Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 116 (2018) 50191-50195

ISSN: 2229-712X

Efficient Multi-Server Password Authenticated Key Agreement

MRS.SK.Shahina, Yeruva.Seethamahalakshmi, P.Alekhy and S. Akhileswari
Department of Computer Science Engineering, Tirumala Engineering College.

ARTICLE INFO

Article history:
Received: 14 February 2018;
Received in revised form:
8 March 2018;
Accepted: 19 March 2018;

Keywords
Multi-server,
E-commerce,
Dynamic ID,
Anonymity.

ABSTRACT

Since the number of server providing the facilities for the user is usually more than one, the authentication protocols for multi-server environment are required for practical applications. Most of password authentication schemes for multi-server environment are based on static ID, so the adversary can use this information to trace and identify the user's requests. It is unfavorable to be applied to special applications, such as e-commerce. In this paper, we develop a secure dynamic ID based remote user authentication scheme to achieve user's anonymity. The proposed scheme only uses hashing functions to implement a robust authentication scheme for the multi-server environment. It provides a secure method to update password without the help of third trusted party. The proposed scheme does not only satisfy all requirements for multi-server environment but also achieve efficient computation. Besides, our scheme provides complete functionality to suit with the real applications.

© 2018 Elixir All rights reserved.

1. Introduction

With the rapid growth of Internet technologies, the system providing resources to be accessed over the network often consists of many different servers around the world. The distribution of the remote system hardware in different places makes the user access the resources more efficiently and conveniently. In a single server environment, the issue of remote login authentication with the smart card has already been solved by a variety of schemes [1–13]. If conventional password authentication methods are applied to multi-servers environ-ment, each network user does not only need to log into various remote servers repetitively but also need to remember many sets of identities and passwords. It is inefficient and easily leads to the compromise of the identities and passwords. Besides, it is an important topic for managing the shared secret key efficiently among the involved participants. On the other hand, with the rapid growth of those e-commerce applications, a remote user authentication with anonymity is required or desirable. Until now, several papers have been devoted to the study of accessing the resources of multi-servers environments [14–23]. Among these schemes, based on the computation complexity, the smart card-based authentication schemes are divided into two types, namely hash-based authentication and public-key based authentication.

A secure and efficient remote user authentication for multi-server environment usually meets the following requirements [21]:

R1: Single registration. It allows the user to register only once at the registration center and then he can access all the registered servers.

R2: Low computation. Due to the computation power constraints of smart card, they may not provide a powerful computation capability. The authentication scheme must take computation efficiency into consideration such that it can be a practical scheme for the smart card applications.

R3: No verification table. It needs no password tables or verification tables are stored in each registered server.

R4: Update password securely and freely. It allows the cardholder to update his password freely after assuring the legality of cardholder.

R5: Mutual authentication and key agreement. It allows the users and servers to authenticate each other and then negotiate a session key to protect the transmitting message.

R6: Security. The authentication scheme must be able to resist all kinds of attacks such that it can be applied in the real world.

In this paper, we present a secure and efficient authentication scheme with anonymity for multi-server environment. The objective of our scheme emphasize that it does not only satisfy the all above requirements but also protect the user's identity to apply to the special service, such as e-economic applications. Our scheme can get service granted from multi-server environment without maintaining any secret key tables in each registered server. Besides, our scheme achieves efficient computation for the smart card applications. The remainder of the paper is organized as follows. In Section 2, we present a secure and efficient authentication for multi-server environment. Then, we review related works in Section 3. We analyze the security of our scheme in Section 4. The comparison of the performance and the functionality of our scheme with the others are shown in Section 5. Finally, the conclusion is given in Section 6.

2. Literature review

Due to the widespread applications of Internet services, the study of accessing the resources of multi-server environment has received considerable attention, and many schemes are proposed successively [14–23]. Those schemes can be dived into two types, namely hash-based authentication and public-key based authentication. Lee and Chang (2000) proposed a user identification and key distribution scheme that is based on the difficulty of factorization and hash function [14]. It agreed with the multi-server environment. Next, Tsaur (2001) proposed a remote user authentication scheme based on RSA cryptosystem and

Lagrange interpolating polynomial for multi-server environments [15]. In the same time, Li et al. proposed a remote password authentication scheme by using neural networks [16]. However, it is impractical to spend too much time and cost on training and maintaining neural networks. Later, Lin et al. (2003) proposed a new efficient remote user authentication scheme based on the simple geometric properties of the Euclidean [17]. Many schemes have pointed out the weakness of the above schemes and have proposed the solving methods intensively [18–20].

Another interactive password authentication based on simple hashing function and symmetric-key cryptosystem also have been proposed successively. Juang (2004) pointed out that Lin et al.'s scheme is not enough efficient for the authentication process, and then proposed an efficient multi-server user authentication and key agreement based on hashing function and symmetric-key crypto-system [21]. He introduces the shared key inquire phase to obtain the shared secret key between the network user and the service provider, and then mitigate the load of each registered server for maintaining the encrypted keys table. However, Juang's scheme neither updates user's password without the help of registration center nor provide the smart card for the mechanism of checking identity and password in the login phase. Thus, it will easily suffer online guessing attack after losing the smart card. Besides, if the secret parameters of the smart card are extracted with some ways [25], Juang's scheme cannot withstand offline dictionary attack. To reduce the computation cost the shared key inquire phase, Chang-Lee (2004) proposed an efficient scheme, which assume that the secret key x of registration center is distributed to each registered server via secure channel [22]. However, the proposed scheme can not withstand the insider attack.

3. Proposed authentication protocol

In this section, we propose an efficient and secure authentication scheme for multi-server environment. The notations used in our scheme are summarized in Table 1. In view of the efficiency computation, the proposed scheme use simple hashing functions to complete the mutual authentication and session key agreement. The proposed scheme introduces dynamic ID to achieve user's anonymity [9]. Besides, our scheme is a nonce-based scheme to avoid the time-synchronization problem. Consider the multi-server environment containing three participants, the user (U_i), the service provider (S_j) and the registration center (RC). It is assumed that RC is a trusted party responsible for the secret keys distribution between U_i and S_j. RC chooses the master secret key x and a secret number y to distribute among the involved parties via secure channel. Let ID_i denotes a unique identification of U_i and SID_j a unique identification of S_j. The proposed scheme is divided into some phases, including registration phase, login phase, mutual verification and session key agreement phase. Moreover, we provide the password change phase to update the user's password without the help of RC.

Different phase works as follows:

3.1. Registration phase

When the user U_i wants to access the resources of the service provider S_j, he has to submit his identity ID_i and password PW_i

Table 1.Definition of notations used in our scheme.

Notation	Definitions
U_i	ith user
S_j	jth server
RC	Registration center
ID_i	Unique identification of U_i
PW_i	Unique password of U_i
SID_j	Unique identification of S_j
CID_i	Dynamic ID of U_i
h(.)	A one-way hash function

x The master secret key of registration center

y A secret number shared with the registration center and all servers

⊕The exclusive-or operation

|| The concatenation operation

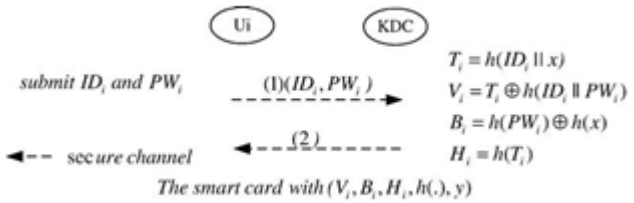

Fig 1. The login phase of our scheme.

to RC. Then, RC performs the following steps as shown in Fig. 1:

1. Compute $T_i = h(ID_i||x)$, $V_i = T_i \oplus h(ID_i||PW_i)$, $B_i = h(PW_i) \oplus h(x)$ and $H_i = h(T_i)$.
2. Issue the smart card with the secret parameters (V_i, B_i,H_i, h(.), y) to the userU_i through a secure channel.

3.2. Login phase

The userU_i keys his identity ID_i , password PW_i and the server identity SID_j in order to login the service provider S_j, and then the smart card performs the following steps:

1. Compute $T_i = V_i \oplus h(ID_i \| PW_i)$ and $H_i = h(T_i)$. Checks whether H_i and H_i is equal or not. If yes, the legality of the user can be assured and proceeds to the next step; otherwise, reject the login request.
2. Generate nonce N_i and compute (CID_i, P_{ij}, Q_i) in accordance with the following equations:

$$CID_i = h(PW_i \| Ph(T \| y \| N_i \| SID_j) \quad (1)$$
$$P_{ij} = T_i \oplus h(y \| N_i \| SID_j) \quad (2)$$
$$Q_i = h(B_i \| y \| N_i) \quad (3)$$

3. Send the login request message $\{CID_i, P_{ij}, Q_i, N_i\}$ to the service provider S_j.

3.3. Mutual verification and session key agreement phase

Upon receiving the login request message $\{CID_i, P_{ij}, Q_i, N_i\}$, the service provider S_j authenticates the user U_i with the following steps:

1. Compute $T_i = P_{ij} \oplus h(y||N_i||SID_j)$, $h(PW_i) = CID_i \oplus h(T_i||y||N_i)$ and $B_i = h(PW_i) \oplus h(x)$.
2. Compute $h(B_i||N_i||y)$, and then compares it with Q_i. If they are not equal, the server S_j rejects the login request and terminates this session.
3. Generate nonce N_j and computes $M_{ij1} = h(B_i||N_i||y||SID_j)$, and then send back the message (M_{ij1}, N_j) to the userU_i.

Upon receiving the acknowledge message (M_{ij1}, N_j) , the user U_i performs the following steps:

4. Computes $h(B_i||N_i||y||SID_j)$ and compare it with M_{ij1}. If they are equivalent, it indicates that the legality of the service provider S_j is authenticated; otherwise, the connection is interrupted.
5. Computes $M_{ij2} = h(B_i||N_j||y||SID_j)$, and then send back M_{ij2} to the service provider S_j.

Upon receiving the message M_{ij2} , the service provider S_j responds to the following step:

6. Compute $h(B_i||N_j||y||SID_j)$ and compare it with M_{ij2}. If it is hold, the identity of U_i can be assured.

After finishing mutual authentication phase, the user U_i and the service provider S_j compute $h(B_i||N_i||N_j||y||SID_j)$ as the session key SK. The authentication protocol also is shown in Fig. 2.

3.4. Password change phase

When the userU_i wants to update his password without the help of RC, he inserts his smart card to card reader and inputs (ID_i , PW_i) corresponding to the smart card. To avoid the adversary

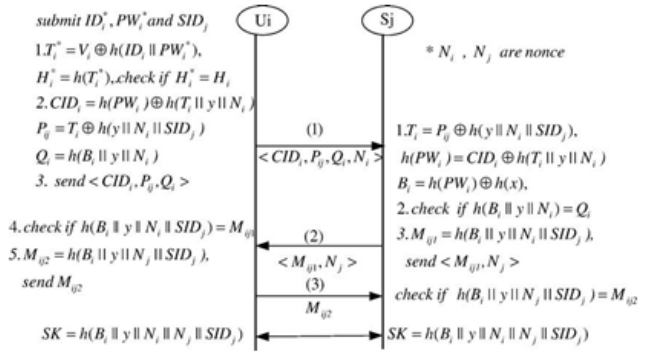

Fig 2. The authentication protocol of our scheme.

updating password freely by way of stealing the smart card, the smart card first works as the step1 of login phase. After assuring the legality of the cardholder, the smart card allows the cardholder to resubmit a new password PW_i^{new}, and then V_i stored in the smartcard can b update with $V_i^{new} = T_i \oplus h(ID_i||PW_i^{new})$. Similarly, B_i stored in the smart card can be replaced with $B_i^{new} = B_i \oplus h(PW_i) \oplus h(PW_i^{new})$.

4. Security analysis

In this section, security analysis of the proposed scheme is given. We will show that the proposed scheme can withstand the various possible attacks.

4.1. Two-factor security

Obviously, if both the user's smart card and his password were stolen, then there is no way to prevent the attacker from masquerading as the user. So the best we can do is to guarantee the security of the scheme when either the user's smart card or his password is stolen, but not both. This security property is called two-factor security [24]. For our scheme, the secret parameters (V_i, B_i, H_i, h(.), y) of the smart card are hard to derive if the attacker has obtained the user's password instead of smart card. Though the attacker may also intercept the user's previous login request messages (CID_i, P_{ij}, Q_i, N_i), it is infeasible to derive T_i and y from CID_i and P_{ij}, which are based on the security of one-way hash function. Similarly, B_i and y are hard to be extracted from Q_i. On the other hand, if the attacker steals the user's smart card and extracts the secret values (V_i, B_i, H_i, h(.), y) stored in the smart card with some ways [25], he still cannot obtain PW_i directly. Although the attacker may calculate $T_i = V_i \oplus h(ID_i || PW_i)$ and $H_i = h(T_i)$, he cannot launch an offline dictionary attack to finds PW_i without knowing corresponding ID_i. Thus, our scheme indeed provides two-factor security.

4.2. Replay attack

The replay attack is replaying the same message of the receiver or the sender again. Our scheme uses nonce instead of timestamp to withstand replay attacks. After incepting the previous login request $bCID_i$, P_i , Q_{ij}, N_i N from the user U_i, the attacker may replay the same message to the service provider S_j. Then the attacker can receive acknowledge message (M_{ij1}, N_j) from the service provider S_j after the step 3 of mutual verification phase. However, the attacker can not compute M_{ij2} to respond to the server S_j without knowing B_i and y. Similarly, when we assume that the attacker replies a previous message (M_{ij1} , N_j) to U_i, where M_{ij1} is associated with N_i . Upon receiving (M_{ij1} , N_j), U_i computes $h(B_i||y||N_i||SID_j)$ and checks whether it is equal to M_{ij1} . It is obvious that the equality cannot hold since N_i is not equal to N_i.

4.3. Server spoofing attack

Our scheme can protect the user from cheating by the masque-raded service provider since the adversary can not construct the session key SK without the knowledge of B_i and y. After communicating with the masqueraded service provider, the legal user can detect immediately and terminate the session.

4.4. Insider and stolen verifier attack

The insider attack is defined that any manager of system purposely leaks the secret information, and then lead to serious security flaws of authentication scheme. In our scheme, the insider can obtain $h(PW_i)$ instead of PW_i according to the step 1 of the mutual verification phase, and it is hard to get PW_i within acceptable interval. Moreover, the insider cannot disclose the master secret key x since it is protected by hash function. Our scheme also does not maintain any verifier table. Thus the insider and stolen verifier attack are resisted.

4.5. Security of session key

4.5.1. Known–key security

The known-key security means that compromise of a past session key can not derive any further session key. In our scheme, the session key SK is associated with B_i and y, which are unknown to the adversary. Even though the past session key SK is disclosed, the attacker cannot derive B_i and y based on the security of one-way hash function. Thus, the attacker can not obtain any further session key.

4.5.2. Forward secrecy

The forward secrecy means that even though the master secret key x is disclosed for some reason, it will not cause the compromise of any earlier session. Suppose the secret key x is compromised, the adversary can not compute Bi without knowing PW_i. Therefore, the adversary can not derive the session key SK, since it is computed by $h(B_i||N_i||N_j||y||SID_j)$. In other words, the adversary can not decrypt any sensitive message encrypted with SK.

4.6. User anonymity protected

The user U_i will send the login request (CID_i, P_{ij}, Q_i, N_i) to the server S_j in each login.

Thus, the attacker may incept and analyze the login message. It is infeasible to derive ID_i from the login message. Moreover, the login message is dynamic in each login. Among the parameters of login message, CID_i is associated with nonce N_i and dynamically changed. Similarly, the values of P_{ij} and Q_i are also related to nonce N_i. Therefore, an adversary can not identify the person who is trying to login. In other words, our scheme can protect user's anonymity.

4.7. Securely chosen password

In the password change phase, the cardholder can freely change password as his favorite stings without the help of RC. To avoid unauthorized users easily changing the password after obtaining the smart card for some reason, the legality of the cardholder must be assured. In our scheme, anyone even having the smart card can not update the password without knowing the identity and password corresponding to the smart card.

5. Performance and functionality analysis

Due to the resources constraints of smart card, the authentication scheme must take efficiency evaluation into consideration. In this section, we will evaluate the performance of the proposed scheme and make comparison with the others in Table 1. In general, the efficiency evolution usually is divided into communication cost and computation cost [19]. We use the following facts and assumptions to evaluate. Assume the identity ID_i, password PW_i, timestamp and nonces are all 128-bit length; the large prime in modular operation is 1024-bit length in practical implementation. Moreover, we also assume both the output size of secure one-way hashing functions h(.) and the block size of secure symmetric cryptosystem are 128-bit. The notations T_h, T_{sym} and T_{exp} are defined as the time complexity for hashing function, symmetric encryption/decryption and exponential operation respectively. Typically, under a modulus n the computation cost of a modular exponentiation computation is about O (| n |) times that of a modular multiplication computation, where | n | denotes the bit length of n [26]. Each of random generation, hashing function, and symmetric encryptions or decryptions does not take longer time than that of a modular multiplication computation in Z_n . Hence, the computation time consumed by few modular multiplications, hashing operations, random number generations and symmetric encryptions or decryptions in the entire existing schemes can be neglected as compared with the modular exponentiation. Under the above assumptions, the time complexity associated with the different operations can be roughly expressed as T_{exp} NN T_{sym} NT$_h$.

Table 2.Efficiency comparison between our scheme and other related schemes.

	Ours	Chang-Lee [22]	Juang [21]	Lin et al. [17]
E1	512 bits (0.5| n |)	256 bits (0.25| n |)	256 bits (0.25| n |)	(4t + 1)|n| bits
E2	7 128 bits (0.875| n |)	8 128 bits (| n |)	13 128 bits (1.625| n |)	7 1024 bits (7| n |)
E3	5T_h bb T	2T_h bb T	T_h bb T	≈5$_t$ T_{exp} = 5tT
E4	9T_h bb T	4T_h + 3T_{sym} bb T	3T_h + 3T_{sym} bb T	≈2T_{exp} = 2T
E5	6T_h bb T	4T_h + 3T_{sym} bb T	4T_h + 8T_{sym} bb T	≈7T_{exp} = 7T

E1: Memory needed in the smart card.
E2: Communication cost of the authentication.
E3: Computation cost of the registration.
E4: Computation cost of the user.
E5: Computation cost of the service provider.
t : the number of servers.
T :the time complexity of a modular exponentiation computation in Z_n ,| n | = 1024 bits.

Table 3.The functionality comparison between our scheme and the others.

	Ours	Chang-Lee [22]	Juang [21]	Lin et al. [17]
Computation cost	Very low	Low	Low	High
Single registration	Yes	Yes	Yes	No
No verification table	Yes	Yes	Yes	Yes
Securely chosen password	Yes	No	No	No
Mutual authentication	Yes	Yes	Yes	No
Session key agreement	Yes	Yes	Yes	No
User's anonymity	Yes	No	No	No
No time synchronization	Yes	Yes	Yes	No
Two factor security	Yes	No	No	No

In our scheme, the parameters stored in the smart card are V_i, B_i, H_i and y, so memory needed in the smart card is 512(=4 128) bits. The communication cost of authentication includes the capacity of transmitting message involved in the authentication scheme. At the user side, the capacity of transmitting message is 640(=5 128) bits, including {CID_i, P_{ij}, Q_i, N_i} and M_{ij2}. As for the service provider side, that is 256(=2 128) bits, including

{M_{ij1}, N_j}.The computation cost of registration is defined as the total time of various operations executed in the registration phase. According to the above definition, the computation cost of registration is 5T_h. Similarly, the computation cost of the user and the service provider are focused on the time spent by the user and the service provider in the process of authentication. Therefore, both the computation cost of the user and that of the service provider are 9T_h and 6T_h respectively. In Juang scheme [21], the communication cost of shared key inquiry phase 1024(=8 128) bits is included that of the authentication. Similarly, the computation cost of shared key inquiry phase 2T_h + 4T_{sym} is included that of the service provider. The performance comparison be-tween our scheme and the others is summarized in Table 2. It obviously shows that our scheme is more efficient than the others except for memory needed in the smart card and computation cost of the registration phase. However, the low-computation property for the smart card is still preserved and exceeds the other schemes. Moreover, we summarize the functionality of the proposed scheme and make comparison with some related schemes in Table 3. It demonstrates that our schemes can achieve the essential requirements as mentioned in Section 1. Moreover, our scheme considers two-factor security and user's anonymity to enhance the security level.

6. Conclusion

In this paper, we present an efficient and secure authentication scheme for multi-server environment. We demonstrate that our scheme can satisfy all of the essential requirements. Our scheme does not only manage the secret key tables associated with the users but also achieve user's anonymity. Moreover, our scheme only uses hashing functions to implement mutual verification and session key agreement. It is well suited to the smart card's applications. The other merits include: (1) our scheme provide a secure password change method to prevent the adversary from updating password freely; (2) our scheme can resist various attack, including two-factor security; (3) the computation cost is more efficient; (4) it is a nonce-based scheme to avoid the time-synchronization problem.

References

[1] C.C. Chang, T.C. Wu, Remote password authentication with smart cards, IEE Proc. E 138 (3) (1991) 165–168.
[2] M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 46 (1) (2000) 28–30.
[3] H.M. Sun, An efficient remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 46 (4) (2000) 958–961.
[4] K. Chan, Li M. Cheng, Cryptanalysis of a remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 46 (2000) 992–993.
[5] J.J. Shen, C.W. Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 49 (2) (2003) 414–416.
[6] K.C. Leung, L.M. Cheng, A.S. Fong, C.K. Chan, Cryptanalysis of a modified remote user authentication

scheme using smart cards, IEEE Trans. Consum. Electron. 49 (4) (2003) 1243–1245.
[7] Amit K. Awashti, Sunder Lal, An enhanced remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 50 (2) (2004) 583–586.
[8] C. Chang, K.F. Hwang, Some forgery attacks on a remote user authentication scheme using smart cards, Informatics 14 (3) (2003) 289–294.
[9] M.L. Das, A. Saxena, V.P. Gulati, A dynamic ID-based remote user authen-tication scheme, IEEE Trans. Consum. Electron. 50 (2) (2004) 629–631.
[10] K. Awasthi, Comment on a dynamic ID-based remote user authentication scheme, Trans. Cryptol. 01 (2) (2004) 15–16.
[11] W.C. Ku, S.T. Chang, Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards, IEICE Trans. Commun. (5) (2005).
[12] J.J. Shen, C.W. Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 49 (2) (2003) 414–416.
[13] C. Lee, M.S. Hwang, W.P. Yang, A flexible remote user authentication scheme using smart cards, ACM Oper. Syst. Rev. 36 (3) (2002) 46–52.
[14] W.B. Lee, C.C. Chang, User identification and key distribution maintaining anonymity for distributed computer network, Comput. Syst. Sci. 15 (4) (2000) 211–214.
[15] W.J. Tsuar, C.C. Wu, W.B. Lee, A flexible user authentication for multi-server internet services, Networking-JCN2001LNCS, vol. 2093, Springer-Verlag, 2001, pp. 174–183.
[16] L. Li, I. Lin, M. Hwang, A remote password authentication scheme for multi-server architecture using neural networks, IEEE Trans. Neural Netw. 12 (6) (2001) 1498–1504.
[17] C. Lin, M.S. Hwang, L.H. Li, A new remote user authentication scheme for multi-server architecture, Future Gener. Comput. Syst. 1 (19) (2003) 13–22.
[18] W.J. Tsuar, An enhanced user authentication scheme for multi-server internet services, Appl. Math. Comput. 170 (2005) 258–266.
[19] T.S. Wu, C.L. Hsu, Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks, Comput. Secur. 23 (2004) 120–125.
[20] Y. Yang, S. Wang, F. Bao, J. Wang, R. Deng, New efficient user identification and key distribution scheme providing enhanced security, Comput. Secur. 23 (8) (2004) 697–704.
[21] W.S. Juang, Efficient multi-server password authenticated key agree-ment using smart cards, IEEE Trans. Consum. Electron. 50 (1) (2004) 251–255.
[22] C. Chang, J.S. Lee, An efficient and secure multi-server password authentication scheme using smart cards, IEEE. Proceeding of the International Conference on Cyberworlds, 2004.
[23] C. Chang, J.Y. Kuo, An efficient multi-server password authenticated keys agreement scheme using smart cards with access control, IEEE. Proceeding of the 19th International Conference on Advanced Information Networking and Applications, 2005.
[24] X. T, R.W. Zhu, D.S. Wong, Improved efficient remote user authentication schemes, Int. J. Netw. Secur. 4 (2) (2007) 149–154.
[25] T.S. Messergers, E.A. Dabbish, R.H. Sloan, Examining smart card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5) (2002) 541–552.
[26] A. Menezes, O.P. Van, S. Vanstone, Handbook of applied cryptography, CRC Press, LLC, Boca Raton, 1997.