# On the Weaknesses and Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards

**Manoj Kumar**

Department of Applied Sciences and Humanities
Hindustan College of Science & Technology
Farah, Mathura, (U.P.) India- 281122.
E. Mail: yamu_balyan@yahoo.co.in

**Abstract.** In 2002, Chien et al. proposed an efficient remote user authentication scheme using smart cards. Later, in 2004, W. C. Ku and S. M. Chen pointed out some attacks on Chien et al.'s scheme. W. C. Ku and S. M. Chen also proposed a modified scheme to prevent the attacks on Chien et al.'s scheme. This paper discusses the security of the W. C. Ku and S. M. Chen's scheme. This paper aims to show that the modified scheme is still vulnerable to the password guessing attack and the insider attack.

Key Words: **Cryptography, Cryptanalysis, Network security, Remote user authentication, Smart card, Password, Reflection attack, Password guessing attack and Insider attack.**

## I. INTRODUCTION

To authenticate the legitimacy of the remote users over insure channel, a remote password authentication scheme is used. In such a scheme, the password often regarded as a secret shared between the *authentication server* (***AS***) and serves to authenticate the identity of the individual logging on to the server. Through the knowledge of the password, the remote user can use it to create a valid login message to the authentication server**.** To provide the access right to the user *U*, *AS* checks the validity of the login message. Password authentication schemes with smart cards have a long history in the remote user authentication environment. So far different types of password authentication schemes with smarts cards [2]-[3]-[4]-[5]-[9]-[11]-[13]-[15]-[16]-[18]-[19]-[28]- [29] have been proposed.

In 1981, Lamport [14] proposed the first well-known remote user authentication scheme without using encryption techniques. In this scheme, a password table is required to achieve user authentication. However, high hash overhead and the necessity for password resetting decrease the suitability and practical use of Lamport's scheme. In addition, the Lamport scheme is vulnerable to a small *n* attack [6]. Since then, many similar schemes [21]-[22] have been proposed. They all have a common feature: *a verification password table should be securely stored in the AS.* Actually, this property is a disadvantage for the security point of view. If the password table is stolen /removed /modified by the adversary, the *AS* will be partially or totally affected.

In 2000, Hwang and Li [18] pointed out that Lamport' s scheme [14] suffered with the risk of a modified password table and the cost of protecting and maintaining the password table is also a matter of concern. They also proposed a new remote user authentication scheme using smart cards. In particular, there is no need of a verification table to check the authenticity of the login request in Hwang and Li's scheme. Further, in 2002, Chien – Jan and Tseng [10] introduced an efficient remote user authentication scheme using smart cards. In 2004, Ku and Chen [28] pointed out some attacks [8]-[25]-[27] on Chien – Jan and Tseng' s scheme. According to Ku and Chen, Chien et al.'s scheme is vulnerable to a reflection attack [8] and an insider attack [27]. Ku and Chen claimed that Chien et al.'s scheme is also not reparable [25]. In addition, they also proposed an improved scheme to prevent the attacks: reflection attack and an insider attack on Chien – Jan and Tseng' s scheme.

### *Contributions*

This paper discusses the security of the W. C. Ku and S. M. Chen's scheme. This paper aims to show that that the modified scheme is still vulnerable to the password guessing attack and the insider attack. This paper is organized as follows.

### *Organization*

Section II reviews the Chien et al.'s Scheme. Section III describes the Ku and Chen's Attacks on Chien et al.'s Scheme. Section IV reviews the Ku and Chen's Scheme. Our observations and analysis about the security of Ku and Chen's scheme are discussed in V. Finally, comes to a conclusion in the section VI.

## II. REVIEW OF CHIEN ET AL.'S SCHEME

This section briefly describes Chien et al's scheme [10], which consists of three phases: the registration phase, login phase and the verification phase. All these three phases are described below.

### *A. Registration Phase*

In the registration phase, the user $U$ sends a request to the $AS$ for the registration. The $AS$ will issue a smart card to every legal user $U$ through a secure channel. The following steps are involved in this phase.

- User $U$ submits her/his identity $ID$ and password $PW$ to the $AS$ through a secure channel.
- $AS$ computes a secret number $R = f\,(ID \oplus x) \oplus PW$ and creates an entry for the user $U$ in his account database.

Here, $x$ is a secret key of the $AS$ and $f$ is a one –way hash function. $AS$ provides a smart card to the user $U$ through a secure channel. The smart card contains the secret number $R$ and a one-way hash function $f$.

### *B. Login Phase*

In the login phase, whenever the user $U$ wants to access the $AS,$ she/he inserts her/his smart card to the smart card reader and then keys the identity $ID$ and the corresponding password $PW$ to access the services. The smart card will perform the following operations:

- Compute $C_1= R$ ▯ $PW$ and $C_2 = f\,(C_1 \oplus T_U)$. Here $T_U$ denotes the current date and time of the smart card reader.
- Sends a login request $C = (ID, C_2, T_U)$ to the $AS$.

### *C. Verification Phase*

Assume $AS$ receives the login request $C$ at time $T_S$ , where $T_S$ is the current date and time at $AS$. Then the $AS$ takes the following actions to check the authenticity of the login request.

- If the identity $ID$ and the time $T_U$ is not valid, then $AS$ accepts this login request. Otherwise, the login request $C$ will be rejected.
- Checks, if $C_2 \overset{?}{=} f\,(f\,(ID \oplus x) \oplus T_U)$, then the $AS$ accepts the login request and computes $C_3 = f\,(f\,(ID \oplus x) \oplus T_S)$. Otherwise, the login request $C$ will be rejected.
- $AS$ sends $(T_S\,, C_3)$ to the user $U$ for mutual authentication.
- If the time $T_S$ is valid, then $U$ verifies the equation $C_3 \overset{?}{=} f\,(C_1 \oplus T_S)$ to authenticates $AS$.

## III. Ku and Chen's Attacks on Chien et al.'s Scheme

According to Ku and Chen, Chien et al.'s scheme is vulnerable to a reflection attack [8] and an insider attack [27]. In addition, if the password of the user $U$ in Chien et al.'s scheme is compromised then the scheme is not reparable [25]. This section reviews these attacks.

### *A. Reflection Attack*

According to Ku and Chen, a malicious user intercepts the login request $C = (ID, C_2, T_U)$ and replaces the pair $(T_s, C_3)$ with $(T_U, C_2)$ in the verification phase. When the user $U$ receives the pair $(T_U, C_2)$, he verifies $C_2 \overset{?}{=} f(C_1 \oplus T_U)$, which holds truly. In this way, a malicious user reflects $AS$ and $U$ will be fooled. Thus, Chien et al.'s scheme fails to provide mutual authentication and vulnerable to the reflection attack.

### *B. Poor Reparability*

According to Ku and Chen, Chien et al.'s scheme is not reparable. In Chien et al.'s scheme an adversary can recover the secret value $R$, which is stored in the smart card of the user $U$. After obtaining this secret value $R$, he can obtain the corresponding password $PW$ by performing a password guessing attack. The adversary intercepts the login request $C = (ID, C_2, T_U)$. First, he guesses a password $PW^*$ and then computes $C_1^* = R \square PW^* = f(ID \oplus x)^*$ and $C_2^* = f(C_1^* \oplus T_U)$. If $C_2^* = C_2$, then the adversary has correctly guessed the password $PW^* = PW$ and $C_1^* = C_1$. Once the adversary has correctly obtain $C_1$, then he can impersonate the legal user $U$. This attack can be failed if user $U$ has detected that his $C_1$ has been compromised and then changed his password $PW$ via some means that is not specified in Chien et al.'s scheme. Since, the password $PW$ is the function of the identity $ID$ of the user $U$ and the secret key $x$ of $AS$, therefore, to change the password $PW$ for $U$, $AS$ has to change $ID$ or $x$. However, since $x$ is commonly used for all users rather than specifically used for only $U$. It is not reasonable and efficient to change the secret key $x$ for the security of a single user $U$. Additionally; it is also impractical to change identity of the user $U$. Thus, they claimed that the Chien et al.'s scheme is not reparable

### *C. Insider Attack*

According to Ku and Chen, the password of the user $U$ will be reveal to $AS$ in the registration phase. If the user $U$ uses the same password to access other servers for convenience, the insider of $AS$ can impersonate the user $U$ to access other services.

## IV. Review of Ku and Chen's Scheme

This section briefly describes Ku and Chen's scheme [28]. This scheme has four phases: the registration phase, login phase, verification phase and the password change phase. All these four phases are described below.

### *A. Registration Phase*

This phase is invoked whenever $U$ initially or re-registers to $AS$. Let $n$ denotes the number of times $U$ re-registers to AS. The following steps are involved in this phase.

- User $U$ selects a random number $b$ and computes $PW_S = f\,(b \oplus PW)$ and submits her/his identity $ID$ and $PW_S$ to the $AS$ through a secure channel.
- $AS$ computes a secret number $R = f\,(EID \oplus x) \oplus PW_S$, where $EID = (ID \| n)$ and creates an entry for the user $U$ in his account database and stores $n = 0$ for initial registration, otherwise set $n = n+1$, and $n$ denotes the present registration.
- $AS$ provides a smart card to the user $U$ through a secure channel. The smart card contains the secret number $R$ and a one-way function $f$.
- User $U$ enters his random number $b$ into his smart card.

### *B. Login Phase*

For login, the user $U$ inserts her/his smart card to the smart card reader and then keys the identity and the password to access services. The smart card will perform the following operation:

- Computes $C_1 = R$ ▯ $f\,(b \oplus PW)$ and $C_2 = f\,(C_1 \oplus T_U)$. Here $T_U$ denotes the current date and time of the smart card reader.
- Sends a login request $C = (ID, C_2, T_U)$ to the $AS$.

### *C. Verification Phase*

Assume $AS$ receives the message $C$ at time $T_S$ , where $T_S$ is the current date and time at $AS$. Then the $AS$ takes the following action:

- If the identity $ID$ and the time $T_U$ is not valid, then $AS$ will rejects this login request.
- Checks, if $C_2 \overset{?}{=} f\,(f\,(EID \oplus x) \oplus T_U)$, then the $AS$ accepts the login request and computes $C_3 = f\,(f\,(EID \oplus x) \oplus T_S)$. Otherwise, the login request $C$ will be rejected.
- $AS$ sends the pair $T_S$ and $C_3$ to the user $U$ for mutual authentication.
- If the time $T_S$ is invalid *i.e.* $T_U = T_S$ then $U$ rejects the request. Otherwise, $U$ verifies the equation $C_3 \overset{?}{=} f\,(C_1 \oplus T_S)$ to authenticates $AS$.

### *D. Password Change Phase*

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

- *U* inserts her/his smart card to the smart card reader keys the identity and the password and then requests to change the password. Next, *U* enters a new password $PW_{new}$.
- *U*'s smart cards computes a new secret number $R_{new} = R \oplus PW_S \oplus f\,(b \oplus PW_{new})$ and then replaces *R* with $R_{new}$.

## V. Our Observation: Cryptanalysis of Ku and Chen' s scheme

Although, Ku and Chen [28] proposed a modified scheme to avoid the reflection [8] and insider attack [27] and they also added one more phase: *password change phase* to enhance the poor reparability [25] of the Chien et al.'s scheme. This section shows that the modified scheme of Ku and Chen cannot withstand password guessing attack and the insider attack by the insider of *AS*. This section shows that the modified scheme is still vulnerable to these attacks: password guessing attack and the insider attack by the an adversary/insider of *AS* and the weaknesses is still exists in the Ku and Chen's scheme. By using similar attacks, an adversary can still impersonate a legal user *U*.

### *A. Password Guessing Attack*

In Ku and Chen's scheme, an adversary is able to obtain the initial password *PW* as well as the renewal $PW_{new}$ of a legal user *U.* The following sub-sections clearly show how can an adversary obtain the password.

### 1. *Attack on the Initial Password PW*

The smart card of a legal user U in Chien et al.'s scheme contains: a *secret value R and a hash function f.* While in Ku and Chen's scheme the smart cards contain: *the secret value R, a random number b and a hash function f.* According to Ku and Chen, for the security point of view to store the secret information in smart cards is not a good practice. On the basis of these assumptions [20]-[26], Ku and Chen proved that Chien et al.'s scheme is not secure and that is under the threat of poor reparability. They proposed a modified form of Chien et al.'s scheme, but, they also committed the same mistake: *store the secret value R, a random number b in the smart cards of the users*. *If an adversary can obtain the secret value R from the smart cards, then he can obtain the secret number b.* Once an adversary has obtained the stored values *R* and *b* from the smart cards of the user *U*, then he can perform a password guessing attack to obtain the password. For the success of this attack, by using the breached secrets $R$ and $b$, the adversary will perform the following operations:

***Step.* 1:** Intercepts the login request $C = (ID, C_2, T_U)$ and guesses a password $PW^*$.

***Step.* 2:** Computes $C_1^* = R \oplus f(b \oplus PW^*) = f(ID \oplus x)^*$ and $C_2^* = f(C_1^* \oplus T_U)$.

***Step.* 3:** Checks if $C_2^* \overset{?}{=} C_2$, then the adversary has correctly guessed the password $PW^* = PW$ and $C_1^* = C_1$. Otherwise, the adversary goes to step: 1.

Once the adversary has correctly obtain $C_1$, then he can impersonate the legal user $U$.

### 2. *Attack on the Renewal Password $PW_{new}$*

According to Ku and Chen, if the user $U$ suspects that her/his $C_1$ has been compromised, she/he selects a new random number $b_{new}$ and a new password $PW_{new}$ and then compute $f(b_{new} \oplus PW_{new})$. Next, the user $U$ reregisters to $AS$ by using $f(b_{new} \oplus PW_{new})$. Upon receiving the re-registration request, $AS$ will set $n_{new} = n + 1$and then computes

$$EID_{new} = (ID \| n_{new}),$$

$$R_{new} = f(EID_{new} \oplus x) \oplus f(b_{new} \oplus PW_{new}).$$

Now $AS$ stores the new secret $R_{new}$ in a new smart card for the user $U$. After, receiving the new smart card, user $U$ enters the new random number $b_{new}$ into it.

As described above, we can easily observe that there is no new change in the security parameters through the renewal phase of the scheme against the password guessing attacks. After the renewal phase, the older secret number $R$ is replace by a new secret number $R_{new}$, which is again computed by the $AS$ and the random number $b$ is replaced by a new random number $b_{new}$, which is again selected by the user $U$. At last, the older smart card is replaced with a new smart cards. Now the user has a new smart card that contains new secret number $R_{new}$ and new random number $b_{new}$. It is clear that all the security parameters and the security environment are remains the same as they were before the renewal phase. It means these new security parameters cannot defend the password guessing attack and the adversary is still able to guess the new password $PW_{new}$ in the same manner as described earlier: attack on the initial password $PW$.

### *B. Insider Attack*

According to Ku and Chen, their scheme is free from the insider attack. They have claimed that the user $U$ registers herself/himself to $AS$ by sending the number $PW_S = f(b \oplus PW)$, instead of $PW$, hence the insider of $AS$ cannot directly obtain the password $PW$. In this way, the random number $b$ will not be reveal to the insider of $AS$. But, we analyze and observe the above situation in a different way and show that Ku and Chen's scheme is not free from the insider attack. We have divided this section into subsections, which clearly show how can an insider of *AS* will be able to impersonate the legal user *U.* The followings are the descriptions of our attack.

**1.** ***Insider Attack Via Initially Registered secret Number R.***

This sub-section shows how an insider of *AS* will successfully impersonate a legal user *U* by an insider attack through the initially registered *ID*. Ku and Chen have claimed that with the help of $PW_S = f\ (b \oplus PW)$, the insider of *AS* is not able to obtain the password *PW.* This argument is backbone of cryptography and we are not against this one-way property of hash function. But, in our observation the insider of *AS* is able to attack Ku and Chen's scheme through a different way.

For the further discussion, first we have to reconsidered the registration phase of Ku and Chen's scheme and then analyze how this registration phase is responsible for the vulnerability of the Ku and Chen's scheme against the insider attack of the insider of *AS.* In this reference, take the following *three true conditions* into consideration:

- *In the registration phase, the User U selects a random number b and computes* $PW_S = f\ (b \oplus PW)$ *and submits her/his identity ID and* $PW_S$ *to the AS through a secure channel. It means the insider of AS is in possession of the number* $PW_S = f\ (b \oplus PW)$ *for the legal user U.*
- *In the registration phase, the AS computes a secret number* $R = f\ (EID \oplus x) \oplus PW_S$*, where* $EID = (ID \| n)$*. Thus, the insider of AS is also in possession of the secret number R for the legal user U.*
- *A remote password authentication is used to authenticate the legitimacy of the remote users over an insecure channel.*

It is clear that the malicious insider of *AS* utilizes these three conditions freely and he can send a valid login request to *AS* or another server $AS^*$, where the user *U* uses the same password *PW* to access several services for her/his convenience. The description of this attack is given below.

Because the insider of *AS* is in the possession of the secret number *R* and another important information $PW_S = f\ (b \oplus PW)$*,* hence by intercepting a valid login request $C = (ID, C_2, T_U)$ emitted from the user *U*, a malicious insider of *AS* (attacker) can construct another fabricated login request $L_B$ such that $L_B$ passes the authentication phase of Ku and Chen's scheme. The $AS/ AS^*$ cannot distinguish between the authentic login request *C* and the fabricated login request $L_B$. The following discussion shows how to do that.

- First, the insider of *AS C*omputes $C_1^{*}= R$ ▯ $PW_S$ and $C_2^{*} = f\,(C_1^{*} \oplus T_U^{*})$. Here $T_U^{*}$ denotes the current date and time, whenever the insider of *AS* (attacker) wants to gain the access right.
- Secondly, the insider of *AS* delivers the fabricated login request $L_{\mathrm{B}} = (ID, C_2^{*}, T_U^{*})$ to the $AS / AS^{*}$.

After receiving the fabricated login request $L_{\mathrm{B}} = (ID, C_2^{*}{}_{,}\ T_U^{*})$, the $AS / AS^{*}$ will authenticate the insider of *AS* (adversary) as a legal user and grant the access right to her/him. The success of the authentication phase is shown below.

Assume $AS / AS^{*}$ receives the fabricated login request $L_{\mathrm{B}} = (ID, C_2^{*}, T_U^{*})$, at time $T_S^{*}$ , where $T_S^{*}$ is the current date and time at *AS*. Then the *AS* takes the following action to authenticate the insider of *AS*.

- Check, the validity of the *ID* and the time $T_U^{*}$. It is obvious because the insider of *AS* has been used a previously registered identity *ID* and the current date and time.
- Check the verification equation $C_2^{*} \overset{?}{=} f\,(f\,(EID \oplus x) \oplus T_U^{*})$, which is also obviously holds true, then $AS / AS^{*}$ computes $C_3 = f\,(f\,(EID \oplus x) \oplus T_S^{*})$.
- *AS* sends the pair $T_S^{*}$ and $C_3$ to the user *U* for mutual authentication.
- Obviously, the time $T_S^{*}$ is valid (since, $T_U^{*} \neq T_S^{*}$) and the equation $C_3 \overset{?}{=} f\,(C_1 \oplus T_S^{*})$ is also holds true to authenticates $AS / AS^{*}$.

In this way, the $AS / AS^{*}$ accepts and then authenticates the fabricated login request $L_{\mathrm{B}}$ that is made by the insider of *AS*. Consequently, the $AS / AS^{*}$ provides all access rights of the legal user *U* to the insider of *AS*. Thus, the insider of *AS* works as an intruder and she/he is able to impersonate a valid user *U*, who holds a valid pair of the identity *ID* and the corresponding password *PW*.

### 2. *Insider Attack Via Renewal Registered Secret Number* $R_{new}$

The insider of *AS* is also able to attack the Ku and Chen's scheme via a renewal registered secret number $R_{new}$. As, we have described earlier that the renewal phase does not make any substantial changes in the security of the scheme. After the renewal phase, the older secret number *R* is replaced by a new secret number $R_{new}$, which is again computed by the *AS* and the random number *b* is replaced by a new random number $b_{new}$, which is again selected by the user *U*. Now the insider of *AS* has the knowledge of a new secret number $R_{new}$ and another important information $f\,(b_{new} \oplus PW_{new})$. Since, the security parameters are remains the same, it means the insider will be able to attack Ku and Chen's scheme by using the information $R_{new}$ and $f\,(b_{new} \oplus PW_{new})$, in the similar way as described in the earlier sub-section. Consequently the insider of *AS* is still able to attack the renewal password $PW_{new}$ of the user *U* in Ku and Chen's scheme.

## VI. CONCLUSION

This paper has analyzed the security lapses in Ku and Chen' s scheme and proved that the modified scheme of Ku and Chen is still vulnerable to the password guessing attack and the insider attack as well. Actually, the secret information, which is stored in the smart card of the user *U,* is responsible for the password guessing attacks and the registration phase is responsible for the insider attacks. As, we have seen that the modification of the scheme just consider the reparability of the attacks and repairs the scheme in the similar direction with same security parameters as it was with previous security parameters. Thus, the security pitfalls are still exists in Ku and Chen's scheme.

## REFERENCES

[1] C. C. Chang and K. F. Hwang, "Some forgery attack on a remote user authentication scheme using smart cards," *Infomatics,* vol. 14, no. 3, pp. 189 - 294, 2003.

[2] C. C. Chang and S. J. Hwang, "Using smart cards to authenticate remote passwords," *Computers and Mathematics with applications,* vol. 26, no. 7, pp. 19-27, 1993.

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

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

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

[6] C. J. Mitchell and l. Chen, "Comments on the S/KEY user authentication scheme," *ACM Operating System Review,* vol. 30, No. 4, pp. 12-16, Oct 1996.

[7] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electronic,* vol. 46, pp. 992-993, 2000.

[8] C. Mitchell, "Limitation of a challenge- response entity authentication," Electronic Letters*,* vol. 25, No.17, pp. 1195- 1196, Aug 1989.

[9] H. M. Sun, "An efficient remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electronic,* vol. 46, no. 4, pp. 958-961, Nov 2000.

[10] H. Y. Chien, J.K. Jan and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computer & Security,* vol. 21, no. 4, pp. 372-375, 2002.

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

[12] K. C. Leung, L. M. Cheng, A. S. Fong and C. K. Chen, "Cryptanalysis of a remote user authentication scheme using smart cards", *IEEE Trans. Consumer Electronic,* vol. 49, no. 3, pp. 1243-1245, Nov 2003.

[13] L. H. Li, I. C. Lin and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks," *IEEE Trans. Neural Networks,* vol. 12, no. 6, pp. 1498-1504, 2001.

[14] L. Lamport, "Password authentication with insecure communication," *communication of the ACM,* vol. 24, no. 11, pp. 770-772, 1981.

[15] M. Kumar, " New remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electronic,* vol. 50, no. 2, May 2004.

[16] M. Kumar, "Some remarks on a remote user authentication scheme using smart cards with forward secrecy." *IEEE Trans. Consumer Electronic,* vol. 50, no. 2, May 2004.

[17] M. S. Hwang, C. C. Lee and Y. L. Tang, "An improvement of SPLICE/AS in the WIDE against guessing attack," *International J. of In formatica,* vol. 12, no. 2, pp. 297-302, 2001.

[18] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electronic,* vol. 46, no. 1, pp. 28-30, Feb 2000.

[19] M. Udi, "A simple scheme to make passwords based on the one-way function much harder to crack," *Computer and Security,* vol. 15, no. 2, pp. 171 - 176, 1996.

[20] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," *Proc. Advances in Cryptography* (CRYPTO'99), pp. 388-397,1999.

[21] R. E. Lennon, S. M. Matyas and C. H. Mayer, "Cryptographic authentication of time-variant quantities." *IEEE Trans. on Commun.,COM*-29, no. 6 , pp. 773 - 777, 1981.

[22] S. M. Yen and K.H. Liao, "Shared authentication token secure against replay and weak key attack," *Information Processing Letters,* pp. 78-80,1997.

[23] T. C. Wu, "Remote login authentication scheme based on a geometric approach," *Computer Communication,* vol. 18, no. 12, pp. 959 - 963, 1995.

[24] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. on Information Theory,* vol. 31, No. 4, pp. 469-472, July 1985.

[25] T. Hwang and W.C. Ku, "Reparable key distribution protocols for internet environments," *IEEE Trans. Commun. ,* vol. 43, No. 5, pp. 1947-1950, May 1995.

[26] T. S. Messerges, E. A. Dabbish and R. H. Sloan, " Examining smart card security under the threat of power analysis attacks," *IEEE Trans. on Computers,* vol. 51, no. 5, pp. 541 –552, May 2002.

[27] W. C. Ku, C. M. Chen and H. L. Lee, " Cryptanalysis of a variant of Peyravian-Zunic's password authentication scheme," *IEICE Trans. Commun,* vol. E86- B, no. 5, pp. 1682 –1684, May 2002.

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

[29] Y. L. Tang, M. S. Hwang and C. C. Lee, "A simple remote user authentication scheme," *Mathematical and Computer Modeling,* vol. 36, pp. 103 - 107, 2002.

**Manoj Kumar** received the B.Sc. degree in mathematics, in 1993; the M. Sc. in Mathematics, in 1995; the M.Phil., in *Cryptography*, in 1997; submitted the Ph.D. thesis in *Cryptography*, in 2003. He also taught applied Mathematics at DAV College, Muzaffarnagar, India from Sep, 1999 to March, 2001; at S.D. College of Engineering & Technology, Muzaffarnagar, U.P., India from March, 2001 to Nov, 2001; at Hindustan College of Science & Technology, Farah, Mathura, continue since, Nov, 2001. He also passed the *National Eligibility Test* (NET), conducted by *Council of Scientific and Industrial Research* (CSIR), New Delhi- India, in 2000. He is a member of Indian Mathematical Society, Indian Society of Mathematics and Mathematical Science and Cryptography Research Society of India. His current research interests include Cryptography, Numerical analysis, Pure and Applied Mathematics.