A REMOTE LOGIN AUTHENTICATION SCHEME WITH SMART CARDS BASED ON UNIT SPHERE

MANOJ KUMAR

Department of Mathematics,
Rashtriya Kisan (Post Graduate) College Shamli,
Chaudhary Charan Singh University Meerut, Uttar Pradesh - India.

M. K. GUPTA

Department of Mathematics
Institute of Advances Studies
Chaudhary Charan Singh University Meerut, Uttar Pradesh - India.

SARU KUMARI

Department of Mathematics
Agra College, Agra
Dr. Bhim Rao Ambedkar University Agra, Uttar Pradesh - India.

Abstract

On the basis of the fact that points on a unit sphere are easy to compute but hard to derive, this paper presents a remote login authentication scheme with smart card based on unit sphere. The proposed scheme is simple, secure, efficient and achieves the other desired functionality. In our scheme, a verification table is not stored at the server to authenticate users. 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 the proposed scheme, the user selects his password himself freely at the time of registration and can also change his password anytime without connecting to the server. The proposed scheme also solves the serious time synchronization problem. The proposed scheme appeals for practical implementation as far as its achievements and resistance to various attacks are concerned.

Keywords: Remote login; network security; smart card; authentication; unit sphere; one- way hash function.

1. Introduction

Owing to the rapid development of computer and information technologies the control of the access to remote resources has become a crucial challenge. Generally, most of the resources available on the internet are not free but paid. So it is essential for the providers of services /facilities to allow the access of protected resources only to the legitimate user. Remote user authentication schemes are used to verify the legitimacy of remote user's login request. In 1981, Lamport proposed a remote user authentication scheme with password table [14] using a one way hash chain, which Haller used to design the famous S/key one time password system [9]. Since then many people have devoted themselves to the investigation field of remote user authentication schemes [3,4, 5].However, one weakness of schemes having a verification table maintained by the server in order to validate the legitimacy of the registered users is that if an attacker can some how break into the server, the table may be easily modified or corrupted [6]. Since then, many password authentication schemes have recognized this problem, and solutions using smart cards [2,7,11,17,19,20,21] and without smart cards [8,12,24] have been proposed, where a verification table is no longer required. Along with the creation of remote login authentication schemes, cryptanalysis [1,10,18,23,25,26] and further improvement [13,15,16,22,27] in them also goes side by side. In a typical smart card based password authentication schemes users are authenticated with their cards as identification tokens. The smart card takes as input a password from the user, creates a login message from the given password, and sends the message to a remote server, which then checks the validity of the login message before allowing access to any services or resources. This way the administrative overhead of the authentication server is reduced, and the user only needs to remember his password. Besides creating and sending login message, smart cards may also support mutual authentication, where a check-response interaction between the card and the server takes place to verify each other's identity. Rest of the paper is organized as follows: Section 2 is about the notations and descriptions. Section 3 presents the proposed scheme. Security of the proposed scheme is analyzed and discussed in section 4, and then achievements are focused by section 5. Finally some brief conclusion is given in section 6.

2. Notations

Table – 1: About notations and descriptions used throughout this paper

NOTATIONS	DESCRIPTION
U_i	The user
I_i	The identity of U_i
P_i	The password of U_i
R_i	Random value chosen by U_i
SC	The smart card
RS	The remote server
K	The long term secret key of RS
V	A secret number of RS
r_u	One time usable random value chosen by U_i
r_s	One time usable random value chosen by RS
S_y	The system
S	The sphere
$F(\cdot)$	A secure one-way hash function publicly known
$\Rightarrow$	The secure network
$\rightarrow$	The open network
$\oplus$	The XOR operation
$\|\|$	The Concatenation

3. The Proposed Scheme

This section introduces a remote user authentication scheme based on the concept of a unit sphere. The concept of a unit sphere enhances the security of the scheme by securing the user password. Consider a unit sphere S, say $x^2+y^2+z^2 = 1$ in the 3-D Geometry. Assume a point (x_1,y_1,z_1) lying outside the sphere S , then a directed line segment from the sphere centre (0,0,0) to the point (x_1,y_1,z_1) intersects the sphere at a point (x_2,y_2,z_2) where

$$x_2=\frac{x_1}{\sqrt{\left(x_1^2+y_1^2+z_1^2\right)}} \qquad (1)$$

$$y_2=\frac{y_1}{\sqrt{\left(x_1^2+y_1^2+z_1\right)}} \qquad (2)$$

$$z_2=\frac{z_1}{\sqrt{\left(x_1^2+y_1^2+z_1^2\right)}} \qquad (3)$$

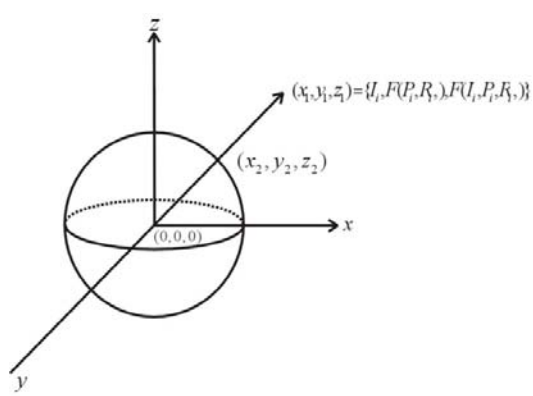

Fig: 2 A point (x_2,y_2,z_2) is located on the sphere.

3.1 Registration Phase

1_R : $U_i \Rightarrow$RS: $\{ x_1 = I_i , y_1 = F(P_i , R_i) , z_1 = F(I_i , P_i , R_i)\}$
For registration at the RS, U_i performs the following operations:

Step-1: Chooses his identity $x_1 = I_i > 1$, a random value R_i and a password P_i.
Step-2: Computes $y_1 = F(P_i, R_i)$ and $z_1 = F(I_i, P_i, R_i)$.
Step-3: Sends the registration request $\{x_1 = I_i, y_1 = F(P_i, R_i), z_1 = F(I_i, P_i, R_i)\}$ to the server through a secure network.

2_R : RS⇒ U_i: smart card containing $\{F(h_i) \oplus F(V \| I_i \| K), F(F(h_i), F(V \| I_i \| K)), F(\cdot)\}$.
On receiving the registration request $\{x_1 = I_i, y_1 = F(P_i, R_i), z_1 = F(I_i, P_i, R_i)\}$ remote server does the following :

Step-1: Computes
$$x_2^2 = \frac{x_1^2}{\left(x_1^2 + y_1^2 + z_1^2\right)} \quad (4)$$

Step-2: Modifies x_2^2 to remove the truncation error as
$$h_i = \frac{x_1^2}{2\log_2\left(x_1^2 + y_1^2 + z_1^2\right)} \quad (5)$$

Step-3: Computes $F(h_i) \oplus F(V \| I_i \| K)$ where V is a secret number and K is a long term secret key of the server.
Step-4: Computes $F(F(h_i), F(V \| I_i \| K))$
Step-5: Releases smart card containing $\{F(h_i) \oplus F(V \| I_i \| K), F(F(h_i), F(V \| I_i \| K)), F(\cdot)\}$ to the user.

3_R : U_i ⇒ SC: R_i i.e. smart card now contains $\{F(h_i) \oplus F(V \| I_i \| K), F(F(h_i), F(V \| I_i \| K)), R_i, F(\cdot)\}$ On receiving the smart card, U_i enters R_i into the smart card so that he need not remember R_i anymore. Thus the smart card is equipped with $\{F(h_i) \oplus F(V \| I_i \| K), F(F(h_i), F(V \| I_i \| K)), R_i, F(\cdot)\}$.

3.2 Login Phase

1_L : SC→ RS: $\{I_i, F(h_i) \oplus F(V \| I_i \| K), r_u \oplus F(V \| I_i \| K), F(r_u, F(h_i), F(V \| I_i \| K))\}$

Whenever U_i wants to login the RS, he inserts his smart card into a login device, enters his identity I_i & password P_i . Then the smart card does the following:

Step-1: Computes h_i and then $F(h_i)$.
Step-2: Retrieves $F(V \| I_i \| K)$ by computing $F(h_i) \oplus F(V \| I_i \| K) \oplus F(h_i)$.
Step-3: Computes $F(F(h_i), F(V \| I_i \| K))$.
Step-4: Compares the calculated and stored value $F(F(h_i), F(V \| I_i \| K))$, if not equal then the SC stops the proceedings, otherwise goes further.
Step-5: Chooses a random number r_u which is used only once.
Step-6: Computes $r_u \oplus F(V \| I_i \| K)$ and $F(r_u, F(h_i), F(V \| I_i \| K))$
Step-7: Sends $\{I_i, F(h_i) \oplus F(V \| I_i \| K), r_u \oplus F(V \| I_i \| K), F(r_u, F(h_i), F(V \| I_i \| K))\}$ to RS.

3.3 Authentication Phase

1_A : RS → SC: $\{r_s \oplus F(V \| I_i \| K), F(r_s, r_u)\}$
On receiving the login request $\{I_i, F(h_i) \oplus F(V \| I_i \| K), r_u \oplus F(V \| I_i \| K), F(r_u, F(h_i), F(V \| I_i \| K))\}$ RS performs the following:

Step-1: Computes $F(V \| I_i \| K)$.
Step-2: Retrieves $F(h_i)$ by computing $F(V \| I_i \| K) \oplus F(h_i) \oplus F(V \| I_i \| K)$.
Step-3: Retrieves r_u by computing $F(V \| I_i \| K) \oplus r_u \oplus F(V \| I_i \| K)$.
Step-4: Calculates $F(r_u, F(h_i), F(V \| I_i \| K))$ and compares it with the received one, if equal then proceeds further.
Step-5:Chooses a random number r_s which is used only once.
Step-6: Computes $r_s \oplus F(V \| I_i \| K)$ and $F(r_s, r_u)$.
Step-7: Sends $\{r_s \oplus F(V \| I_i \| K), F(r_s, r_u)\}$ to U_i .

2_A : SC → RS: $F(r_u, r_s)$ and U_i authenticates the RS

On receiving $\{r_s \oplus F(V \| I_i \| K), F(r_s, r_u)\}$ smart card performs the following:

Step-1: Retrieves r_s by computing $F(V \| I_i \| K) \oplus r_s \oplus F(V \| I_i \| K)$.
Step-2: Computes $F(r_s , r_u)$.
Step-3: Compares the calculated and received value $F(r_s , r_u)$, if not equal then the connection is terminated, otherwise the RS is authenticated successfully.
Step-4: Computes $F(r_u , r_s)$.
Step-5: Sends $F(r_u , r_s)$ to RS.

3_A : RS authenticates U_i

On receiving $F(r_u , r_s)$ RS performs the following :
Step-1: Computes $F(r_u , r_s)$.
Step-2: Compares the received and calculated value $F (r_u , r_s)$, if not equal connection is terminated, otherwise U_i is authenticated successfully and access to the RS is granted.
Step-3: Agreement of U_i and RS on session key $F (r_u , r_s , F(V \| I_i \| K))$.

3.4 Password Change Phase

1_p: When ever U_i wants to change his password, he inserts his smart card into the smart card reader of a terminal, enters I_i & P_i and requests to change the password, then the smart card performs the following:

Step-1:
Step-2: same as in 1_L
Step-3:
Step-4: Compares the calculated and stored value $F(F(h_i) , F(V \| I_i \| K))$, if not equal then the smart card rejects the password change request, otherwise U_i is authenticated successfully as the legitimate user and now U_i can enter P_i^*, the new password.

Step-5: Computes new h_i^* corresponding to new password P_i^*, computes $F(h_i^*)$, $F(h_i^*) \oplus F(V \| I_i \| K)$ and $F(F(h_i^*), F(V \| I_i \| K))$.

Step-6: Replaces old $F(h_i) \oplus F(V \| I_i \| K)$ and $F(F(h_i) , F(V \| I_i \| K))$ by the new $F(h_i^*) \oplus F(V \| I_i \| K)$ and $F(F(h_i^*) , F(V \| I_i \| K))$ respectively.

The password change phase is performed only with in the smart card of U_i , and U_i need not interact with RS.

4. Security Analysis

4.1 An Overview of Security

The proposed scheme is secure under the following:

- Fact that points on a unit sphere are easy to compute but hard to derive.
- Secure one way hash function.
- Well defined tamper resistant smart card device .
- One time usable random numbers.

Let us show how the above mentioned quartet provides strength to the proposed scheme:

- Mutual authentication between user and server is achieved by means of response messages. After the registration phase, server equips the smart card of the user with $F(h_i) \oplus F(V \| I_i \| K)$ which provides access of $F(V \| I_i \| K)$ to the user. Thus both user and server can authenticate each other.

The user has $\{ F(h_i) \oplus F(V \| I_i \| K), R_i \}$and remembers I_i & P_i . *Firstly* $\{ F(h_i) \oplus F(V \| I_i \| K) , R_i \}$ is assumed to be well protected in the tamper resistant smart card from extracting $F(h_i) \oplus F(V \| I_i \| K)$, *secondly* without knowing the correct $F(h_i)$, the value $F(V \| I_i \| K)$, cannot be extracted out from $F(h_i) \oplus F(V \| I_i \| K)$. *Thirdly* to know the correct $F(h_i)$, it is necessary to know the correct triplet (I_i , P_i , R_i) which is a very tedious job . Moreover Pi, & R_i are well secure under the one way property. Thus here occurs layered security i.e., one security feature is protected within another security feature.

In login phase user sends the message $(U_i \text{ to RS })_{1M} = \{ I_i , F(h_i) \oplus F(V \| I_i \| K) , r_u \oplus F(V \| I_i \| K)\}, F(r_u , F(h_i) , F(V \| I_i \| K))\}$ to the server. In authentication phase since server can compute $F(V \| I_i \| K)$ using his long term secret key K, and secret number V to extract $F(h_i)$ from the sent message, he can compute the response message $(RS \text{ to } U_i)_M =\{ r_s \oplus F(V \| I_i \| K) , F(r_s , r_u)\}$ and sends to the user. On receiving the response message(RS to U_i $)_M$, user authenticates the server and computes the response message (U_i to RS$)_{2M}$ = F(r_u , r_s) and sends to the server. Lastly the server authenticates the user using (U_i to RS $)_{2M}$.

- In the proposed scheme an attacker can be successful in two ways:

Way 1:Either he acts as a legitimate user to login.
Way 2:Or he acts as a normal server to cheat the user.

Let us show how both the ways are infeasible in the proposed scheme.

It has been shown that F(V || I_i || K) along with F(h_i) are key factors to security. It is F(V || I_i || K) and F(h_i) which enables the proposed scheme to achieve mutual authentication.

Infeasibility of way 1**:** Without being able to extract F(V || I_i || K) (which is possible if the correct value of F(h_i), be calculated) an attacker pretending to be a legitimate user cannot calculate the valid message

(U_i to RS $)_{1M}$ = { I_i , F(h_i) ⊕ F(V || I_i || K) , r_u ⊕ F(V || I_i || K) , F(r_u , F(h_i) , F(V || I_i || K))} in step 1_L and response message (U_i to RS $)_{2M}$ = F(r_u , r_s) in step 2_A.

Infeasibility of way 2**:** Without being able to calculate F(V || I_i || K) an attacker pretending to be a normal server cannot forge a valid response message (RS to $U_i)_M$ = ={ r_s ⊕ F(V || I_i || K) , F(r_s , r_u) } to convince legitimate user.

- Moreover, without knowing one time usable random numbers r_u and r_s , it is senseless to think of obtaining F(V || I_i || K) or F(h_i), from any of the intercepted messages r_u ⊕ F(V || I_i || K) or r_s ⊕ F(V || I_i || K).

4.2 Analytic Discussion on Possible Attacks

4.2.1 Replay attacks: The replay attacks cannot work on the proposed scheme because of the renewal of r_s and r_u for each new login . Replaying neither the login message { I_i , F(h_i) ⊕ F(V || I_i || K) , r_u ⊕ F(V || I_i || K)}, F(r_u , F(h_i) , F(V || I_i || K))} in the login phase nor the response message { r_s ⊕ F(V || I_i || K) , F(r_s , r_u)} in the authentication phase will be success, as the validity in both the cases can be checked with the random numbers r_u and r_s. Even if an attacker intercepts the login request and replays it to fool the remote server , he fails in step-1 of authentication phase 2_A because only the legal user can retrieve r_s. Again if an attacker intercepts the response message { r_s ⊕ F(V || I_i || K) , F(r_s , r_u) } and replays it to fool the user, he fails in step-3 of authentication phase 2_A as the received and calculated values of F(r_s , r_u) will be different from each other due to one time usability of r_u .

4.2.2 Stolen verifier attack: Since the server neither maintains any verification table nor stores any entry in its database, so no question arises for an attacker to make a way inside the scheme with the help of the stolen verifier attack.

4.2.3 Forged user attack: To act as a legal user an attacker must be able to send a valid login request so as to pass the authentication phase .Without knowing F(h_i) & consequently not being able to calculate F(V || I_i || K) an attacker cannot compute a valid login request. Moreover, if the attacker forges/modifies the login request by XORing or appending some value to r_u ⊕ F(V || I_i || K) or to F(h_i) ⊕ F(V || I_i || K) this effort goes waste in step-4 of authentication phase 1_A when the received and the calculated value of F(r_u , F(h_i) , F(V || I_i || K)) are different from each other.

4.2.4. Forged server attack: To act as a successful remote server, an attacker must be able to send a valid response message in 1_A. But due to lack of access to F(V || I_i || K) the attacker is not able to compute a valid response message**.** Also, if the attacker forges/modifies the valid response massage by XORing or appending some value to r_s ⊕ F(V || I_i || K), this exercise proves to be a nonsense in step-3 of authentication phase 2_A as the received and calculated value of F(r_s, r_u) is different from one another .

4.2.5. Cut-paste attacks: This attack is quite similar to message modification attack**.** In this type of attack attacker replaces a portion of the valid massage by a different portion that seems quite similar to the replaced one. Here the three massages { I_i , F(h_i) ⊕ F(V || I_i || K) , r_u ⊕ F(V || I_i || K) , F(r_u , F(h_i) , F(V || I_i || K))} , { r_s ⊕ F(V || I_i || K) , F(r_s , r_u)} and F(r_u , r_s) traveling through open network, depend either on r_u or on r_s or on both .Thus the possibility of any such attack is ruled out.

4.2.6. Stolen smart card attack: Even if an attacker happens to steal the smart card of the legal user, he cannot access the facilities provided by the remote server. The reason being the inability of attacker to extract $F(V \| I_i \| K)$ from the smart card in the absence of the correct triplet (I_i, P_i, R_i) & hence of $F(h_i)$.

4.2.7. Remote server's secret key loss attack: Server's secret key is protected under the one way property so this attack is useless.

4.2.8. Insider attack: U_i registers to RS by submitting $\{x_1 = I_i, y_1 = F(P_i, R_i), z_1 = F(I_i, P_i, R_i)\}$ instead of P_i, so the insider of RS cannot directly obtain P_i. Besides, as R_i is not revealed to RS, the insider of RS cannot obtain P_i by performing an off-line guessing attack either on $y_1 = F(P_i, R_i)$ or on $Z_1 = F(I_i, P_i, R_i)$.

4.2.9. Password guessing attack: Of all the messages traveling via open network only $F(h_i) \oplus F(V \| I_i \| K)$ has contribution of password in it**.** And from $F(h_i) \oplus F(V \| I_i \| K)$ password guessing is very far away from possible, first because of inaccessibility of $F(h_i)$ without knowing $F(V \| I_i \| K)$ and second because of the construction of $F(h_i)$.

4.2.10. Denial of service attack: The possibility of this attack is ruled out because the password change phase involves no communication with the remote server**.**

5. Achievements of the Proposed Scheme

5.1 Mutual Authentication: Login user is authenticated at two stages, *first* in step-4 of authentication phase 1_A by checking if the received $F(r_u, F(h_i), F(V \| I_i \| K))$ is equal to the computed one; and *second* in step-4 of authentication phase 3_A by checking if the received $F(r_u, r_s)$ is equal to the calculated one. *First* aims to check if the user knows the common secret $F(V \| I_i \| K)$**.** But the login massage can be replayed by an attacker. Thus *second* is invoked to rule out the possibility of replay attacks by using one time usable r_s by the RS. Also the RS is authenticated by checking if the received $F(r_s, r_u)$ is equal to the calculated one. It aims to check if the RS possess the secret key K and the secret number V to generate $F(V \| I_i \| K)$ to retrieve r_u in step-3 of the authentication phase 1_A and compute the response message $(\text{RS to } U_i)_M = \{r_s \oplus F(V \| I_i \| K), F(r_s, r_u)\}$**.** Thus the proposed scheme achieves mutual authentication.

5.2 Fast wrong password detection: If U_i enters the wrong password by mistake or if an attacker possessing the I_i & the smart card of U_i tries to login by inserting a wrong password, this wrong password is quickly detected by the smart card in step-4 of login phase 1_L comparing the calculated and stored value of $F(F(h_i), F(V \| I_i \| K))$.

5.3 Secure password change: Since the smart card can verify the correctness of P_i by comparing the calculated and stored value of $F(F(h_i), F(V \| I_i \| K))$, in step-4 of password change phase 1_P, therefore when the smart card is lost/stolen, unauthorized users cannot change the password of the card. Also the password change phase involves no communication through the open network hence the password change phase is secure**.**

5.4 Server's ignorance of user's password: A user may have the same password used for various network services on different servers**.** If the server knows the user's password, it can gain by impersonating a legal user , especially in the sensitive application of network banking. In the proposed scheme U_i sends $\{x_1 = I_i, y_1 = F(P_i, R_i), z_1 = F(I_i, P_i, R_i)\}$ to the server , in which without knowing R_i the server has no way to obtain or guess P_i

5.5 Computational cheapness: The proposed scheme is based on one-way hash functions, and other then one-way hash function it uses XOR and concatenation. It involves none of the three ; public key cryptosystem, modular exponential operation or symmetric en (de) cryption The computation of equation (5)

$$h_i = \frac{X_1^2}{2\log_2\left(x_1^2 + y_1^2 + z_1^2\right)}$$

is done once by the user and once by the server in login phase and registration phase respectively.

5.6 Easy password change: It is because the password change phase involves no communication with the RS, the entire phase is done between user and his smart card .

5.7 Forward secrecy : If remote server's secret key K is revealed accidentally, even then an attacker cannot compute the common secret $F(V \| I_i \| K)$ between user and server and the verifying factor $F(r_u, F(h_i), F(V \| I_i \| K))$, as he does not know the secret number V of the server, user's one time usable random number r_u and user's hash value $F(h_i)$**.** Therefore, an attacker cannot impersonate a legal user using the revealed key K.

6. Conclusion

In this paper, the authors propose a new remote user authentication scheme which is based on a unit sphere**.** The proposed scheme achieves mutual authentication between the remote server and the user such that the forged server attack has no effect on it**.** Except this, the scheme provides freedom to the user to choose and change password at will and maintains distance from various attacks including replay attack without involving any complex mechanism. Besides**,** its low computational cost and simplicity increases its suitability for practical approach**.** Briefly the proposed scheme can be marked as a simple, efficient, secure, user-friendly and practically applicable in the field of remote user authentication with smart card**.**

References

[1] Chan C.K., Cheng L.M., "Cryptanalysis of a remote user authentication scheme using smart cards", IEEE *Transaction on consumer Electronics* 46 (4) (2000) 992-993.
[2] Chang C.C., Hwang K.F., "Some forgery attacks on a remote user authentication scheme using smart cards", *Informatica* 14 (3) (2003) 289-294.
[3] Chang C.C, Hwang S.J., "Using smart cards to authenticate remote passwords", *Computer Maths Appl,* 26 (7): 19 – 27 (1993).
[4] Chang C.C., Liao W.Y., "A remote password authentication scheme based upon ElGamal's signature scheme", *Computer Security*; 13(2): 137-144 (1994).
[5] Chang C.C., Wu T.C., "Remote password authentication with smart cards"*, IEE Proceedings –E 138*, no-3:165 – 168 (1991).
[6] Chen C.M., Ku W.C., "Stolen verifier attack on two new strong- password authentication protocol", *IEICE Transactions on communications* E85 – B(11), 2519 – 2521 (2002).
[7] Chien H.Y., *et al.* "An efficient and practical solution to remote authentication: smart card," *Computer and Security* 21(4) (2002) 372-375.
[8] Fan L., *et al.* "An enhancement of timestamp-based password authentication scheme", *Computers and Security* 21 (7) (2002) 665-667.
[9] Haller N.M., "The S/ key (TM) one time password system"*, In: Proceedings of the Internet society Symposium on network and distributed system security:P* – 151 – 157 (1994).
[10] Hsu C.L., "Security of Chien et al's remote user authentication scheme using smart cards", *Computer Standards and Interfaces* 26 (3) (2004) 167-169.
[11] Hwang M.S., Li L.H., "A new remote user authentication scheme using smart card", *IEEE Transactions on Consumer Electronics* 46 (1) (2000) 28-30.
[12] Hwang T., *et al.* "Non –interactive password authentication without password tables",*Proc. IEEE Region* 10 *Conference on Computer and Communication System, Hong Kong, Sept.* 1990, pp. 429-431.
[13] Ku. W.C., Chen S.M., "Weakness and improvements of an efficient password based remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics* 50 (1) (2004) 204-207.
[14] Lamport L., "Password authentication with insecure communication"*, communication of the ACM* 24 (1981).
[15] Lee N.Y., Chiu Y.C., "Improved remote authentication scheme with smart card", *Computer Standards and Interfaces* 27 (2005) 177-180.
[16] Lee S.W., *et al.* "Improvement of Chien et al's remote user authentication scheme using smart cards", *Computer Standards and Interfaces* 27 (2005) 181-183.
[17] Liu J.Y., *et al.* "A new mutual authentication scheme based on nonce and smart cards", *Computer Communication* 31 (2008) 2205-2209.
[18] Shen J.J., *et al.* "Security enhancement for the timestamp-based password authentication scheme using smart cards ", *Computers and Security* 22(7) (2003) 591-595.
[19] Sun H.M., "An efficient remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronic* 46 (4) (2000) 958-961.
[20] Tsai J.L., "Efficient multi-server authentication scheme based on one way hash function without verification table", *Computer and Security* 27 (3-4) (2008) 115-121.
[21] Wang M., *et al.* "Remote password authentication scheme based on smartcard ", *Computer Applications* 25 (10) (2005) 2289-2290.
[22] Wang X.M., *et al.* "Cryptanalysis and improvement on two efficient remote user authentication scheme using cards", *Computer Standards and Interfaces* 29 (5) (2007) 507-512.
[23] Wang Y.J., Li J.H., "Security improvement on a timestamp-based password authentication scheme", *IEEE Transactions on consumer Electronics* 50 (2) (2004) 580-582.
[24] Yamaguchi S., *et al.* "Design and implementation of an authentication system in WIDE internet environment"*, In : Proceedings of the 10th IEEE Regional Confrence on Computers and Communication Systems* (Hong Kong, 24 -27 September 1990) P. 653 – 657 (1990).
[25] Yeh H.T., *et al.* "Security of a remote user authentication scheme using smart cards", *IEICE Transactions on communications* E87-B (1) (2004) 192-194.
[26] Yoon E.J., *et al.* "Attacks on the Shen et al's timestamp-based password authentication scheme using smart cards ", *IEICE Transactions on Fundamentals* E88-A (1) (2005) 319-321.
[27] Yoon E.J., *et al.* "Further improvement of an efficient password based remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics* 50 (2) (2004) 612-614.