer the identified weaknesses, a robust authentication scheme based on the secure one-way hash function and the well-known discrete logarithm problem is presented.

The remainder of this paper is organized as follows: in Section 2, we briefly review Li-Lee's authentication scheme. Section 3 describes the weaknesses of Li-Lee's scheme. Our proposed scheme is presented in Section 4, and its security analysis is given in Section 5. The comparison of the performance of our scheme with the other related schemes is shown in Section 6. Section 7 concludes the paper.

II. REVIEW OF LI-LEE'S SCHEME

In this section, we briefly illustrate the remote user authentication scheme proposed by Li and Lee [18] in 2011. Their scheme consists of four phases: the registration phase, the login phase, the verification phase and password update phase. For ease of presentation, we employ some intuitive abbreviations and notations listed in Table 1.

TABLE I.
NOTATIONS

Symbol	Description
U_i	i^{th} user
S	remote server
ID_i	identity of user U_i
P_i	password of user U_i
x	the secret key of remote server S
n	a large prime number
g	a primitive element in Galois field $GF(n)$
$h(\cdot)$	collision free one-way hash function
$\oplus$	the bitwise XOR operation
$\|\|$	the string concatenation operation
$A \Rightarrow B: M$	message M is transferred through a secure channel from A to B
$A \rightarrow B: M$	message M is transferred through a common channel from A to B

A. Registration Phase

The registration phase involves the following operations:

Step R1. User U_i chooses his/her identity ID_i and password P_i, and then generates a random number RN_1.

Step R2. $U_i \Rightarrow S$: $\{ID_i, h(h(P_i \oplus RN_1))\}$.

Step R3. On receiving the registration message from U_i, the server S creates an entry $\{ID_i, N, h(h(P_i \oplus RN_1))\}$ in the verification table, where $N = 0$ if it is U_i's initial registration, otherwise S sets $N = N + 1$. Then, the server S computes $C_1 = h(ID_i \| x \| N) \oplus h(h(P_i \oplus RN_1))$.

Step R4. $S \Rightarrow U_i$: A smart card containing security parameters $\{ID_i, C_1, h(\cdot)\}$.

Step R5. Upon receiving the smart card, user U_i stores RN_1 into the smart card.

B. Login phase

When U_i wants to login to S, the following operations will be performed:

Step L1. U_i inserts his/her smart card into the card reader and inputs ID_i, P_i and a random number RN_2.

Step L2. The smart card generates a random number RC and then computes $C_2 = h(P_i \oplus RN_1)$, $C_3 = C_1 \oplus h(C_2)$, $C_4 = C_3 \oplus C_2$, $C_5 = h(h(P_i \oplus RN_2))$ and $C_6 = E_{K_{U_i}}(C_5, RC)$, where $K_{U_i} = h(C_2 \| C_3)$.

Step L3. $U_i \rightarrow S$: $\{ID_i, C_4, C_6\}$.

C. Verification Phase

After receiving the login request message from user U_i, the server S performs:

Step V1. The server S checks the validity of identity ID_i by checking whether ID_i is already stored in its verification table. If not, the request is rejected. Otherwise, the S computes $C_7 = h(ID_i \| x \| N)$, $C_8 = C_4 \oplus C_7$, $C_9 = h(C_8)$, and compares C_9 with the

third field of the entry corresponding to ID_i in its verification table. If it equals, S successfully authenticates U_i and computes symmetric key $K'_{U_i} = h(C_8 \| C_7)$, and obtains (C_5, RC) by decrypting C_6 . Then, S replaces the third field $h(h(P_i \oplus RN_1)$ of the entry corresponding to ID_i with $C_5 = h(P_i \oplus RN_2)$, generates a random RS and computes $K_S = h(C_7 \| C_8)$.

Step V2. $S \to U_i : \{E_{K_S}(RC, RS, C_5)\}$.

Step V3. On receiving the response from server S, the smart card computes the symmetric key $K'_S = h(C_3 \| C_2)$ and obtains (RC', C'_5) by decrypting the received message using K'_S . Then, the smart card checks whether (RC', C'_5) equals to (RC, C_5) generated in the login phase. This equivalency authenticates the legitimacy of the server S and replaces original RN_1 and C_1 with new RN_2 and $C_3 \oplus C_5$, respectively.

Step V4. $U_i \to S : \{h(RS)\}$.

Step V5. On receiving $h(RS)'$, the serve S compares the computed $h(RS)$ with the received value of $h(RS)'$. If they are not equal, the connection is terminated.

Step V6. The user U_i and the server S agree on the session key $SK = h(RC \oplus RS)$ for securing future data communications.

D. Password Change Phase

The password change phase is provided to allow users to change their passwords freely. Since the password change phase has little to do with our discussion, we omit it here and detailed information is referred to Ref. [18].

III. Cryptanalysis of Li-Lee's Scheme

In this section we will show that Li-Lee's scheme is vulnerable to offline password guessing attack and denial of service attack. In addition, their scheme fails to preserve user anonymity and forward secrecy. Although tamper resistant smart card is widely assumed in most of the published authentication schemes, such an assumption is difficult in practice. Many researchers have shown that the secret information stored in a smartcard can be breached by analyzing the leaked information or by monitoring the power consumption [8-10]. Be aware of this threat, Li and Lee intentionally based their scheme on the assumption of non-tamper resistance of the smart card. However, Li-Lee's scheme fails to serve its purposes.

A. Offline Password Guessing Attack

In Li-Lee's scheme, a user is allowed to choose his/her own password at will during the registration and password change phases. The user usually tends to select a password, e.g., his phone number, which is easily remembered for his/her convenience. Hence, these easy-to-remember passwords, called weak passwords [19], have low entropy and thus are potentially vulnerable to password guessing attack. Therefore, one of the most important security requirements for sound password-based authentication protocols is to resist against this threat. Li and Lee showed that Kim and Chung's scheme is vulnerable to offline password guessing attack once the adversary has obtained the secret information stored in the stolen smart card. However, we will show that Li-Lee's scheme still suffers from this threat as follows.

Let us consider the following scenarios. In case a legitimate user U_i's smart card is stolen by an adversary A just before U_i's jth login, and the stored secret values such as C_1 and RN_j can be revealed. Then, A returns the smart card to U_i and eavesdrops on the insecure channel. Because U_i's identity is transmitted in plaintext within the login request, it is not difficult for A to identify the login request message from U_i. Once the jth login request message $\{ID_i, C_4^j = h(ID_i \| x \| N) \oplus h(P_i \oplus RN_j), C_6^j\}$ is intercepted by A, an offline password guessing attack can be launched in the following steps:

Step 1. Guesses the value of P_i to be P_i^* from a uniformly distributed dictionary.

Step 2. Computes $T = h(h(P_i^* \oplus RN_j)) \oplus h(P_i^* \oplus RN_j)$, as RN_j is known.

Step 3. Computes $T' = C_1 \oplus C_4^j$, as C_1 has been extracted and C_4^j has been intercepted, where $C_1 = h(ID_i \| x \| N) \oplus h(h(P_i \oplus RN_j))$, $C_4^j = h(ID_i \| x \| N) \oplus h(P_i \oplus RN_j)$.

Step 4. Verifies the correctness of P_i^* by checking if T is equal to T' .

Step 5. Repeats Steps1, 2, 3, and 4 of this phase until the correct value of P_i is found.

After guessing the correct value of P_i, the adversary can compute $C_3^j = C_1 \oplus h(h(P_i \oplus RN_j))$, $C_2^j = h(P_i \oplus RN_j)$ and $K_{U_i}^j = h(C_2^j \| C_3^j)$. Then the adversary can obtain RC_j by decrypting C_6^j using $K_{U_i}^j$, and gets RS_j in a similar way. Hence the malicious user can successfully compute the session key $SK_j = h(RC_j \oplus RS_j)$ and renders the jth session between U_i and S completely insecure.

Moreover, once the jth login request message is intercepted, the adversary may block the communication channel between U_i and S completely until the session key $SK_j = h(RC_j \oplus RS_j)$ was obtained as stated above. Thereafter, he/she can fabricate and send a valid login request to the server S and masquerade as a legitimate user U_i, or he/she can fabricate and send a valid password change request to update the entry corresponding to U_i in the verification table on S. In either case, from then on U_i will not be able to login to the server S. This leads to a strong denial of service attack.

B. Denial of Service Attack

A denial of service attack is an offensive action whereby the adversary could use some methods to work upon the server so that the login requests issued by the legitimate

user will be denied by the server. In Li et at.' scheme, an adversary can easily launch a denial of service attack in the following steps:

Step 1. Eavesdrops over the channel, intercepts a login request $\{ID_i, C_4^j, C_6^j\}$ from U_i and blocks it, supposing it is U_i's *j*th login.

Step 2. Replaces C_6^j with an equal-sized random number *R*, while ID_i and C_4^j are left unchanged.

Step 3. Sends $\{ID_i, C_4^j, R\}$ instead of $\{ID_i, C_4^j, C_6^j\}$ to the remote server *S*.

After receiving this modified message, *S* will perform Step V1 and V2 of the verification phase without observing any abnormality, as a result, the verifier corresponding to ID_i in the verification table will be updated and the response $E_{K_S}(RC_j^*, RS_j, C_5^{j*})$ will be sent to U_i. On receiving the response from *S*, U_i decrypts $E_{K_S}(RC_j^*, RS_j, C_5^{j*})$ and will find (RC_j^*, C_5^{j*}) unequal to (RC, C_5), thus the session will be terminated. Thereafter, U_i's succeeding login requests will be denied unless he/she re-registers to *S* again. That is, the adversary can easily lock the account of any legitimate user without using any cryptographic techniques. Thus, Li-Lee's protocol is vulnerable to denial of service attack.

C. Failure to Achieve Forward Secrecy

Let us consider the following scenarios. Supposing the server *S*'s long time private key *x* is leaked out by accident or intentionally stolen by an adversary *A*. Once the value of *x* is obtained, with previously intercepted C_4^j, C_6^j and $E_{K_S}(RC, RS, C_5)$ transmitted in the legitimate user U_i's *j*th authentication process, *A* can compute the session key of *S* and U_i's *j*th encrypted communication through the following method:

Step 1. Assumes $N = 0$.

Step 2. Computes $C_7^* = h(ID_i \| x \| N)$ and $C_8^* = C_7^* \oplus C_4^j$, where ID_i is previously obtained by eavesdropping on the insecure channel.

Step 3. Computes $K_{U_i}^* = h(C_8^* \| C_7^*)$ and $K_S^* = h(C_7^* \| C_8^*)$.

Step 4. Decrypts C_6^j to obtain RC_j^* using $K_{U_i}^*$.

Step 5. Decrypts $E_{K_S}(RC, RS, C_5)$ to obtain RC_j^{**} using K_S^*.

Step 6. Verifies the correctness of N by checking if RC_j^* is equal to RC_j^{**}. If they are unequal, sets $N = N + 1$ and goes back to Setp2.

Step 7. Decrypts $E_{K_S}(RC, RS, C_5)$ to obtain RS_j using K_S^*.

Step 8. Computes $SK_j = h(RC_j \oplus RS_j)$.

Note that the value of *N* should not be very big, since the re-registration phase is not performed frequently in practice, and thus the above procedure can be completed in polynomial time. Therefore, Li-Lee's scheme fails to provide forward secrecy.

D. Failure to Preserve User Anonymity

In many e-commerce applications, the violation of user anonymity may leak some personal secret information (e.g., secret online-order placement, transaction records, etc.) about the logging user to the adversary, and thus the provision of user anonymity is very important. What's more, the leakage of the user identity may cause an unauthorized entity to track the user's login history and current location [5]. Therefore, assuring anonymity does not only preserve user privacy but also make remote user authentication protocols more secure.

In Li-Lee's scheme, user's identity *ID* is static and in plaintext form in all the transaction sessions, an adversary can easily obtain the plaintext identity of this communicating client once the login messages were eavesdropped, and hence, different login request messages belonging to the same user can be traced out and may be interlinked to derive some secret information related to the user. Hence, user anonymity is not preserved.

IV. Our Proposed Scheme

According to our analysis, three principles for designing a sound password-based remote user authentication scheme are presented. First, user anonymity, especially in some application scenarios, (e.g., e-commence), should be preserved, because from the identity ID_i, some personal secret information may be leaked about the user. Second, a nonce based mechanism is often a better choice than the timestamp based design to resist replay attacks, since clock synchronization is difficult and expensive in existing network environment, especially in wide area networks, and these schemes employing timestamp may still suffer from replay attacks as the transmission delay is unpredictable in real networks [20]. Finally, the password change process should be performed locally without the hassle of interaction with the remote authentication server for the sake of security, user friendliness and efficiency [3]. In this section, we present a new remote user authentication scheme to satisfy all the twelve criteria listed in section 1.

A. Registration Phase

Let (x, $y = g^x \bmod n$) denote the server *S*'s private key and its corresponding public key, where *x* is kept secret by the server and *y* is stored inside each user's smart card. The registration phase involves the following operations:

Step R1. U_i chooses his/her identity ID_i, password P_i and a random number *b*.

Step R2. $U_i \Rightarrow S$: $\{ID_i, h(b \| P_i)\}$.

Step R3. On receiving the registration message from U_i, the server *S* computes $N_i = h(b \| P_i) \oplus h(x \| ID_i)$ and $A_i = h(ID_i \| h(b \| P_i))$.

Step R4. $S \Rightarrow U_i$: A smart card containing security parameters $\{N_i, A_i, n, g, y, h(\cdot)\}$.

Step R5. Upon receiving the smart card, U_i enters *b* into his smart card.

B. Login Phase

When U_i wants to login the system, the following operations will be performed:

Step L1. U_i inserts his/her smart card into the card reader and inputs ID_i^* and P_i^*.

Step L2. The smart card computes $A_i^* = h(ID_i \| h(b \| P_i^*))$ and verifies the validity of A_i^* by checking whether A_i^* equals to the stored A_i. If the verification holds, it implies $ID_i^* = ID_i$ and $P_i^* = P_i$. Otherwise, the session is terminated.

Step L3. The smart card chose a random number u and computes $C_1 = g^u \bmod n$, $Y_1 = y^u \bmod n$, $h(x \| ID_i) = N_i \oplus h(b \| P_i)$, $CID_i = ID_i \oplus h(C_1 \| Y_1)$ and $M_i = h(CID_i \| C_1 \| h(x \| ID_i))$.

Step L4. $U_i \rightarrow S$:$\{C_1, CID_i, M_i\}$.

C. Verification Phase

After receiving the login request, the server S performs the following operations:

Step V1. The server S computes $Y_2 = (C_1)^x \bmod n$ using its private key x, and derives $ID_i = CID_i \oplus h(C_1 \| Y_2)$ and $M_i^* = h(CID_i \| C_1 \| h(x \| ID_i))$. S compares M_i^* with the received value of M_i. If they are not equal, the request is rejected. Otherwise, server S generates a random number v and computes the session key $SK = (C_1)^v \bmod n$, $C_2 = g^v \bmod n$ and $C_3 = h(SK \| C_2 \| h(x \| ID_i))$.

Step V2. $S \rightarrow U_i$: $\{C_2, C_3\}$.

Step V3. On receiving the reply message from the server S, U_i computes $SK = (C_2)^u \bmod n$, $C_3^* = h(SK \| C_2 \| h(x \| ID_i))$, and compares C_3^* with the received C_3. This equivalency authenticates the legitimacy of the server S, and U_i goes on to compute $C_4 = h(C_3 \| h(x \| ID_i) \| SK)$.

Step V4. $U_i \rightarrow S$: $\{C_4\}$.

Step V5. Upon receiving $\{C_4\}$ from U_i, the server S first computes $C_4^* = h(C_3 \| h(x \| ID_i) \| SK)$ and then checks if C_4^* is equal to the received value of C_4 . If this verification holds, the server S authenticates the user U_i and the login request is accepted else the connection is terminated.

Step V6. The user U_i and the server S agree on the common session key SK for securing future data communications.

D. Password Change Phase

In this phase, we argue that the user's smart card must have the ability to detect the failure times. Once the number of login failure exceeds a predefined system value, the smart card must be locked immediately to prevent the exhaustive password guessing behavior. This phase involves the following steps.

Step P1. U_i inserts his/her smart card into the card reader and inputs the identity ID_i and the original password P_i.

Step P2. The smart card computes $A_i^* = h(ID_i \| h(b \| P_i))$ and verifies the validity of A_i^* by checking whether A_i^* equals to the stored A_i. If the verification holds, it implies the input ID_i and P_i are valid. Otherwise, the smart card rejects.

Step P3. The smart card asks the cardholder to resubmit a new password P_i^{new} and computes $N_i^{new} = N_i \oplus h(b \| P_i) \oplus h(b \| P_i^{new})$, $A_i^{new} = h(ID_i \| h(b \| P_i^{new}))$. Thereafter, smart card updates the values of N_i and A_i stored in its memory with N_i^{new} and A_i^{new}.

V. Security Analysis

Although it is important to user formal methods to provide a formal security proof on any cryptographic protocols, the formal security proof of remote user authentication protocols with smart cards remains a challenging problem in cryptography research domain [21]. As far as we know, an efficient, simple, and convincing formal methodology for security analysis of protocols is still an important subject of research and an open issue. Few schemes [e.g., 6, 13] do provide formal security proof, unfortunately they are shortly found contradictory to their security claims because the formal methods employed all fail to capture some realistic attack scenarios [14]. Due to these reasons, most published user authentication schemes using smart cards [e.g., 1–5, 7, 15-18, 22-24] have been demonstrated with a simple proof. Therefore, we follow the approaches used in [5, 7] for comparison purpose. This opens a prominent future scope of this work to develop a simple and robust formal method for security analysis of user authentication protocols with smart cards.

The security of our proposed authentication scheme is based on the secure hash function and the discrete logarithm problem. In the following, we will analyze the security of the proposed scheme to verify whether the security requirements mentioned in Section 1 have been satisfied under the assumption that the secret information stored in the smart card can be revealed, i.e., the security parameters N_i, A_i ,b, and y can be obtained by a malicious privileged user.

1) User anonymity: Suppose that the attacker has intercepted U_i's authentication messages $\{CID_i, M_i, C_1, C_2, C_3, C_4\}$. Then, the adversary may try to retrieve any static parameter from these messages, but these messages are all session-variant and indeed random strings due to the randomness of u and/or v. Accordingly, without knowing the random number u, the adversary will face to solve the discrete logarithm problem to retrieve the correct value of ID_i from CID_i, while ID_i is the only static element corresponding to U_i in the transmitted messages. Hence, the proposed scheme can preserve user anonymity.

2) Offline password guessing attack: Suppose that a malicious privileged user U_i has got U_k's smart card, and the secret information b, N_k, A_k and y can also be revealed under our assumption of the non-tamper resistant smart card. Even after gathering this information, the attacker has to at least guess both ID_i and P_i correctly at the same time, because it has been demonstrated that our scheme can provide identity protection. It is impossible to guess these two parameters correctly at the same time in polynomial time, and thus the proposed scheme can resist offline password guessing attack with smart card security breach.

3) Stolen verifier attack and password disclosure to server: In the proposed protocol, no sensitive verifiers corresponding to users are maintained by S. Therefore, the proposed protocol is free from stolen verifier attack. With

$h(b \| P_i)$ instead of plaintext password P_i submitted to server S, it is computationally infeasible to derive P_i from $h(b \| P_i)$ without knowing the random number b due to the one-way property of the secure hash function.

4) User impersonation attack: As CID_i, M_i, C_3 and C_4 are all protected by secure one-way hash function, any modification to these parameters of the legitimate user U_i's authentication messages will be detected by the server S if the attacker cannot fabricate the valid CID_i^*, M_i^*, $C_3^*$and C_4^*. Because the attacker has no way of obtaining the values of ID_i, P_i and N_i corresponding to user U_i, he/she cannot fabricate the valid CID_i^*, M_i^*, $C_3^*$and C_4^*. Therefore, the proposed protocol is secure against user impersonation attack.

5) Server masquerading attack: In the proposed protocol, a malicious server *MS* cannot compute the correct $Y_2 = (C_1)^x \bmod n$ because he/she does not know the value of S's private key x, and thus *MS* cannot derive the valid $ID_i = CID_i \oplus h(C_1 \| Y_2)$. Without knowing U_i's valid ID_i and S's private key x, *MS* has to break the secure one-way hash function to retrieve $h(x \| ID_i)$. Furthermore, because *MS* cannot obtain $h(x \| ID_i)$, it is impossible to fabricate the proper $C_3 = h(SK \| C_2 \| h(x \| ID_i))$ to pass the verification of U_i in Step V3 of the verification phase. Therefore, the proposed protocol is free from server masquerading attack.

6) Replay attack and parallel session attack: Our scheme can withstand replay attack because the authenticity of authentication messages $\{M_i, C_3, C_4\}$ is verified by checking the fresh random number u and/or v. On the other hand, the presented scheme resists parallel session attack, in which an adversary may masquerade as legitimate user U_i by replaying a previously intercepted authentication message. The attacker cannot compute valid C_3 because he does not know the values of $h(x \| ID_i)$ corresponding to user U_i. Therefore, the resistance to replay attack and parallel session attack can be guaranteed in our protocol.

7) Mutual authentication: In our dynamic ID-based scheme, the server authenticates the user by checking the validity of C_4 in the access request. We have shown that our scheme can preserve user anonymity, so user ID_i is only known to the server S and the user U_i itself. We have proved that our scheme can resist user impersonation attack. Therefore, it is impossible for an adversary to forge messages to masquerade as U_i in our scheme. To pass the authentication of server S, the smart card first needs U_i's identity ID_i and password P_i to get through the verification in Step L2 of the login phase. In this Section, we have shown that our scheme can resist offline password guessing attack. Therefore, only the legal user U_i who owns correct ID_i and P_i can pass the authentication of server S. On the other hand, the user U_i authenticates server S by explicitly checking whether the other party communicating with can compute the valid C_3 or not. Since the malicious server does not know the values of ID_i corresponding to user U_i and x corresponding to server S, only the legitimate server can compute the correct $C_3 = h(SK \| C_2 \| h(x \| ID_i))$. From the above analysis, we conclude that our scheme can achieve mutual authentication.

8) Denial of service attack: Assume that an adversary has got a legitimate user U_i's smart card. However, in our scheme, the smart card computes $A_i^* = h(ID_i \| h(b \| P_i))$ and compares it with the stored value of A_i in its memory to checks the validity of user identity ID_i and password P_i before the password update procedure. It is not possible for the adversary to guess out U_i's identity ID_i and password P_i correctly at the same time in polynomial time. Moreover, once the number of login failure exceeds a predefined system value, the smart card will be locked immediately. Therefore, our protocol is secure against denial of service attack.

9) Forward secrecy: Following our scheme, the client and the server can establish the same session key $S \equiv (C_1)^v \equiv (C_2)^u \equiv g^{uv} \bmod n$. Based on the difficulty of the computational Diffie-Hellman problem, any previously generated session keys cannot be revealed without knowledge of the ephemeral u and v. As a result, our scheme provides the property of forward secrecy.

VI. PERFORMANCE ANALYSIS

To evaluate our scheme, we compare the performance and the satisfaction of the criteria among relevant authentication schemes and our proposed scheme in this section. The reason why the schemes presented in [4,5, 24], instead of other works mentioned earlier in this paper, are selected to compare with is that, these three schemes are the few ones that can withstand offline password guessing attack under the non-tamper resistance assumption of the smart cards. The criteria of a secure and practical remote user authentication scheme are introduced in Section 1, and the comparison results are depicted in Table 2 and 3, respectively.

Since the login phase and verification phase are executed much more frequently than the other two phases, only the computation cost, communication overhead and storage cost during the login phase and verification phase are taken into consideration. Without loss of generality, the identity ID_i, password P_i, random numbers, timestamp values and output of secure one-way hash function are all recommended to be 128-bit long, while n, y and g are all 1024-bit long. Let T_H, T_E, T_I, T_S and T_X denote the time complexity for hash function, exponential operation, inverse operation, symmetric cryptographic operation and XOR operation respectively. Since the time complexity of XOR operation is negligible as compared to the other three operations, we do not take T_X into account. Typically, time complexity associated with these operations can be roughly expressed as $T_E \approx T_I > T_S \geq T_H >> T_X$ [25-27].

In our scheme, the parameters $\{N_i, A_i, y_i, n, g\}$ are stored in the smart card, thus the storage cost is 3456 ($= 3 * 128 + 3 * 1024$) bits. The communication overhead includes the capacity of transmitting message involved in the authenti cation scheme, which is 2560 ($= 4 * 128 + 2 * 1024$) bits. During the login and verification phase, the

total computation cost of the user and server is $6T_E$+$12T_H$. As illustrated in Table 2, the proposed scheme is more efficient than Horng et al.'s scheme, enjoys nearly the same performance with Chen et al.'s scheme and Chung et al.'s scheme.

TABLE II.
PERFORMANCE COMPARISON AMONG RELEVANT AUTHENTICATION SCHEMES

	Our scheme	**Li and Lee[18] (2011)**	**Chung et al.[22] (2009)**	**Chen et al.[4] (2010)**	**Horng et al.[5] (2010)**
Total computation cost	$6T_E$+$12T_H$	$12T_H$	$4T_E$+$2T_I$ +$12T_H$	$6T_E$+$5T_H$	$7T_E$+$4T_S$+$8T_H$
Communication cost	2560 bits	856 bits	2560 bits	2560 bits	2432 bits
Storage overhead	3456 bits	384 bits	3200 bits	3200 bits	3328 bits

TABLE III.
CRITERIA COMPARISON AMONG RELEVANT AUTHENTICATION SCHEMES

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**C11**	**C12**
Our scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Li and Lee[18]	No	Yes	Yes	No	No	Yes	No	Yes	No	Yes	No	No
Chung et al.[22]	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes
Chen et al.[4]	Yes	Yes	No	No	No	Yes	No	No	No	Yes	No	Yes
Horng et al.[5]	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes

As compared to Li-Lee's scheme, to withstand offline password guessing attack, public-key techniques are employed, which has been proved necessary by Halevi and Krawczyk in [28], and thus at least two exponentiations are required; to provide the feature of forward secrecy, the generation of the session key based on the Diffie-Hellman key exchange algorithm is common practice, and hence it needs another four exponentiations; to achieve user anonymity and other functionalities simultaneously, some additional costs are necessary. As a word, to conquer all the identified security flaws, the decrease of some performance is unavoidable and reasonable.

Table 3 gives a comparison of the admired features of our proposed scheme with the other relevant authentication schemes. Our proposed scheme provides forward secrecy (C12) and can change password locally (C6), while the schemes presented by Li and Lee fails to achieve these features; Our proposed scheme preserves user anonymity (C11), while the schemes presented by Li and Lee, Chung et al. and Chen et al. do not provide this property; our proposed scheme can resist various kinds of sophisticated attacks (C5), while Li-Lee's scheme is vulnerable to denial of service attack and Chen et al.'s scheme cannot withstand reflection attack. Our scheme and Chung et al.'s scheme is secure against smart card loss attack (C4) while all the other three schemes are prone to offline password guessing attack once the secret data stored in smart card is revealed, thereby these three schemes fail to achieve this security requirement. It is clear that our scheme meets more criteria as compared to other relevant authentication schemes using non-tamper resistant smart cards.

VII. CONCLUSION

In this paper, we have demonstrated several attacks on Li-Lee's scheme. As to our main contribution, a robust authentication scheme is proposed to remedy these identified flaws, the security and performance analysis demonstrate that our presented scheme achieves all of the twelve independent requirements with high efficiency and thus our scheme is more secure and efficient for practical use. Remarkably, our scheme eliminates several hard security threats that are difficult to be solved at the same time in previous scholarship.

ACKNOWLEDGMENT

This research was supported by the National Natural Science Foundation of China (NSFC) under Grants No. 61170241 and No. 61073042, and the open program of State Key Laboratory of Networking and Switching Technology under Grant No. SKLNST-2009-01-10.

REFERENCES

[1] C.C. Chang and T.C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, no. 3, pp. 165–168, 1993.

[2] W.C. Ku and S.M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 204–207, 2004.

[3] I.E. Liao, C.C. Lee, and M.S. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727–740, 2006.

[4] Y. Chen, J.S. Chou, and C.H. Huang, "Improvements on two password-based authentication protocols," Cryptology ePrint archive, Technical report 561, 2010.

[5] W.B. Horng, C.P. Lee, and J. Peng, "A secure remote authentication scheme preserving user anonymity with non-tamper resistant smart cards," *WSEAS Transactions on Information Science and Applications*, vol. 7, no. 5, pp. 619–628, 2010.

[6] J. Xu, W.T. Zhu, and D.G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[7] S.K. Sood, "Secure Dynamic Identity-Based Authentication Scheme Using Smart Cards," *Information Security Journal: A Global Perspective*, vol. 20, no. 2, pp. 67–77, 2011.

[8] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in proceedings of CRYPTO'99, LNCS, vol. 1666, 1999, pp. 388–397.

[9] F.X. Standaert, T.G. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," in proceedings of Advances in Cryptology-EUROCRYPT 2009, LNCS, vol 5479, 2009, pp. 443–461.
[10] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.
[11] S.B. Wilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in proceedings of 6th IMA International Conference on Cryptography and Coding, Cirencester, LNCS, vol. 1355, 1997, pp.30–45.
[12] H. Krawczyk, "HMQV: A High-Performance Secure Diffie-Hellman Protocol," in proceedings of CRYPTO'05, LNCS, vol. 3621, 2005, pp. 546–566.
[13] R.C. Wang, W.S. Juang, and C.L. Lei, "Robust authentication and key agreement scheme preserving the privacy of secret key," *Computer Communications*, vol. 34, no. 3, pp. 274–280, 2011.
[14] S.H. Wu, Y.F. Zhu, and Q. Pu, "Robust smart-cards-based user authentication scheme with user anonymity," *Security and Communication Networks*, vol. 5, no. 2, pp. 236-248, 2012.
[15] C.G. Ma, D. Wang and Q. M Zhang, "Cryptanalysis and improvement of Sood et al.'s dynamic id-based authentication scheme," in proceedings of 8th International Conference on Distributed Computing and Internet Technology, Lecture Notes in Computer Science, Vol. 7154, 2012, pp. 141–152.
[16] E.J. Yoon, E.K. Ryu, K.Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 612–614, 2004.
[17] H. C. Hsiang and W. K. Shih, "Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," Computer Communications, vol. 32, no. 4, pp. 649–652, 2009.
[18] C.T. Li and C.C. Lee, "A Robust Remote User Authentication Scheme using Smart Card," Information Technology and Control, vol. 40, no. 3, pp. 231–238, 2011.
[19] D.V. Klein, "Foiling the Cracker: A Survey of, and Improvements to, Password Security," in proceedings of 2nd USENIX Security Workshop, 1990, pp. 5–14.
[20] L. Gong, "A security risk of depending on synchronized clocks," *ACM Operating System Review*, vol. 26, no. 1, pp. 49–53, 1992.
[21] D. He, M. Ma, Y. Zhang, and C. Chen, "A strong user authentication scheme with smart cards for wireless communications," *Computer Communications*, vol. 34, no. 3, pp. 367–374, 2011.
[22] C.G. Ma, D. Wang, P. Zhao and Y.H. Wang, "A new dynamic ID-based remote user authentication scheme with forward secrecy," in proceedings of the 14th Asia-Pacific Web Conference (APWeb Workshops 2012), Lecture Notes in Computer Science, Vol. 7234, pp. 199–211, Springer-Verlag, 2012.
[23] D. Wang and C.G. Ma, "Cryptanalysis and security enhancement of a remote user authentication scheme", The Journal of China Universities of Posts and Telecommunications, vol. 19, no. 5, pp.104-114, 2012
[24] H.R. Chung, W.C. Ku, and M.J. Tsaur, "Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 863–868, 2009.
[25] W.B. Mao, *Modern Cryptography: Theory and Practice*, Prentice Hall PTR, New Jersey (2004)
[26] D.S. Wong, H.H. Fuentes, and A.H. Chan, "The Performance Measurement of Cryptographic Primitives on Palm Devices," in Proceedings of ACSAC'01, pp. 92–101, 2001.
[27] N.R. Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Transactions on Mobile Computing*, vol.5, no. 2, pp. 128–143, 2006.
[28] S. Halevi, H. Krawczyk, "Public-key cryptography and password protocols," ACM Transactions on Information and System Security, vol. 2, no. 3, pp. 230–268, 1999.
[29] D. Wang, C.G. Ma, and W. P., "Secure password-based remote user authentication scheme with non-tamper resistant smart cards," in proceedings of 26th Annual IFIP Conference on Data and Applications Security and Privacy (DBSec 2012), Lecture Notes in Computer Science, Vol. 7371, pp. 114–121, Springer Berlin /Heidelberg, 2012.

Ding Wang received his B.S. Degree in Information Security from Nankai University, China, in 2008. And then he went to Information Engineering University of PLA to work toward Information Security Engineering. Currently, he is under the supervision of Prof. Chunguang Ma. He has published more than 20 research papers in international journals and conferences. His research interests include cryptographic protocols and wireless network security.

Chunguang Ma is currently a Professor and Ph.D. candidate supervisor in the Department of Computer Science and Technology, Harbin Engineering University. He got his Ph.D. degree in cryptography from Beijing University of Posts and Telecommunications. His current research interests include cryptography, information security and wireless sensor networks.

Qiming Zhang got his Bachelor degree from Henan Polytechnic University in 2010. Currently, he is under the supervision of Prof. Chunguang Ma. His research interests include cryptography, wireless network security and trusted computing.

Sendong Zhao is currently one postgraduate student of Harbin Engineering University. His current research interests include cryptography, network security, software security, network massive data processing.