A New Remote User Authentication Scheme Using Smart Cards with Forward Secrecy

Manoj Kumar

Abstract – *Hwang and Li proposed the first remote user authentication scheme using smart cards to solve the problems of Lamport scheme. Unfortunately, Hwang and Li's scheme has some security weaknesses. First, Chan- Chang, Shen- Lin- Hwang and then Chang-Hwang pointed out some attacks on Hwang – Li's scheme. This paper presents a new remote user authentication scheme with forward secrecy, which provides forward secrecy to the long term secret key of the authentication server. This scheme is also secure against Chan – Cheng and all the extended attacks*[1].

Index Terms — Cryptography, Remote user authentication, Authentication server, Smart card, Password, Cryptanalysis, Network security, Check digit, Forward secrecy

I. INTRODUCTION

PASSWORD based remote user authentication schemes are used to check the validity of a login request made by a remote user *U* to gain the access rights on an *authentication server* **(*AS*).** In these schemes, the *AS* and the remote user *U* share a secret, which is often called as password. With the knowledge of this password, the remote user *U* uses it to create a valid login request to the *AS***.** To provide the access rights to the user *U*, *AS* checks the validity of the login request. 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]-[4]-[5]-[6]-[7]-[11]-[12]-[18]-[20]-[21]-[23]-[24]-[31] have been proposed.

Lamport [21] proposed the first well-known remote password authentication scheme using smart cards. In Lamport's scheme, the *AS* stores a password table at the server to check the validity of the login request made by the user. However, high hash overhead and the necessity for password resetting decreases the suitability and practical ability of Lamport's scheme. In addition, the Lamport scheme is vulnerable to a small *n* attack [8]. Since then, many similar schemes [26]-[29] 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 braked/affected.

In 2000, Hwang and Li [23] pointed that Lamport's scheme suffers from the risk of a modified password table and the cost of protecting and maintaining the password table. Further, they proposed a new remote user authentication scheme using smart cards. This scheme does not maintain the password table to check the validity of the login request. Also, it can withstand message-replaying attack.

In [9], Chan and Cheng pointed out an attack on the Hwang-Li's scheme. In 2003, Shen-Lin- Hwang [18] discussed a different attack on the Hwang-Li's scheme and they also proposed a modified scheme to prevent the attacks on Hwang-Li's scheme. In the same year, Chang and Hwang [3] explained the practical problems of the Chan – Cheng's attack on the Hwang-Li's scheme and Leung, - Cheng, - Fong and Chen [19] pointed out that the Shen-Lin-Hwang's scheme is still vulnerable to the attack proposed by Chan and Cheng. Awasthi and Lal [2] pointed a different type of attack on Hwang-Li's scheme and they also introduced a remote user authentication scheme. Awasthi and Lal claimed that their scheme provides forward secrecy [1] - [38] to the *AS.* In 2004, Kumar [22] analyzed the practical pitfalls of Awasthi and Lal's scheme. Kumar also pointed out the security pitfalls of Awasthi and Lal's scheme. In the same year, Lee et al. [30] raised a question on the correctness of Awasthi and Lal's scheme. Lee et al. also proved that Awasthi and Lal's scheme is incorrect and does not provide the forward secrecy to the secret key of the *AS.*

Contributions

This paper proposes a new remote user authentication scheme with forward secrecy. Our scheme provides forward secrecy with respect to the secret key of the long - term secret key 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. Our scheme is also removes the security pitfalls of Hwang and Li's scheme.

Organization

Section II reviews the Hwang – Li's scheme [23]. Section III describes the cryptanalysis of Hwang – Li's scheme. Section IV reviews Shen-Lin- Hwang's scheme [18]. Section V describes the cryptanalysis of Shen-Lin- Hwang's scheme. Section VI reviews the Awasthi and Lal's scheme [2]. The security pitfalls and the comments on Awasthi and Lal's scheme are described in the section VII. Section VIII presents a new remote user authentication scheme with forward secrecy. The security of the new scheme is analyzed in section IX. Finally, comes to a conclusion in the section X.

II. REVIEW OF HWANG-LI'S SCHEME

There are three phases in the Hwang-Li's scheme**:** the registration phase, login phase and the authentication phase. In the registration phase, the user *U* sends a request to the *AS* for the registration. The *AS* will issue a smart card and a password to every user legal through a secure channel. In the

[1] Manoj Kumar is with the Department of Applied Sciences and Humanities, Sharda Group of Institutions (*SGI*), Jawahar Nagar, Khandri, Agra, India - 282004, (e-mail: Balyanyamu@rediffmail.com, Chayayamu@yahoo.co.in)

login Phase, when 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 and the password to access services. In the authentication phase, the *AS* checks the validity of the login request.

A. Registration Phase

A user U submits her/his ID to the *AS*. *AS* computes the password PW for the user U, as,

$$PW = ID^{x_s} \bmod p,$$

where, x_s is a secret key maintained by the *AS* and p is a large prime number. *AS* provides a password PW and a smart card to the user U through a secure channel. The smart card contains the public parameters (f, p), where f a one-way function

B. Login Phase

User U attaches her/his smart card to the smart card reader and keys ID and PW. The smart card will perform the following operations:

1. Generate a random number r.
2. Compute $C_1 = ID^r \bmod p$.
3. Compute $t = f(T \oplus PW) \bmod p - 1$, where T is the current date and time of the smart card reader.
4. Compute $M = ID^t \bmod p$.
5. Compute $C_2 = M(PW)^r \bmod p$.
6. Sends a login request $C = (ID, C_1, C_2, T)$ to the *AS*.

C. Authentication Phase

Assume *AS* receives the message C at time T_c, where T_c is the current date and time at *AS*. Then the *AS* takes the following actions:

1. Check the format of ID**.** If the identity format is not correct, then *AS* will rejects this login request.
2. Check, whether $T_c - T \le \Delta T$, where ΔT is the legal time interval due to transmission delay, if not, then rejects the login request C.
3. Check, if $C_2 (C_1^{x_s})^{-1} \stackrel{?}{=} (ID)^{f(T \oplus PW)} \bmod p$, then the *AS* accepts the login request. Otherwise, the login request will be rejected.

III. Cryptanalysis of the Hwang- Li Scheme

A. Chan and Cheng's Attack

According to Chan and Cheng [9], a legal user Alice can easily generate a valid pair of identity and password without knowledge of the secrete key 'x_s' of *AS*. Alice uses her valid pair (ID_A,PW_A) to generate another valid pair (ID_B, PW_B) as follows:

Alice computes $ID_B = (ID_A \times ID_A) \bmod p$. Then, she can computes the corresponding password

$$\begin{aligned} PW_B &= ID_B^{x_s} \bmod p \\ &= (ID_A \times ID_A)^{x_s} \bmod p \\ &= (PW_A \times PW_A) \bmod p \end{aligned}$$

As a result, Alice can generate a valid pair (ID_B ,PW_B) without knowing the secret key x_s.

B. Shen-Lin-Hwang's Attack: Masquerading Attack

According to Shen, Lin and Hwang [18] masquerading attack is possible on Hwang- Li's scheme. A user Bob can masquerade another user Alice to login a remote server and gain access right. Bob computes an identity $ID_B = ID_A^k \bmod p$, where k is a random number such that $gcd(k, p) = 1$.Then, he submits this identity ID_B to *AS* for registration. *AS* provides a smart card and a password

$$PW_B = ID_B^{x_s} \bmod p.$$

With the knowledge of PW_B, Bob can compute

$$PW_A = ID_A^{x_s} \bmod p = PW_B^{-k} \bmod p.$$

As a result, Bob can masquerade as Alice to login a remote server and gain access privilege.

C. Chang- Hwang's Attack

According to Chang and Hwang [3], there is a mistake in the Chan- Cheng's attack. It is not always possible that the square of a legal identity satisfies the specific identity format. Chang and Hwang generalized the Chan- Cheng's attack. They described two attacks.

Attack- I

Alice computes $ID_B = ID_A^k \bmod p$, where k is a random number. Then, he can compute the corresponding password

$$PW_B = PW_A^k \bmod p.$$

As a result, a legal user Alice can impersonate other user Bob with a valid pair of (ID_B, PW_B) to login the AS. If ID_A is a primitive root of Zp, then all the valid identities and their corresponding password can be generated easily.

Attack- II

A group of eavesdroppers (intruders) may cooperate to generate a valid pair of identity (ID_G, PW_G), as follows:

$$ID_G = \prod ID_{Aj} \bmod p \text{ and } PW_G = \prod PW_{Aj} \bmod p$$

Chang and Hwang pointed out that in Hwang – Li's scheme, it is still difficult to obtain the corresponding password for a known arbitrary valid identity, but once the valid identity is generated, its corresponding password will be obtained easily.

IV. Shen, Lin and Hwang's scheme

Shen-Lin-Hwang [18] proposed a modified remote user authentication scheme to solve the security pitfalls of the Hwang-Li's scheme. Shen-Lin-Hwang's scheme uses the concept of hiding the identity to prevent the masquerading attack. They modified the registration phase, now a shadow identity SID will be issued to the legal user. This modified in the registration phase is described below.

Modified Registration Phase

A user U submits her/his identity string J to the *AS* for the registration. The string J contains the name, address, unique number etc. This information in the string J is unique for every user. Then the *AS* computes a pair (SID, PW) for the user U after the identity J is identified. The pair (SID, PW) is computed as follows:

$$SID = Red(J) \text{ and } PW = (SID)^{x_s} \bmod p$$

where, *Red* (.) is a shadow identity of device which is only maintained in the remote server and S_{ID} is the shadow identity of the user *U*. Furthermore, the *AS* distributes the smart card and (*SID, PW*) to the user *U* in a secure way. The smart card contains the public parameters (*f*, *p*).

In this scheme, the message sent to the *AS* now contains (*SID*, C_1, C_2, *T*). Because J_i specially formatted, the evil user cannot compute new identity string J_i via SID_i.

V. CRYPTANALYSIS OF THE SHEN, LIN AND HWANG'S SCHEME

A. Leung- Cheng-Fong –Chan's Attack

According to Leung-Cheng-Fong-Chan [19], Shen-Lin-Hwang's scheme [18] defends the attacks of registration for a new identity ID_B via ID_A for a legal user Alice. They also pointed out that the modified scheme is still vulnerable to the attack described by Chan and Cheng. They showed that the modified scheme is not secure against the attack that is similar to Chan - Cheng and Chang – Hwang's attacks. If we replace ID_A with SID_A, then the Chang and Hwang's attack will work as follows.

Alice computes $SID_B = (SID_A)^k \bmod p$, where *k* is a random number. Then, he can compute the corresponding password

$$PW_B = PW_A{}^k \bmod p.$$

As a result, a legal user Alice can impersonate other user Bob with a valid pair of (SID_B, PW_B) to login the AS. If SID_A is a primitive root of *Zp*, then all the valid identities and their corresponding password can be generated easily. Since, Chan – Cheng's attack is one case of this attack so it also works well.

VI. REVIEW OF AWASTHI - LAL 'S SCHEME

Awasthi – Lal introduced a new type attack on Hwang – Li's scheme. They are of the opinion that if a malicious attacker Bob has stolen the system's secret key x_s, then he can compute each user's password as $PW = ID^{x_s} \bmod p$. Now to stop Bob from doing destructive activity, it is must to replace the system's secret key x_s with X_s and re-compute all passwords by using changed secret key X_s. However, it would be much expensive to communicate these passwords to all users.

To overcome this difficulty of Hwang and Li's scheme, Awasthi and Lal modified the registration phase of Hwang - Li's scheme and proposed a new scheme, which avoids change in previous passwords.

Awasthi and Lal's scheme has four phases: Initial, Registration, Login and Authentication as described below.

A. Initial Phase

The AS generates the following system parameters:

p: a large prime number.

x_s: a secret key of the system.

f (.): a public one-way function.

Besides these parameters *TSA* is a trusted time stamping authority that provide current time stamp whenever required.

B. Registration Phase

A user *U* submits her/his *ID* to the *AS*. First, the *AS* computes $m = h(ID \oplus T)$, where *T* is time stamp provided by *TSA* and then the password *PW* for the user *U, as*,

$$PW = m^{x_s} \bmod p.$$

AS provides a password *PW* and a smart card to the user *U* through a secure channel. The smart card contains the parameters (*f*, *p, T*).

C. Login Phase

User *U* attaches her/his smart card to the smart card reader and keys *ID* and *PW*. The smart card will perform the following operation:

1. Generate a random number *r*.
2. Compute $m = f(ID \oplus T)$.
3. Compute $C_1 = m^r \bmod p$.
4. Compute $t = f(T_c \oplus PW) \bmod p - 1$, where T_c is the current date and time of the smart card reader.
5. Compute $M = ID^t \bmod p$.
6. Compute $C_2 = M (PW)^r \bmod p$.
7. Sends a login request $C = (ID, C_1, C_2, T_c)$ to the *AS*.

D. Authentication Phase

Assume *AS* receives the message *C* at time T^{Θ}, where T^{Θ} is the current date and time at *AS*. Then the *AS* takes the following action:

1. Check the format of *ID***.** If the identity format is not correct, then *AS* will rejects this login request.
2. Check, whether $T_c - T^{\Theta} \le \Delta T$, where ΔT is the legal time interval due to transmission delay, if not, then rejects the login request C.
3. Check, if $C_2 (C_1^{x_s})^{-1} = (ID)^{h(Tc \oplus PW)} \bmod p$, then the *AS* accepts the login request. Otherwise, the login request will be rejected.

VI. SECURITY ANALYSIS OF AWASTHI - LAL'S SCHEME

A. Kumar's Attacks

Awasthi and Lal have claimed that with the reveled secret key x_s, any attacker, Bob cannot obtain the passwords corresponding to the previously registered identities. Kumar [22] pointed out the security weaknesses of Awasthi and Lal's scheme and then proved that Awasthi and Lal's scheme does not provide forward security to the *AS*. The following discussion proves that the Awasthi and Lal's scheme is vulnerable to a destructive attack by Bob.

Take the following three conditions into consideration:

- Since the attacker, Bob is in possession of the secret key x_s of the *AS*.
- The *AS* does not retain the records of the registered identities and their corresponding passwords.
- A remote password authentication is used to authenticate the legitimacy of the remote users over an insecure channel.

The malicious user Bob utilized these three conditions and he can send a valid login request to the *AS*. Bob can login to

the *AS* by having a valid pair of (ID_B, PW_B). The description of this attack is given below.

A. Attack Via the Previously Registered ID

Because the attacker Bob is in the possession of the secret key x_s, hence by intercepting a valid login request $C = (ID, C_1, C_2, T_c)$ emitted from the user *U*, a malicious intruder (attacker) Bob can construct another login request L_B such that L_B passes the authentication phase. The *AS* cannot distinguish between the authentic login request *C* and the fabricated login request L_B. The following discussion show how to do that.

1. Chooses a random number r^* and a timestamp T_B^*.
2. Compute $m^* = f(ID \oplus T_B)$.
3. Compute $PW^* = (m^*)^{x_s} \bmod p$.
4. Compute $C_1^* = m^{*r^*} \bmod p$.
5. Compute $t^* = f(T^*_c \oplus PW^*) \bmod p - 1$, whenever the attacker wants to gain the access right at a time T^*_c.
6. Compute $M^* = ID^{t^*} \bmod p$.
7. Compute $C_2^* = M^* (PW^*)^{r^*} \bmod p$.
8. The attacker Bob delivers the fabricated login request $L_B = (ID, C_1^*, C_2^*, T^*_c)$ to the to *AS*.

After receiving the login request $L_B = (ID, C_1^*, C_2^*, T^*_c)$ at time T^{Θ}, the *AS* will authenticate the adversary as a legal user and grant the access right to him. The success of the authentication phase is shown below.

1. The identity format will be correct since the attacker has been used a previously used identity *ID*.
2. The transmission delay $T^*_c - T^{\Theta}$ will be less than the legal time interval ΔT, since the attacker selects the appropriate time T^*_{cc} to gain the access right.
3. Obviously the verification equation
$$C_2^* (C_1^{*x_s})^{-1} = (ID)^{h(T^*c \oplus PW^*)} \bmod p,$$
holds true.

In this way, the *AS* accepts the fabricated login request L_B. Thus, the intruder Bob can impersonate a valid user, who holds a valid pair of the identity *ID* and the password *PW*.

B. Attack Via a New ID

The intruder is able to attack via a new identity. He chooses a valid identity format and performs all the steps as described above.

By above discussion, it is clear that Awasthi and Lal's scheme does not provide forward security to the *AS*.

B. Lee et al. Comment

Lee et al. [30] pointed out that Awasthi and Lal's scheme is incorrect. In the authentication phase, the system has not sufficient information to validate the login request, which is made by the remote user *U* in the login phase. In Awasthi and Lal's scheme, after receiving the login request $C = (ID, C_1, C_2, T_c)$ from the user *U,* the *AS* Check, if

$$C_2 (C_1^{x_s})^{-1} = (ID)^{h(Tc \oplus PW)} \bmod p, \quad \ldots\ldots(1)$$

then the *AS* accepts the login request. Otherwise, the login request will be rejected.

However, the *AS* cannot validate the above congruence because there is no way for the *AS* to compute the password *PW* of the user *U.* At the time of registration, the *AS* computes the password $PW = m^{x_s} \bmod p$, where $m = h(ID \oplus T)$ and T is time stamp. The value T is stored in the smart cards, but it is not provide to the *AS* to verify the validity of the congruence (1).

Lee et al. also pointed out that there is no secure way to provide the value T to the *AS.* Once this value T is revealed, then a malicious attacker Bob with the knowledge of secret key x_s and T can easily compute the corresponding password of the user *U*. The attacker is also free to construct any fabricated login request and then he will be able to gain all the access right at the *AS,* as a valid user. Thus, again it is clear that Awasthi and Lal's scheme does not provide forward security to the *AS.*

VIII. Our Contribution

New Remote User Authentication Scheme Using Smart Cards With Forward Secrecy

Since, the secret key of the *AS* is a *long-term key*. It means it 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 the corresponding passwords.*

On the other end, the Hwang and Li's scheme [12] has two categories of security attacks. The first category of attacks is attack by a malicious Bob, which is not registered user at the *AS*: *Shen- Lin- Hwang's attack* and the second category of attacks is attack by a malicious user Alice, which is already registered at the *AS*: Chan- *Cheng's attack and Chang-Hwang's Attack.* This section also provides a solution to prevent these security weaknesses.

This section presents a new remote user authentication scheme using smart cards with forward secrecy. 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. Additionally, our scheme is secure against all types of attacks.

This scheme has four phases: initial phase, registration phase, login phase and verification phase. These phases are described below.

A. Initialization Phase

For our requirement, we have modified the registration phase of Hwang and Li's scheme. This scheme uses two more functions: redirected function *Red* (.) to redirect the registered identity *ID* and a check digit function C_K (.) to generates the corresponding check digit [13]-[14]-[15]-[16]-[17]-[36] for each registered identity. In this scheme, only the *AS* can redirect the registered identity *ID* only he is able to generate a

valid identity and the corresponding *check digit*.

The notations used through out in our scheme can be summarized as follows:

- U denotes the *remote user*.
- ID denotes the *identity* of the remote user U.
- PW denotes the *password* corresponding to the registered identity ID.
- AS denotes the *authentication server*.
- x_s denotes the *permanent secret key* of the authentication server.
- $f(.)$ denotes a cryptographic *one way hash function*.
- $\leftrightarrow$ denotes a *secret channel* between the remote user U and the authentication server AS.
- $\rightarrow$ denotes a *public channel* (*insecure channel)* between the remote user U and the authentication server AS.
- p denotes a *large prime number*.
- S_{ID} denotes the redirected identity corresponding to a registered identity ID.
- C_{ID} denotes the check digit corresponding to a registered identity ID.

In addition to these parameters the AS generates the following parameters

- Red (.) denotes a function to redirect the identity ID for every user U, which is only possessed with the AS.
- C_K(.) denotes a function to generate *check digit* for the registered identity, which is only possessed with the AS.

B. Registration Phase

This phase is executed over a secure channel. The following steps are involved in this phase.

Step R1. $U \leftrightarrow AS$: J

The string J consists the name of the user U, address, identity ID and a unique identification number etc, which are unique for the user U.

Step R2. AS computes the followings:

$S_{ID} = Red(ID)$, $C_{ID} = C_K(S_{ID})$ and $PW = (S_{ID})^{x_s} \bmod p$.

Step R3. $AS \leftrightarrow U$: a smart card containing the public parameters (f, p) and a pair ($C_{ID} \| ID$, $S_{ID} \| PW$) to the user U.

In this scheme, the identity and the password of the user have two sub-parts. Now after the registration, the identity $C_{ID} \| ID$ of the user U is called as *balyan identity* and the password $S_{ID} \| PW$ is called as *balyan password*.

C. Login Phase

Whenever, the user wants to gain the access right on the AS, then the following steps are involved for the proper execution of this phase.

Step L1. U attaches her/his smart card to the smart card reader at any time T and keys her/his *balyan identity* $C_{ID} \| ID$ and the corresponding *balyan password* $S_{ID} \| PW$.

Step L2. The smart card of the user U conducts the following computations:

- Generate a random number r.
- Computes $C_1 = (S_{ID})^r \bmod p$.
- Compute $t = f(T \oplus PW) \bmod p - 1$.
- Compute $m = (S_{ID})^t \bmod p$.
- Compute $C_2 = m(PW)^r \bmod p$.

Step L3. $U \rightarrow AS$: $L_R = (C_{ID} \| ID, C_1, C_2, T_c)$.

D. 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 V1. Check the specific format of the *balyan identity* $C_{ID} \| ID$. If the format of the *balyan identity* is incorrect, then AS rejects the login request L_R.

Step V2. Computes the redirected value $S_{ID} = Red(ID)$.

Step V3. Check, whether the condition $C_{ID} = C_K(S_{ID})$ holds, if not, then AS rejects the login request L_R.

Step V4. Check, whether $T_c - T \le \Delta T$, where ΔT is the legal time interval due to transmission delay, if not, then AS rejects the login request L_R.

Step V5. Check, if $C_2 \stackrel{?}{=} (C_1^{x_s})(S_{ID})^{f(T \oplus PW)} \bmod p$, then the AS accepts the login request. Otherwise, the login request will be rejected by AS.

VII. Security Analysis of the Proposed Scheme

The above scheme is a modified form of the original scheme: Hwang-Li's scheme. The security analysis has been already discussed and demonstrated in [23]. Therefore, this section will only discuss the enhanced security features of the proposed scheme.

A. Shen- Lin- Hwang's attack

In *Shen- Lin- Hwang's attack*, the attacker Bob is not a registered user at the AS. To create some favorable results for a successful attack, he requires the redirected identity S_{ID_A} of a previously registered user, say Alice. But in our scheme, the redirected identity S_{ID} of every registered user is calculated secretly by the AS with the help of Red (.) function. The function Red (.) redirects a valid identity into a shadow identity S_{ID} on the basis of the information, which is sent by the user at the time of registration request. AS computes the password by using the $PW = (S_{ID})^{x_s} \bmod p$, where S_{ID} a redirected secret value corresponding to the registered identity ID of the string J.

This secret redirected identity S_{ID} is then attached with the password as a necessary part to obtain the balyan password $S_{ID} \| PW$. Assume that an eavesdropper, Bob intercepts the logon request $L_R = (C_{ID} \| ID, C_1, C_2, T_c)$ from a public network, then it is clear that by using the login request L_R neither he can obtain any information to attack the scheme nor he can compute the balyan password $S_{ID} \| PW$ from this login request L_R. Thus, in our scheme, there is no way for the attacker to obtain the complete balyan password $S_{ID} \| PW$.

In our scheme, there is no way for the attacker to register herself/himself by intercepting the login request L_R. He is not able to produce any favorable results for a successful attack. Consequently, the functionality of Red (.) blocks the masquerade attack via identity: *Shen- Lin- Hwang's attack.*

B. Chan- Cheng's attack and Chang- Hwang's Attack

In *Chan- Cheng's attack and Chang- Hwang's Attack,* the attacker Alice is a registered user at the *AS.* To create some favorable results for a successful attack, only he has the knowledge of a secret redirected identity S_{ID} corresponding to her registered identity *ID.* To perform Chan- Cheng's attack and Chang- Hwang's attack, the attacker Alice computes

$$S_{ID_B} = (S_{ID_A})^k \bmod p,$$

where k is a random number. Then, he can compute the corresponding password

$$PW_B = PW_A{}^k \bmod p.$$

This result is incomplete; still, it is essential to obtain the check digit corresponding to S_{ID_B}. In our scheme, only the *AS* can generate a valid check digit corresponding to the redirected identity S_{ID_B}. As a result, a legal user Alice cannot compute a valid pair of balyan identity and balyan password to impersonate other user Bob to gain the access login right at the *AS*. Thus, *Chang- Hwang's Attack* will not work. Since, Chan – Cheng's attack is another form of this attack, so this attack also does not work properly.

Consequently, the functionality of C_K (.) blocks the attacks via password - *Cheng's attack and Chang- Hwang's Attack.*

c. 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 corresponding to the previously registered identity string *J/ID* or he can try to generate new passwords 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 balyan password corresponding to a previously registered *ID* or the balyan password corresponding to a newly selected valid identity string J_{new}, for the success of the attack, 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 he 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.

VIII. CONCLUSIONS

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 balyan passwords corresponding to the previously registered identities strings *J.* The attacker is also not able to construct or generate new balyan passwords by selecting a newly valid identity string J_{new}. Due the combined functionality of *Red* (.) and C_K (.) at the *AS,* the malicious user will not be able to make any type of attack on the proposed scheme. 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.

Hwang- Li's scheme is suffered with two types of attacks: attacks by an adversary, which is not registered at the *AS*: *Shen- Lin- Hwang's attack* and the attacks by an adversary, which is already registered at the *AS*: *Chan- Cheng's attack and Chang- Hwang's Attack.* The proposed scheme blocks both the ways of attacks. At the first door, the functionality of *Red* (.) blocks the masquerade attack: *Shen- Lin- Hwang's attack* by a non-registered adversary, say Bob and at the second door the functionality of C_K (.) blocks the attacks: *Cheng's attack and Chang- Hwang's Attack* by a registered adversary, say Alice. Thus, the proposed scheme removes the security flaw of the original scheme: Hwang-Li's scheme. The proposed scheme is also secure against all the attacks: *Shen-Lin- Hwang's attack, Chan- Cheng's attack and Chang-Hwang's Attack.*

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 security flaws of Hwang – Li's scheme.

REFERENCES

[1] A. J. Menezes, P. C. vanOorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, pp. 490 – 524, 1997.

[2] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smarts cards with forward secrecy", *IEEE Trans. Consumer Electronic,* vol. 49, no. 4, pp. 1246-1248, Nov 2003.

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.
[10] C. Mitchell, "Limitation of a challenge- response entity authentication," Electronic Letters, vol. 25, No.17, pp. 1195- 1196, Aug 1989.
[11] 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.
[12] 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.
[13] J. A. Gallian and S. Winters, *Modular Arithmetic in the Marketplace.* The American Mathematical Monthly- 95, pp. 548-551, 1988.
[14] J. A. Gallian, "*Assigning driver's license number," Mathematics Magazine* -64, pp. 13-22, 1991.
[15] J. A. Gallian, "*Breaking the missouri license code,*" *The UMAP Journal* -13, pp. 37-42, 1992.
[16] J. A. Gallian, "*The mathematics of identification numbers*," *The College Mathematics Journal* -22, pp. 194-202, 1991.
[17] J. A. Gallian, *Contemporary Abstract Algebra. Narosa Publishing House, ISBN* 81 – 7319 – 077 - 1, pp. 8 -13, 1999.
[18] 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.
[19] 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.
[20] 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.
[21] L. Lamport, "Password authentication with insecure communication," *communication of the ACM,* vol. 24, no. 11, pp. 770-772, 1981.M. S.
[22] M. Kumar, "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.
[23] 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.
[24] 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.
[25] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," *Proc. Advances in Cryptography* (CRYPTO'99), pp. 388-397, 1999.
[26] 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.
[27] S. J. Wang, "Yet another login authentication using N-dimensional construction based on circle property," *IEEE Trans. Consumer Electronic,* vol. 49, No. 2, pp. 337-341, May 2003.
[28] S. Lin and D. Costello, *Error Control Coding:* Fundamental and Applications. Prentice – Hall, Englewood- Cliffs, NJ, 1983.
[29] S. M. Yen and K.H. Liao, "Shared authentication token secure against replay and weak key attack," *Information Processing Letters,* pp. 78-80, 1997.
[30] S. W. Lee, H. S. Kim and K. Y. Yoo, " Comment on a remote user authentication scheme using smart cards with forward secrecy," *IEEE Trans. Consumer Electronic,* vol. 50, no. 2, pp. 576-577, May 2004.
[31] T. C. Wu, "Remote login authentication scheme based on a geometric approach," *Computer Communication,* vol. 18, no. 12, pp. 959 - 963, 1995.
[32] 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.
[33] 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.
[34] 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.
[35] 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.
[36] W. Leveque, *Elementary Theory of Number*. Dover- 1990.
[37] 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.
[38] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption)<< cost(signature) + cost(encryption)," In Advances in Cryptology – *CRYPTO* - 97,vol. 1294, LNCS, pp. 165-179, 1997

Manoj Kumar received the B.Sc. degree in mathematics from Meerut University Meerut, in 1993; the M. Sc. in Mathematics (Goldmedalist) from C.C.S.University Meerut, in 1995; the M.Phil. (Goldmedalist) in *Cryptography*, from Dr. B.R.A. University Agra, in 1996; 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, and U.P., India from March, 2001 to Nov, 2001; at Hindustan College of Science & Technology, Farah, Mathura, continue since Nov, 2001. He also qualified 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, Ramanujan Mathematical society, and Cryptography Research Society of India. His current research interests include Cryptography, Numerical analysis, Pure and Applied Mathematics.