Journal of Engineering and Applied Sciences 14 (19): 7013-7019, 2019
ISSN: 1816-949X

Weaknesses of Anonymous Mutual Authentication Schemes for Roaming Service with Smart Cards

Younsung Choi
Department of Computer Science, Major of Cyber Security, Howon University,
Gunsan-si, 54058 Jeollabuk-do, Republic of Korea, yschoi@howon.ac.kr

Abstract: In wireless communications, various anonymous mutual authentication schemes use public key cryptosystems to provide secure roaming service but are not computationally efficient. Guo *et al*., first, proposed an efficient mutual authentication protocol providing user anonymity and using smart cards but this scheme has security weaknesses. Liu *et al*. attempted to address this by proposing a mutual authentication scheme in wireless communications with anonymity for roaming service with smart cards in wireless communications but this scheme still has security vulnerabilities. The present study demonstrates security problems of mutual authentication scheme: it is vulnerable to offline password (and identity) guessing attack does not provide perfect forward secrecy is vulnerable to DoS attack and provides weak anonymity.

Key words: Roaming service, authentication scheme, mutual authentication scheme, guessing attack, anonymity, scheme

INTRODUCTION

Provided by the Home Agent (HA) in a Foreign network, the global mobility network furnishes global roaming service permitting Mobile Users (MUs) to connect to services. When an MU roams to a Foreign network controlled by a Foreign Agent (FA), it authenticates with the FA under the assistance of their HA in the home network. Therefore, the remote user authentication scheme in wireless networking has raised security concerns among MUs and service providers and various authentication protocols have recently been proposed for the global mobility network (Lee *et al*., 2006; Xu *et al*., 2011).

MU can connect the services provided by HA in an FA and provide mutual authentication with the corresponding FA in wireless networks. Secure user authentication schemes in wireless networks should assure each of the following: user friendly behavior, mutual authentication, user anonymity, forward and backward secrecy, security, no password table, confidentiality of the session key, fairness in key agreement, low communication cost and computation complexity and ability to update passwords securely and freely (Xu *et al*., 2011; Guo *et al*., 2013). Various smart card-based authentication schemes have been proposed for roaming services but some authentication schemes have security problems, allowing insider attack, password-guessing attack, lack of mutual authentication and masquerade attack. To resolve these security weaknesses, various researchers have proposed schemes for mutual authentication with anonymity (Xu *et al*., 2011; Guo *et al*., 2013; He *et al*., 2010).

He *et al*. (2010) introduced a secure authentication scheme for wireless communications including the use of a smart card in 2011. Various previous schemes proposed for wireless networks used modular exponential computing and scalar multiplication on elliptic curves to ensure security. Guo *et al*. (2013) proposed a mutual authentication key agreement protocol for wireless communications based on Chebyshev chaotic maps and the use of smart cards. They asserted that their protocol provides user anonymity even, if the attacker can extract all information from the smart card. However, Liu *et al*. (2016) demonstrated that Guo *et al*., scheme is vulnerable to impersonation attack and does not allow Mus to update their passwords freely. Liu *et al*. (2016), then proposed an alternative scheme an efficient and anonymous authentication protocol for wireless communications (Guo *et al*., 2013; He *et al*., 2010; Jerabek, 2016; Rabin, 1979; Williams, 1980; Liu *et al*., 2016).

However, the present study demonstrates that Liu *et al*. (2016) authentication scheme is vulnerable to offline password (and identity) guessing attack does not provide perfect forward secrecy is vulnerable to DoS attack and provides weak anonymity.

MATERIALS AND METHODS

Review of Liu *et al*. (2016) mutual authentication scheme: Before the registration phase starts, HA

generates two distinct large primes p_1 and q_1 ($p_1 = q_1 = 3 \pmod 4$) and computes $n_1 = p_1 \times q_1$. The HA then selects its secret key d and generates n_1 and h(•) but keeps d, p_1 and q_1 secret, here, h(•) represents a secure one-way hash function. The FA selects two distinct large primes p_2 and q_2 ($p_2 = q_2 = 3 \pmod 4$), computes $n_2 = p_2 \times q_2$ and generates n_2. K_{FH} is a secret key previously shared between FA and HA. Liu *et al.* (2016) mutual authentication scheme consists of three phases: a registration phase, a mutual authentication phase and a password update phase. These are detailed in the following sections.

Registration phase: When an MU wants to register with a system, she/he chooses a Password PW_M and a random number b_M and computes $h(PW_M||b_M)$ where the double bar symbol is the string concatenation operator. The MU, then, sends her/his Identity ID_M and the hashed password $h(PW_M||b_M)$ to the HA for registration (Liu *et al.*, 2016).

Stage 1; HA computes:

$$u = (h(ID_M|| d))^2 \bmod n_1,$$
$$C = h(u||ID_M),$$
$$v = u \oplus h(PW_M|| b_M)$$

Stage 2 HA issues a smart card containing n_1, h(•), v and C and sends the smart card to MU by means of a secure channel. Stage 3 MU inputs b_M into the smart card.

Mutual authentication phase: Figure 1 shows the mutual authentication scheme. In this phase, MU and FA perform the mutual authentication as follows (Liu *et al.*, 2016).

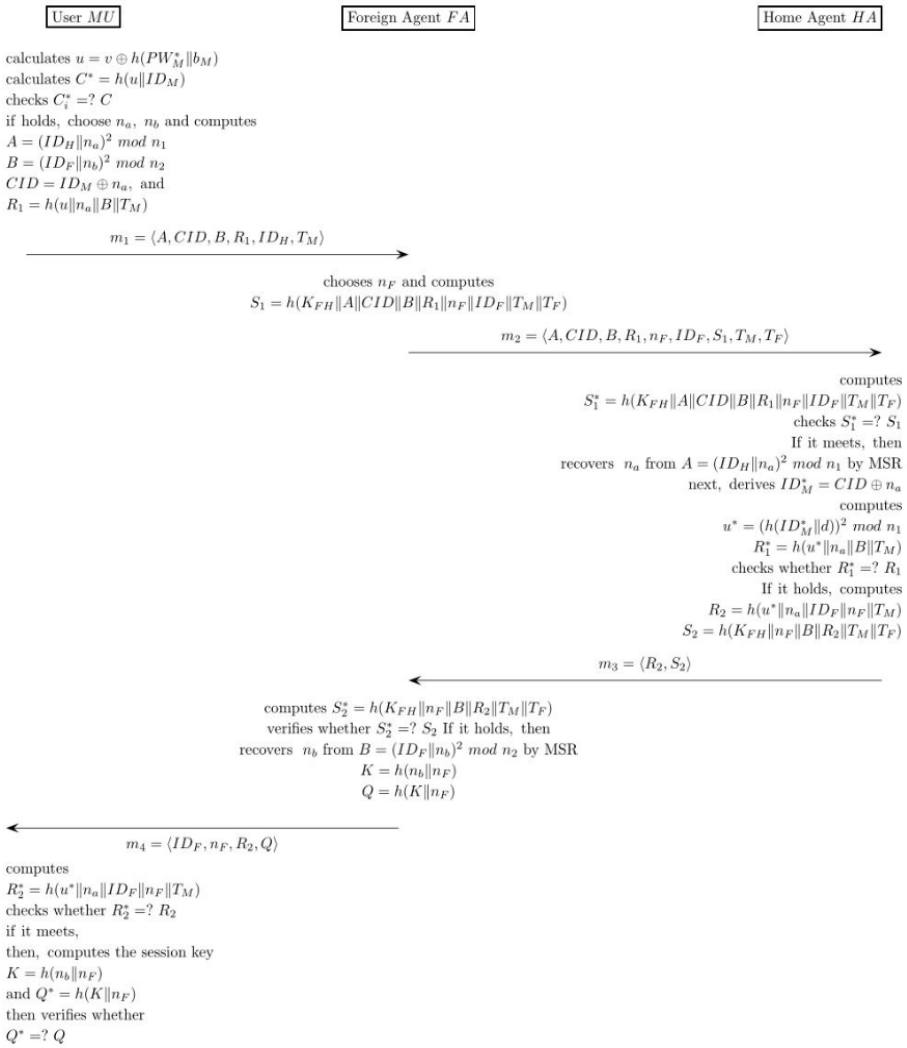

Fig. 1: Mutual authentication phase of Liu *et al.* (2016) scheme

Stage 1: When MU enters a Foreign network managed by FA, she/he inserts the smart card into the smart card reader and inputs ID_M and PW_M. Then, the device computes:

$$u^* = v \oplus h(PW_M||b_M)$$
$$C^* = h(u^*||ID_M)$$

and checks whether $C^* = C$. If not, the device discontinues the login and disallows further login requests for a period of time. Otherwise, the device chooses two random numbers n_a and n_b and then computes:

$$CID = (ID_M \oplus n_a)$$
$$A = (ID_H||n_a)^2 \bmod n_1$$
$$B = (ID_F||n_b)^2 \bmod n_2$$
$$R_1 = h(u^*|| n_a||B||T_M)$$

where, T_M is the current Timestamp. Then, the device sends the information $m_1 = \{A, CID, B, R_1, ID_H, T_M\}$ to FA, where, ID_H and ID_F are the identity numbers of HA and FA, respectively.

Stage 2: Upon receiving $m_1 = \{A, CID, B, R_1, ID_H, T_M\}$, FA first checks whether the Timestamp T_M is fresh. If so, FA randomly selects n_F and computes:

$$S_1 = h(K_{FH}||A||CID||B||R_1||n_F||ID_F||T_M||T_F)$$

and then forwards the information $m_2 = \{A, CID, B, R_1, n_F, ID_F, S_1, T_M, T_F\}$ to HA where, T_F is the current timestamp of FA.

Stage 3: After receiving m_2, HA checks whether T_F is fresh. If so, HA computes the following:

$$S_1^* = h(K_{FH}||A||CID||B||R_1||n_F||ID_F||T_M||T_F)$$

and checks whether $S^*_1 = S_1$. If so, HA can obtain the nonce n_a from MSR of $A = (ID_H||n_a)^2 \bmod n_1$ with knowledge of ID_H and computes the following with its secret key d:

$$ID^*_M = CID \oplus n^*_a,\ u^* = \left(h(ID^*_M||d)\right)^2 \bmod n_1,$$
$$R^*_1 = h(u^*||n_a||B||T_M)$$

Next, HA checks whether $R^*_1 = R_1$; if so, HA computes $R_2 = h(u^*||n_a||ID_F||n_F||T_M)$ and $S_2 = h(K_{FH}||n_F||B||R_2||T_M||T_F)$, then, sends the message $m_3 = \{R_2, S_2\}$ to FA. Otherwise, HA ignores the request for a period of time.

Stage 4: Upon receiving $m_3 = \{R_2, S_2\}$, FA computes $S^*_2 = h(K_{FH}||n_F||B||R_2||T_M||T_F)$ with K_{FH}. Then, FA checks whether $S^*_2 = S_2$. If so, FA concludes that MU is authorized. Then, FA can derive the nonce n_b from MSR of $B = (ID_F||n_b)^2 \bmod n_2$ with knowledge of the identity number ID_F. Next, FA computes the session Key $K = h(n_b||n_F)$, computes $Q = h(K||nF)$ and then delivers the message $m_4 = \{ID_F, n_F, R_2, Q\}$ to MU.

Stage 5: After receiving $m_4 = \{ID_F, n_F, R_2, Q\}$, MU computes:

$$R^*_2 = h(u^*||n_a||ID_F||n_F||T_M)$$

and checks whether $R^*_2 = R_2$. If so, MU concludes that FA is authenticated and computes the session key $K = h(n_b||n_F)$ and $Q^* = h(K||n_F)$. Then, MU checks whether $Q^* = Q$. If so, then, K is used as a common session key for secure communications with FA. Otherwise, MU stops the request.

Through the above steps, both MU and FA can use the common session Key K for secure communications. Here, K, n_a, n_b and n_F are each only used once.

Password update phase: When MU wants to arbitrarily update her/his own Password PW_M, it is not necessary to re-register with HA (Liu *et al*., 2016).

Stage 1: MU inserts the smart card into the smart card reader and then inputs her/his ID_M and old Password PW_M. Next, the device computes the following:

$$u = v \oplus h(PW_M||b_M)$$
$$C^* = h(u||ID_M)$$

and then checks whether $C^* = C$. If so, MU selects a new Password PW_M' and performs stage 2; otherwise, the device terminates the update request and disallows further update requests for a period of time.

Stage 2: The device computes:

$$v' = v \oplus h(PW_M||b_M) \oplus h(PW'_M||b_M)$$

Stage 3: The device replaces v with v′ in the smart card memory. It is accepted because:

$$v' = v \oplus h(PW_M||b_M) \oplus h(PW'_M||b_M)$$
$$= u \oplus h(PW_M||b_M) \oplus h(PW_M||\ b_M) \oplus h(PW'_M||b_M)$$
$$= u \oplus h(PW'_M||b_M)$$

RESULTS AND DISCUSSION

Weakness of Liu *et al.* (2016) mutual authentication scheme: In this study, we analyze Liu *et al.* (2016) mutual authentication scheme to demonstrate various security weaknesses, namely its vulnerability to offline password (and identity) guessing attack, lack of perfect forward secrecy, vulnerability to DoS attack and weak anonymity.

Offline password (and identity) guessing attack: If an adversary steals or otherwise acquires the user's smart card and is also able to learn ID_M and PW_M, this is a serious problem. Figure 2 shows the offline password (and identity) guessing attack of Liu *et al.* (2016) mutual authentication. Messerges *et al.*, have shown that confidential information stored in all smart cards could be extracted by physically monitoring power consumption and analyzing it by means of simple power analysis and differential power analysis (Choi *et al.*, 2014a, b).

By Liu *et al.* (2016) mutual authentication scheme, the smart card stores important information during the user login and authentication phases. If an adversary steal's a user's smart card, the adversary can extract information from the smart card using a side-channel attack including simple power analysis or differential power analysis. So, if a user by Liu *et al.* (2016) mutual authentication scheme loses her/his smart card, all secrets in the smart card including b_M, C, v and h(•) can be revealed to the adversary who could then, compute the following:

$$C = h(u||ID_M)$$
$$u = v \oplus h(PW_M||b_M)$$
$$C = h(v \oplus h(PW_M||b_M)||ID_M)$$

In this formula, an adversary knows all parameters {C, v, b_M, h(•)} except ID_M and PW_M. $|D_{id}|$ and $|D_{pw}|$ represent the number of identities in D_{id} and the number of passwords in D_{pw}, respectively. The password and identity are human-memorable short strings but not high-entropy keys; they are often chosen from two corresponding dictionaries of small size. Therefore, the running time of the aforementioned attack procedure is O ($|D_{id}|*|D_{pw}|*T_H$) where, T_H is the running time for the hash. As $|D_{id}|$ and $|D_{pw}|$ are very limited in practice, $|D_{id}| \leq |D_{pw}| \leq 10^6$, the guessing attack can be completed in polynomial time. The adversary an obtain all parameters in the C formula except ID_M and PW_M, so, an adversary can determine ID_M and PW_M from $C = h(v \oplus h(PW_M||b_M)||ID_M)$ using an off-line password (and identity) guessing attack (Ma *et al.*, 2014).

Lack of perfect forward secrecy: Perfect forward secrecy means that a session key computed from a set of long-term keys will not be compromised, if one of the long-term keys is compromised later. Without perfect forward secrecy an adversary can compute the session between the user and the server (Sui *et al.*, 2005). Figure 3 shows why Liu *et al.* (2016) mutual authentication scheme does not achieve perfect forward secrecy.

By Liu *et al.* (2016) mutual authentication scheme an adversary can obtain ID_F, n_F and B from public communication including the previous session. If the adversary acquires one of the long-term secrets n_2, the adversary can then determine K ($K = h(n_b||n_F)$):

$$B = (ID_F||n_b)^2 \bmod n_2$$

The adversary can extract n_b from the above formula in the same way that FA does. Then, the adversary will

An adversary stole user's own smart card

An adversary extracted smart card's inside information using SPA and DPA

⟶ So an adversary can obtain b_M, C, v, $h(\cdot)$

$C = h(u \| ID_M)$

$u = v \oplus h(PW_M \| b_M)$

$\rightarrow C = h(v \oplus h(PW_M \| b_M) \| ID_M)$

An adversary knows all parameter { C, v, b_M, $h(\cdot)$ } except for ID_M, PW_M

⟶ | $\mathcal{D}_{id}$ | and | $\mathcal{D}_{pw}$ | denote the number of identities and passwords in $\mathcal{D}_{id}$, $\mathcal{D}_{pw}$

⟶ $\mathcal{D}_{id}$ and $\mathcal{D}_{pw}$ are very limited in practice such as | $\mathcal{D}_{id}$ | ≤ | $\mathcal{D}_{pw}$ | ≤ 10^6

→ So an adversary find out ID_M and PW_M from $C = h(v \oplus h(PW_M \| b_M) \| ID_M)$

Fig. 2: Offline password (and identity) guessing attack on Liu *et al.* (2016) mutual authentication scheme

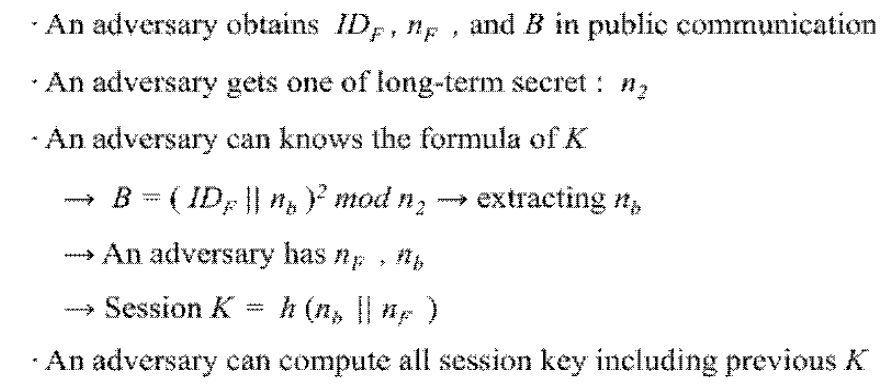

Fig. 3: Lack of perfect forward secrecy by Liu *et al*. (2016) mutual authentication scheme

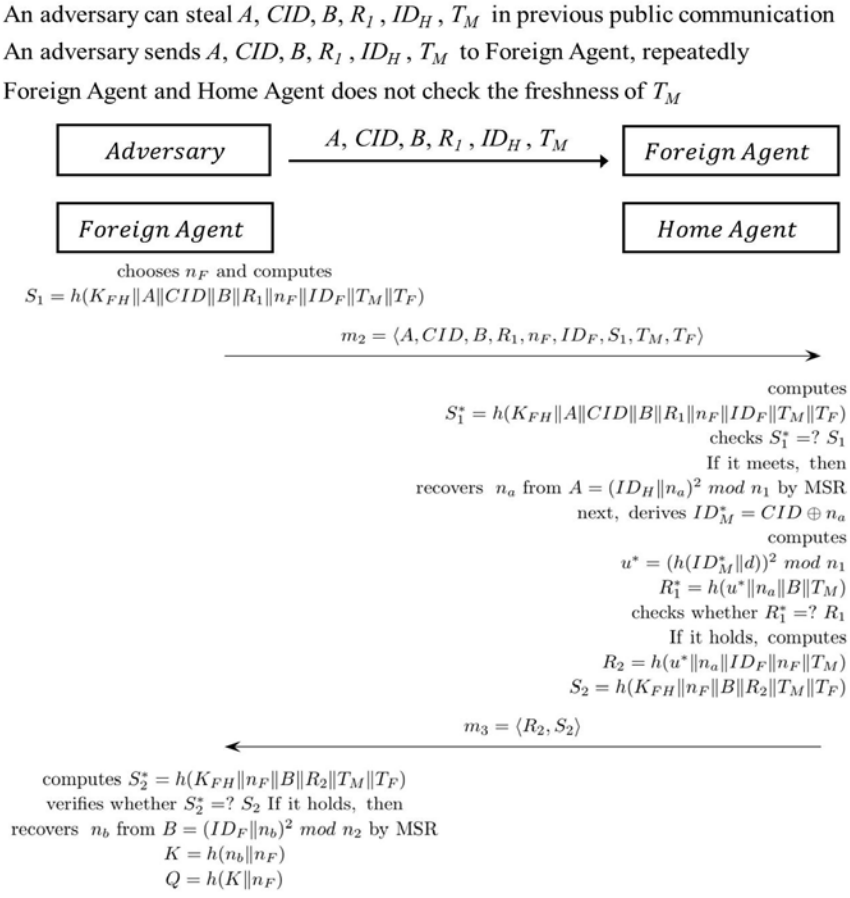

Fig. 4: Vulnerability of Liu *et al*. (2016) mutual authentication scheme to DoS attack

know both n_F and n_b and thus, be able to compute the session key $K = h(n_b\|n_F)$. Moreover, the adversary can compute all session keys including previous keys using the parameters of previous communications. Therefore, Liu *et al*. (2016) mutual authentication scheme has the weakness of not providing perfect forward secrecy.

Vulnerability to DoS attack: Liu *et al*. (2016) mutual authentication uses the Timestamps T_M and T_F but FA and HA do not check the freshness of T_M, so, they are vulnerable to DoS attack. Figure 4 illustrates the weaknesses of Liu *et al*. (2016) mutual authentication scheme to DoS attack (Jung *et al*., 2016).

An adversary can steal a previous authentication message {A, CID, B, R_1, ID_H, T_M} from public communication. The adversary can then send {A, CID, B, R_1, ID_H, T_M} to FA repeatedly after the user's normal authentication phase ends. By Liu *et al.* (2016) mutual authentication scheme, FA does not check the freshness of incoming authentication messages; it only chooses n_F, computes S_1 and sends m_2 = {A, CID, B, R_1, n_F, ID_F, S_1, T_M, T_F} to HA. Also, HA executes all steps for authentication after receiving m_2 because it does not check the freshness of timestamps; HA, then, sends m_3 = {R_2, S_2} to FA. Moreover, FA cannot know that there are problems with such messages m_3, so, it executes all authentication steps after receiving each one. Thus, FA and HA perform the entire series of authentication computations when a previous authentication message is resent. This is a serious problem, indicating the need to assess timestamp freshness at each stage of the authentication process by both the FA and the HA.

Weak anonymity: By Liu *et al.* (2016) mutual authentication scheme, the anonymous identity CID is provided to achieve user anonymity but it is insecure and weak. By Liu *et al.* (2016) mutual authentication scheme, MU sends CID to FA for authentication using public communication, so, an adversary can obtain CID, ID_H and A. If the adversary then acquires the user's smart card and extracts its information including n_1 (Choi *et al.*, 2014 a, b; Kang *et al.*, 2016; Mun *et al.*, 2015), the adversary can then compute the following:

$$CID = (ID_M \oplus n_a)$$
$$\rightarrow n_a = CID_M \oplus ID_M$$
$$A = (ID_H || n_a)^2 \bmod n_1$$
$$\rightarrow A = (ID_H || CID_M \oplus IDM)^2 \bmod n_1$$

In the above formula, the adversary can determine all parameters except ID_M. Using these known parameters, the adversary can determine the user's real identity ID_M using offline guessing attack. Thus, Liu *et al.* (2016) mutual authentication scheme cannot provide complete user anonymity.

CONCLUSION

Liu *et al.* (2016) proposed an efficient remote user authentication protocol for wireless communications based on MSR and using smart cards. However, the present analysis has shown that that this scheme has security problems, namely vulnerability to offline password (and identity)-guessing attack, lack of perfect forward secrecy, vulnerability to DoS attack and weak anonymity.

ACKNOWLEDGEMENT

This research was supported by the National Research Foundation of Korea grant funded by Korea Government (Ministry of Science, ICT and Future Planning) (NRF-2017R1C1B5017492) and this research was supported by financial support of Howon University in 2019.

REFERENCES

Choi, Y., D. Lee, J. Kim, J. Jung, and J. Nam *et al.*, 2014b. Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. Sens., 14: 10081-10106.

Choi, Y., J. Nam, D. Lee, J. Kim and J. Jung *et al.*, 2014a. Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics. Sci World J., 2014: 1-15.

Guo, C., C.C. Chang and C.Y. Sun, 2013. Chaotic maps-based mutual authentication and key agreement using smart cards for wireless communications. J. Inf. Hiding Multimedia Signal Proc., 4: 99-109.

He, D., M. Ma, Y. Zhang, C. Chen and J. Bu, 2010. A strong user authentication scheme with smart cards for wireless communications. Comput. Commun., 34: 367-374.

Jerabek, E., 2016. Integer factoring and modular square roots. J. Comput. Syst. Sci., 82: 380-394.

Jung, J., J. Kim, Y. Choi and D. Won, 2016. An anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks. Sens., 16: 1-30.

Kang, D., J. Jung, J. Mun, D. Lee and Y. Choi *et al.*, 2016. Efficient and robust user authentication scheme that achieve user anonymity with a Markov chain. Secur. Commun. Netw., 9: 1462-1476.

Lee, C.C., M.S. Hwang and I.E. Liao, 2006. Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE. Trans. Ind. Electron., 53: 1683-1687.

Liu, C.S., L. Xu, L. Lin, M.C. Tseng and S.Y. Lin *et al.*, 2016. Mutual authentication with anonymity for roaming service with smart cards in wireless communications. Proceedings of the International Conference on Network and System Security, September 28-30, 2016, Springer, Cham, Switzerland, ISBN:978-3-319-46297-4, pp: 47-61.

Ma, C.G., D. Wang and S.D. Zhao, 2014. Security flaws in two improved remote user authentication schemes using smart cards. Intl. J. Commun. Syst., 27: 2215-2227.

Mun, J., J. Kim, D. Lee, J. Jung and Y. Choi *et al*., 2015. An improvement of efficient dynamic ID-based user authentication scheme using smart cards without verifier tables. Proceedings of the International Conference on Security and Management (SAM'15) and the Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), July 27-30, 2015, Las Vegas, Nevada, pp: 152-156.

Rabin, M.O., 1979. Digitalized signatures and public-key functions as intractable as factorization. Master Thesis, Massachusetts Institute of Technology Cambridge, Massachusetts USA.

Sui, A.F., L.C.K. Hui, S.M. Yiu, K.P. Chow and W.W. Tsang *et al*., 2005. An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication. Proceedings of the IEEE International Conference on Wireless Communications and Networking Vol. 4, March 13-17, 2005, IEEE, New Orleans, Louisiana, USA., pp: 2088-2093.

Williams, H., 1980. A modification of the RSA public-key encryption procedure (Corresp.). IEEE. Trans. Inf. Theory, 26: 726-729.

Xu, J., W.T. Zhu and D.G. Feng, 2011. An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. Comput. Commun., 34: 319-325.