

# A Secure Remote User Authentication Scheme with Smart Cards

Manoj Kumar

Department of Mathematics

R. K. College Shamli-Muzaffarnagar U.P.-India- 247776

E-mail: yamu\_balyan@yahoo.co.in

## Abstract

*Remote user authentication scheme is one of the simplest and the most convenient authentication mechanisms to deal with secret data over insecure networks. These types of schemes are applicable to the areas such as computer networks, wireless networks, remote login systems, operation systems and database management systems. The goal of a remote user authentication scheme is to identify a valid card holder as having the rights and privileges indicated by the issuer of the card. In recent years, so many remote user authentication schemes have been proposed to authenticate a legitimate user, but none of them can solve all possible problems and withstand all possible attacks. This paper presents a secure remote user authentication scheme with smart cards. The proposed scheme provides the essential security requirements and achieves particular attributes.*

## 1. Introduction

In today's electronic era, smart card based remote user authentication schemes are widely acknowledged as one of the most secure and reliable forms of electronic identification. With the help of remote user authentication schemes, people can interact with the sever through distributed or portable terminals. In a remote user authentication scheme, the authenticity and integrity of the user and the server are important elements over an insecure network. At their best, the remote user and remote server can securely authenticate each other, processing and protecting the communication in a convenient and user friendly manner. At the worst, some security vulnerabilities can be there.

Actually, a password based remote user authentication scheme consists three components: remote user, remote server and an insecure channel to connect them. A typical smart card based remote user authentication scheme comprises three phases: registration phase, login phase and authentication phase. In the registration phase, a user  $U$  sends a registration request to  $AS$  and submits some necessary information to the server through a secure channel. The server uses the user's identity and password along with its long-term secret to generate some values and stores some of them in a smart card, which then delivered to the user. In the login phase, a user attaches his smart card to a smart card reader and keys in his identity and password to login the server to gain access right. The smart card then uses the password and the values in the card to construct a login request and then sends it to the remote server. In the authentication phase, the server uses its long-term secret to check the validity of the login request. If mutual authentication is required, the server also uses its long-term secret to construct a message and sends it back to the user. The user then uses his password and the values in the smart card to check the validity of the message.

Lamport [27] proposed the first well-known password based remote user authentication scheme using smart cards. However, Lamport's scheme has the three drawbacks as follows:

- it has high hash overhead.
- it requires password resetting.
- a password (verification) table should be stored at the server.

Researchers later have tried to solve the the drawbacks of Lamport's scheme. Recently, quite a number of password authentication schemes with smart cards have been proposed [10]. Although, so many remote user authentication with smart cards have been proposed, but none of them can solve all possible problems and withstand all possible attacks.

### 1.1 Points of vulnerabilities in a remote user authentication scheme

A remote user authentication scheme consists remote user, remote server and a insecure channel for communication. These all three components are responsible for the security strength and vulnerabilities in a remote user authentication scheme. This section categories all those security vulnerabilities in three parts:

- *security vulnerabilities due to remote user* - The registered remote user is a strong antagonist. He can use the registered identity and the corresponding password to construct a fabricated login request or he can construct new identity and password. The registered user can use his credentials to impersonate other users or can frame any kind of guessing attack, impersonation attack, password guessing attack, guessing attack on the long term secret key of the remote server, replaying the previous sessions.
- *security vulnerabilities due to remote server*- The insider at the server is also a powerful attacker. He can guess the password of the registered remote user, if some information stored at the server. If at the time of registration, the password is transmitted in plaintext, then the insider can misuse this password. On the other side, the insider is also able to guess some useful information with the help of registered information.
- *security vulnerabilities due to insecure channel* - In a remote user authentication scheme, some information are openly transmitted through the insecure channel. It is assumed that any attacker can intercept the insecure channel and then these intercepted information can be used to construct any fabricated information.

Thus, in order to develop a secure remote user authentication scheme, we are concerned with these above three points of vulnerabilities. To solve these vulnerabilities, mutual authentication and secure session key generation are two different tools provided by cryptography. For security point of view, it is better to consider these topics jointly rather than separately. A remote user authentication without secure session key exchange is susceptible to an enemy who waits until the authentication is complete and then takes over one end of the communications line. Such an attack is not precluded by a key exchange that is independent of authentication. Secure key exchange and mutual authentication should be linked in such a way that a party has assurances that an exchanged key (which might be used to facilitate privacy or integrity and thus keep authenticity alive) is in fact shared with the authenticated party, and not an impostor. For these reasons, it is essential to keep secure key exchange in mind in the design and analysis of a remote user authentication scheme with smart cards. Keeping in mind the necessary requirements for a secure remote user authentication scheme, this paper proposed a secure remote user authentication scheme. This paper also discusses the security and attributes of the proposed scheme.

The remainder of this paper is organized as follows. Section 2 is about the notations used throughout this paper. Section 3 presents a secure remote user authentication scheme with smart cards. The security of the proposed scheme is analyzed in section 4. Section 5 is about the attributes of proposed scheme. Finally, comes to a conclusion in the section 6.

## 2. Notations

The notations used through out this paper are summarized as follows:

- $U$  denotes a remote user.
- $ID$  denotes an identity of a remote user  $U$ .
- $ID_S$  denotes an identity of a remote server.
- $PW$  denotes a password corresponding to a registered identity  $ID$ .

- $AS$  denotes an authentication server.
- $x_s$  denotes a permanent secret key of an authentication server.
- $f(\cdot)$  denotes a cryptographic one way hash function.
- $\oplus$  denotes the bitwise XOR operation.
- $U \Leftarrow AS: M$  denotes that the user  $U$  sends  $M$  to the server  $AS$  through a secret channel.
- $U \Rightarrow AS: M$  denotes that user  $U$  sends  $M$  to the server  $AS$  through an open channel.
- $p$  denotes a large prime number.
- $S_{ID}$  denotes the redirected identity corresponding to a registered identity  $ID$ .
- $C_{ID}$  denotes a check digit sum corresponding to a registered identity  $ID$ .
- $Red(\cdot)$  denotes a function to redirect the identity  $ID$  for every user  $U$ , which is only possessed with the  $AS$ .
- $C_K(\cdot)$  denotes a function to generate check digit for the registered identity, which is only possessed with the  $AS$ .

### 3. A Secure Remote User Authentication Scheme with Smart Cards

Most of the previous remote user authentication schemes [10] do not have password change phase and there is no mutual authentication and session key generation between the remote user and remote server for secure communication. On the other end, the secret key of the  $AS$  is a long-term key. It means the secret key of the server requires further security. Consider the situation, when the secret key of the  $AS$  is revealed or compromised by an accident or stolen etc, then it is not better to replace/alter the whole system at the  $AS$ . It is also not efficient to replace/alter the secret key of the  $AS$  with the previously registered identities and their corresponding passwords. However, the secret key of the  $AS$  requires further security in term of forward secrecy: the revelation or publication of the secret key of the  $AS$  does not result in compromise of the security

of the previously registered identities and their corresponding passwords.

Keeping in mind all the above requirements, this section presents a secure remote user authentication scheme with smart cards. The proposed scheme provides forward secrecy to the  $AS$ . Forward secrecy ensures that the previously generated identities and their corresponding passwords in the  $AS$  are secure even if the systems secret key  $x_s$  has been revealed or known publicly by an accident or is stolen by any adversary etc. The proposed scheme uses two functions: redirected function  $Red(\cdot)$  to redirect the registered identity  $ID$  and a check digit function  $C_K(\cdot)$  to generate the corresponding check digit for each registered identity. In this scheme, only the  $AS$  can redirect the registered identity  $ID$  and he is able to generate a valid identity and the corresponding check digit. This scheme has four phases: registration phase, login phase and verification phase and password change phase. These phases are described below.

#### 3.1. Registration Phase

This phase is invoked whenever a user  $U$  wants to register himself at the remote server  $AS$ . This phase is executed over a secure channel. The following steps are involved in this phase.

Step  $R_1$

$U \Leftarrow AS: J$ .

The string  $J$  is a unique registration request, consists the name of the user  $U$ , address, identity  $ID_U$ ,  $R_1 = ID^{PW} \bmod p$  where  $PW$  is a password selected by the user and a identification number etc.

Step  $R_2$

Upon receiving the registration request, the  $AS$  computes the followings parameters:

- $S_{ID} = Red(ID)$ ,
- $C_{ID} = C_K(S_{ID})$ ,
- $R_2 = R_1^{x_s} \bmod p$ .

Step  $R_3$

$AS \Leftarrow U$ : Smart card.

In the proposed scheme, the smart card of a user  $U$  contains the parameters  $S_{ID}, C_{ID}, R_1, R_2, p, f$ .

### 3.2. The Login Phase

Whenever, the user wants to gain the access right on the *AS*, *U* attaches her/his smart card to the smart card reader and keys in the PIN (Personal Identification Number) [15], [34] to active the smart card. If the PIN code is entered incorrectly multiple times, the smart card may request a PUK (Personal Unblocking Key) [15], [34] code. The user inputs her/his identity *ID* and the corresponding password *PW*. The smart card of the user *U* conducts the following computations:

Step L<sub>1</sub>

- Computes  $R_3 = S_{ID} \oplus PW$  and stores this value in the smart card. This sub-step is computed only when the user *U* attaches his smart card at the first time to the smart card reader, otherwise skip this.
- Compute  $R_1 = ID^{PW} \bmod p$  and compare the calculated  $R_1$  and stored  $R_1$ , if they are equal the smart card accept the password *PW* and proceeds to the next step ,otherwise demands the password again. If the password is entered incorrectly multiple times, the smart card may request a *PUK* (Personal Unblocking Key) code.

Step L<sub>2</sub>

- Compute  $C_1 = R_2^{PW^{-1}} \bmod p$  and  $C_2 = f(C_1 \oplus T_U)$ , where  $T_U$  is the current date and time of the smart card reader.

Step L<sub>5</sub>

- $U \implies AS: L_R = (ID, C_2, T_U)$ .

### 3.3. The Verification Phase

Assume that the *AS* receives the login request  $L_R$  at time  $T_c$ . Then, *AS* does the following computations to check the validity of the login request  $L_R$ .

Step V<sub>1</sub>

- Check the specific format of the identity *ID*. If the format of the identity is incorrect, then *AS* rejects the login request  $L_R$ .

Step V<sub>2</sub>

- Computes the value  $S_{ID} = Red(ID)$ . Check, whether the condition  $C_{ID} = C_K(S_{ID})$  holds, if not, then *AS* rejects the login request  $L_R$ .

Step V<sub>3</sub>

- Check, whether  $T_c - T_U \leq \Delta T_K$ , where  $\Delta T_K$  is the legal time interval due to transmission delay, if not, then *AS* rejects the login request  $L_R$ .

Step V<sub>4</sub>.

- Check, if  $C_2 = f(ID^{x_s} \oplus T_U) \bmod p$ , then the *AS* accepts the login request and proceeds to the next step, Otherwise the login request will be rejected by *AS*.

Step V<sub>5</sub>.

The *AS* select a random number *r* and computes

- $C_3 = f(ID^{x_s} \oplus T_S)$ , where  $T_S$  is the current time at *AS*.
- $S_{key} = f(ID, ID_S, C_3, r)$ ,
- $C_4 = C_3 \oplus S_{key}, C_5 = C_3 \oplus r$ .

Step V<sub>6</sub>

- $AS \implies U: (C_4, C_5, T_S)$ .

Step V<sub>7</sub>

Assume that the *U* receives the message  $(C_4, C_5, T_S)$  at time  $T_L$ , then

- *U* verifies, whether  $T_L - T_S \leq \Delta T_U$ , where  $\Delta T_U$  is the legal time interval due to transmission delay, if not, then *U* interrupts the connection.
- *U* computes  $C_3^* = f(C_1 \oplus T_S)$ .
- Computes  $K^* = C_3^* \oplus C_4$ .
- Computes  $r^* = C_3^* \oplus C_5$ .
- Computes  $S_{key}^* = f(ID, ID_S, C_3^*, r^*)$ .
- Compares  $S_{key}^*$  and  $K^*$  for mutual authentication, if they are equal the user *U* ensures that the responding system is a real *AS* and proceeds to the next step. otherwise *U* interrupts the connection. The number  $S_{key}^*$  will be the session key between the user *U* and *AS*,

Step V<sub>8</sub>

- $U$  Computes  $C_6 = f(C_3^*, S_{key}^*)$ ,
- $U \implies AS: (ID, C_6)$

Step V<sub>9</sub>

- $AS$  checks, if  $C_6 = f(C_3, S_{key})$ , then the  $AS$  assures that the user  $U$  also generates the same session key, otherwise rejects the connection.

### 3.4. The Password Change Phase

This phase is invoked whenever  $U$  wants to change his password  $PW$  with a new password, say  $PW_{new}$ . This phase has the following steps.

Step P<sub>1</sub>

- $U$  inserts her/his smart card to the smart card reader and then keys in the PIN to active the smart card, then inputs her/his identity and the old password  $PW$  and then requests to change the password.

Step P<sub>2</sub>

- Compute  $S_{ID}^* = R_3 \oplus PW$  and compare the calculated  $S_{ID}^*$  and stored  $S_{ID}$ , if they are equal the smart card accept the password  $PW$  and proceeds to the next step, otherwise demands the password again. If the password is entered incorrectly multiple times, the smart card may request a PUK (Personal Unblocking Key) code.

Step P<sub>3</sub>

- $U$ 's smart cards computes  $R_3^* = S_{ID} \oplus PW_{new}$ ,  $R_2^* = R_2^{PW_{old}^{-1} \times PW_{new}}$ , then replaces  $R_2$  with  $R_2^*$  and  $R_3$  with  $R_3^*$ .

## 4 Security Analysis of the Proposed Scheme

This section analyzes the security of the proposed scheme.

- **Replay Attacks**-When the adversary impersonates a legal user to login the specified server by replaying the transmitted messages between the

legal user and that server, then we say that this protocol is vulnerable to the replay attack [30]. Suppose that an adversary collects the messages  $L_R = (ID, C_2, T_U)$  from Step L<sub>5</sub>,  $(C_4, C_5, T_S)$  from Step V<sub>6</sub> and  $(ID, C_6)$  from Step V<sub>8</sub> of the proposed protocol when the user  $U$  logs into the server  $AS$ . The adversary impersonates the user  $U$  to login the server  $AS$  by replying the message  $L_R = (ID, C_2, T_U)$ . The Step V<sub>3</sub> of the verification phase does not satisfy, due to the invalid time interval. It is clear that the adversary can not select a valid time  $T$  to avoid this invalid transmission delay. Thus, the server will detect that he/she is not a valid user  $U$ .

Also, the adversary can not generate the correct  $(C_4, C_5, T_S)$  corresponding to  $r_1$  and returns it to the user  $U$  because he does not know the secret key of the server  $AS$ . In this case, the user  $U$  will detect the fabricated server with the help of Step V<sub>7</sub>. In the same way, the Step V<sub>9</sub> will detect the replaying of the message  $(ID, C_6)$ . Hence, it is very hard for an adversary to masquerade the legal user to login the server by replaying the old message.

- **Denial of Service Attacks**- In this attack, an attacker can update false verification information of a legal user for the next login phase. Afterwards, the legal user will not be able to login successfully anymore. In our scheme no information is stored at the server, so this attack will not work.
- **Explicit key authentication**- Let  $U$  and  $AS$  be two honest terminals who execute the steps of an authentication protocol correctly, then an authentication scheme provides the explicit key authentication, if it should satisfy following two properties [16]:
  - **Implicit key authentication**- Informally speaking, an authentication protocol is said to provide implicit key authentication ( of  $AS$  to  $U$ ) if entity  $U$  is assumed that no other entity from a specifically identified second entity  $AS$  can possibly learn the value of the particular secret key.
  - **Key confirmation** - an authentication protocol is said to provide key confirmation( of

AS to  $U$ ) if entity  $U$  is assumed that second entity  $AS$  actually possession of a particular secret key

Observe the steps  $V_5$  to  $V_7$  verification section of the proposed scheme. These steps shows that only the specified user and specified server can get correct information which can be used to generate a valid session key. This means that the proposed scheme provides implicit key authentication. In step  $V_7$  the server  $AS$  assures the user had computed the same session By this result, it is clear that the proposed protocol provides explicit key authentication.

- **Stolen verifier attack** - The proposed scheme is free from the stolen verifier attack [9]. There is no such information is stored at the server by which an adversary can make a fabricated login request to impersonate a legal user to login the server or can impersonate the server to cheat the legal user.
- **Parallel Session Attacks**- In parallel session attack, without knowing the correct password of the user, an attacker can masquerade as the legal user by creating a valid login message out of some eavesdropped communication between the user and the server. The verification steps  $V_3$ ,  $V_7$  and  $V_9$  block this attack. The attacker is also not able to get any information about the password from the login request.
- **Password Guessing Attacks**- Most passwords have such low entropy that it is vulnerable to password guessing attacks, where an attacker intercepts authentication messages and stores them locally and then attempts to use a guessed password to verifies the correctness of his/her guess using these authentication messages. In our scheme, the password is not transmitted in plain text over the network. Thus, the attacker will not be able to guess the password.
- **Smart Card Loss Attacks**- When the smart card is lost or stolen, unauthorized users can easily change the password of the smart card, or can guess the password of the user by using password guessing attacks, or can impersonate the user to

login to the system. In our scheme, the old password id requires to have a new password, in this way, only the authorized user is able to change his password. On the other side, if the password is entered incorrectly multiple times and the attacker tries to guess the password, the smart card may request a PUK (Personal Unblocking Key) code.

## 5. Attributes of the Proposed Scheme

- **Forward Secrecy**- Take a look on the registration phase of our scheme. With a secret key  $x_s$ , the  $AS$  uses two additional functions:  $Red(.)$  and  $C_K(.)$ , which are always in possession of  $AS$ . In this way, only the  $AS$  is able to compute a redirected/ shadowed identity  $S_{ID}$  and a check digit sum  $C_{ID}$  corresponding to every valid identity  $ID$ . Unfortunately, if the secret key  $x_s$  of the  $AS$  is revealed or compromised by an accident or stolen etc, then with the help of revealed secret key  $x_s$  any attacker Bob can try to obtain the password  $PW$  corresponding to the previously registered identity string  $J>ID$  or he can try to generate new password by selecting a newly valid identity string  $J_{new}$ . Thus, he can try to obtain some fake passwords. But, when he tries to obtain the password  $PW$  corresponding to a previously registered  $ID$  or the password corresponding to a newly selected valid identity string  $J_{new}$ , he is required to compute a redirected/ shadowed identity  $S_{ID}$  and a check digit sum  $C_{ID}$  corresponding to every valid identity string  $J$ , whether it is old or new. Without the knowledge of corresponding shadowed identity  $S_{ID}$  and a check digit sum  $C_{ID}$  for a identity  $ID$ , the attacker will not be able to recover a valid pair of proper identity and the proper corresponding password to make a valid login request. The login request does not leak any information for the attacker, while the attacker is in possession of the secret key of the  $AS$ . Thus, our scheme provides forward secrecy with respect to the long - term secret key  $x_s$  of the  $AS$  if compromised of the secret key of the  $AS$  does not result in compromise of the security of the previously registered identities and the corresponding passwords. It ensures that the previously gen-

erated passwords in the system are secure even if the systems secret key has been revealed in public by accident or is stolen.

- **Mutual Authentication**-The user and the server can authenticate each other. Not only can the server verify the legal users, but the users can also verify the legal server. Mutual authentication can help withstand the server spoofing attack where an attacker pretends to be the server to manipulate sensitive data of the legal users.
- The password or verification tables are not stored at the server.
- The password cannot be revealed by the administrator of the server.
- The password is not transmitted in plain text over the network.
- In the login phase, whenever the user wants to gain the access right on the AS,  $U$  attaches her/his smart card to the smart card reader and keys in the PIN (Personal Identification Number) [15], [34] to active the smart card. If the PIN code is entered incorrectly multiple times, the smart card may request a PUK (Personal Unblocking Key) [15], [34] code. On the other side, in the password change phase, if the password is entered incorrectly multiple times and the attacker tries to guess the password, the smart card also request a PUK (Personal Unblocking Key) code. Thus in the proposed scheme, any unauthorized login can be quickly detected when a user inputs a wrong PIN/password.
- The proposed scheme has a secure session key generation phases. In the verification phase, a session key is also established to provide confidentiality to the communication.

## 6 Conclusions

This paper proposes a secure remote user authentication scheme with smart cards. The proposed scheme not only provides mutual authentication between the user and server, but also establishes a common session key to provide message confidentiality. In addition, the proposed protocol provides the explicit key

authentication property for established common session keys. The proposed protocol is provably secure to withstand the replay attack, the stolen verifier attack. In the password change phase of the proposed protocol, each user can change his password without connecting to any server.

Always it is prudent to keep the secret key of any AS so that only the authorized person/system can retrieve the secret key, whenever it is required. A possible way is to encrypt the key in a way that it can only be constructed with the help of some sorts of independent servers/machines. To avoid the risk of stealing the secret key of the AS, protection of the secret key can be traded off against revealing or stealing. Unfortunately, if the secret key  $x_s$  of the AS is revealed or compromised by an accident or stolen etc, then with the help of revealed secret key  $x_s$  any attacker Bob/Alice can not recover the complete passwords corresponding to the previously registered identities strings  $J$ . Consequently, the proposed scheme provides the forward secrecy to the long term secret  $x_s$  of the AS and as well as it also overcomes the common security flaws of a remote user authentication scheme.

## References

- [1] B. Wang, J. H. Li, and Z. P. Tong, "Cryptanalysis of an enhanced timestamp-based password authentication scheme," *Computers & Security*, vol. 22, no. 7, pp. 643-645, 2003.
- [2] C. C. Chang and K. F. Hwnag, "Some forgery attack on a remote user authentication scheme using smart cards," *Infomatics*, vol. 14, no. 3, pp. 189-194, 2003.
- [3] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, pp. 165-168, May 1991.
- [4] C. C. Chang and W. Y. Liao, "A remote password authentication scheme based upon ElGamal's signature scheme," *Computers & Security*, vol. 13, no. 2, pp. 137-144, 1994.
- [5] C. C. Yang, H. W. Yang, and R. C. Wang, "Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 578-579, 2004.
- [6] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, vol. 46, pp. 992-993, 2000.

- [7] C. L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 26, no. 3, pp. 167-169, 2004.
- [8] C. L. Hsu, "Security of two remote user authentication schemes using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1196-1198, 2003.
- [9] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," *IEICE Transactions on Communications*, vol. E85-B, pp. 2519-2521, November 2002.
- [10] C. S. Tsai, C. C. Lee, and M. S. Hwang, "Password Authentication Schemes: Current Status and Key Issues," *International Journal of Network Security*, Vol.3, No.2, pp.101115, Sept. 2006.
- [11] H. M. Sun and H. T. Yeh, "Further cryptanalysis of a password authentication scheme with smart cards," *IEICE Transactions and Communications*, vol. E86-B, no. 4, pp. 1412-1415, 2003.
- [12] H. M. Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958-961, 2000.
- [13] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "A modified remote login authentication scheme based on geometric approach," *Journal of Systems and Software*, vol. 55, pp. 287-290, 2001.
- [14] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers & Security*, vol. 21, pp. 372-375, 2002.
- [15] <http://www.gsm-security.net/>
- [16] IEEE P1363.2-D13, 2004. Standard Specifications for Password-based Public Key Cryptographic Techniques. IEEE P1363 working group, 12 March.
- [17] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414-416, 2003.
- [18] J. J. Shen, C. W. Lin, and M. S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards," *Computers & Security*, vol. 22, no. 7, pp. 591-595, 2003.
- [19] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1243-1245, 2003.
- [20] K. F. Chen and S. Zhong, "Attacks on the (enhanced) Yang Shieh authentication," *Computers & Security*, vol. 22, no. 8, pp. 725-727, 2003.
- [21] K. Manoj, "A forward secure remote user authentication," Report No. 2007/303. <http://www.eprint.iacr.org>
- [22] K. Manoj, "A new remote user authentication scheme using smart cards with forward secrecy," Report No. 2004/192. <http://www.eprint.iacr.org>.
- [23] K. Manoj, "New remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 597-600, 2004.
- [24] K. Manoj, "Some remarks on a remote user authentication scheme using smart cards with forward secrecy," *IEEE Trans. Consumer Electronic*, vol. 50, no. 2, pp. 615-618, May 2004. 15.
- [25] K. Manoj, "A Forward Secure remote user authentication scheme," Report No. 2007/303. The full paper is also available on <http://www.eprint.iacr.org>
- [26] Kuhn, Markus (July 1997). "Probability theory for pickpockets - ec-PIN guessing".
- [27] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, pp.770-772, November 1981.
- [28] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28-30, 2000.
- [29] M. S. Hwang, C. C. Lee, and Y. L. Tang, "A simple remote user authentication scheme," *Mathematical and Computer Modelling*, vol. 36, pp. 103-107, 2002.
- [30] S. M. Yen and K. H. Liao, "Shared authentication token secure against replay and weak key attacks," *Information Processing Letters*, vol. 62, pp. 77-80, 1997.
- [31] S. W. Lee, H. S. Kim, and K. Y. Yoo, "Improved efficient remote user authentication scheme using smart cards," *IEEE Transactions on Communications*, vol. 50, pp. 565-567, May 2004.
- [32] T. C. Wu, "Remote login authentication scheme based on a geometric approach," *Computer Communications*, vol. 18, no. 12, pp. 959-963, 1995.
- [33] T. C. Yeh, H. Y. Shen, and J. J. Hwang, "A secure one-time password authentication scheme using smart cards," *IEICE Trans. On Communications*, vol. E85-B, pp. 2515-2518, Nov. 2002.
- [34] Timothy M. Jurgensen, Scott B. Guthery, *Smart Cards: The Developer's Toolkit*, ISBN-10: 0-13-093730-4; ISBN-13: 978-0-13-093730-8; Published by Prentice Hall.
- [35] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," *Computers & Security*, vol. 18, no. 8, pp. 727-733, 1999.
- [36] W. S. Juang, "Efficient multi-server password authentication key agreement using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 251-255, 2004.