TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 12, No. 10, October 2014, pp. 7353 ~ 7360
DOI: 10.11591/telkomnika.v12i8.5259

A Security Enhanced Password Authentication and Update Scheme Based on Elliptic Curve Cryptography

Hang Tu
School of Mathematics and Statistics, Wuhan University, Wuhan, China 430072
email: tuhang2013@163.com

Abstract

As two fundamental requirements to ensure secure communications over an insecure public network channel, password authentication and update of password have received considerable attention. To satisfy the above two requirements, Islam et al. proposed a password authentication and update scheme based on elliptic curve cryptography. They claimed that their scheme could withstand various attacks. Unfortunately, He et al. found Islam et al.'s scheme is still vulnerable to off-line password guessing attack and stolen-verifier attack. In this paper, a security enhanced scheme is developed to eliminate the identified weaknesses. The analysis shows that our scheme can not only overcome the security vulnerability in Islam et al.'s scheme, but also has better performance than their scheme. Then our scheme is more suitable for practical applications.

Keywords*: password authentication, elliptic curve cryptography, off-line password guessing attack, stolen-verifier attack*

1. Introduction

With the advancement and tremendous development of communication technology, communication networks have brought convenience to people as well as the potential threat of security problems. However, the current communication networks are not yet secure, such that remote servers could be cracked, communication content could be eavesdropped, authentication messages could be modified, and identities could be impersonated. User authentication is the essential security mechanism to overcome the above problems. Due to simplicity and convenience for providing an efficient and accurate way to identify valid remote users, password based authentication scheme has become one of the most promising techniques to secure Internet based applications.

In 1981, Lamport [1] proposed the first password authentication scheme for network communications. However, Lamport's scheme is vulnerable to reply attack and stolen-verifier attack [2]. To improve the security and performance, Peyravian et al. [3] proposed a password authentication and password change schemes using only collision-resistant one-way hash function. However, Lee at el. [4] demonstrated that Peyravian et al.'s scheme [3] suffers from off-line password guessing attack. They also proposed an improved scheme. Unfortunately, Ku et al. [5] pointed out that Lee et al.'s scheme [4] is vulnerable to service attack (DoS), stolen-verifier attack and off-line password guessing attack. In 2004, Yoon et al. [6] proposed an improvement of Lee et al.'s scheme. However, Ku et al. [7] have shown that Yoon et al.'s scheme is vulnerable to off-line guessing attack, stolen-verifier attack and their scheme does not provide forward secrecy. In 2002, Hwang et al. [8] demonstrated that Peyravian et al.'s scheme [3] is vulnerable to password guessing attack, server spoofing attack and data eavesdropping attack. The also proposed an improved scheme using public key cryptosystem. Ku et al. [9] pointed that Hwang et al.'s scheme is vulnerable to the replay attack. Lin et al. [10] also pointed out that Hwang et al.'s scheme[8] suffers from DoS attack and does not provides perfect forward secrecy and afterward proposed. In 2006, Peyravian et al. [11] proposed a security enhanced scheme based on Peyravian et al.'s work [3]. Shim [11] claimed that Peyravian and Jeffries's scheme suffers from off-line password guessing and DoS attacks. In 2006, Chang et al. [13] proposed a new password authentication scheme based on symmetric key cryptosystem. However, application of symmetric key distribution was a burden on the user as the symmetric key exchange is an immense challenge over the unreliable networks.

Received December 1, 2013; Revised July 8, 2014; Accepted July 30, 2014

Recently, Zhu et al. [14] proposed an enhanced scheme to eliminate the weaknesses of Hwang et al.'s scheme, based on public key encryption/decryption with timestamp and salting technique. However, Zhu et al. have the serious clock synchronization problem due to timestamp, and the trusted platform module (TPM) puts a burden on the user.

To improve the system security, many smart card based password authentication schemes have been proposed in the last decays (e.g., [15-22]). However, these solutions tend to still be vulnerable to some sophisticated attacks such as offline password dictionary searching, observing power consumption, and physically exposing the chip to extract the data it stores. Besides, most existing smart card based schemes are vulnerable to stolen/lost smart card attack [23], because some sensitive verifier and secret values stored in the smartcard which can be extracted by monitoring their timing information, power consumption [24] and reverse engineering techniques as mentioned by Kocher et al. [25] and Messerges et al. [26]. Therefore if an adversary steals a smartcard of a legitimate user, he can use it to produce a fabricated login message, and then impersonate as a legal user. In addition, tamper-resistant card readers are not available everywhere [27], the smart card based authentication schemes proposed in [15-22] are not practical for real world.

Very recently, Islam et al.[28] proposed a password authentication and update scheme based on elliptic curve cryptography to satisfy the requirement of applications. However, He et al. [29] pointed out that Islam et al.'s scheme is vulnerable to off-line password guessing attack and stolen-verifier attack. In this paper, we will propose a security enhanced scheme to overcome security weaknesses. The remainder of this paper is organized as follows. Section 2 proposes our improved scheme. The security analysis of the proposed scheme is presented in Section 3. In Section 4, performance and security analysis are presented. Some conclusions are given in Section 5.

2. Our Improved Scheme

Like Islam et al.'s scheme, our scheme also consists of four phases: Registration phase, Password authentication phase, Password change phase and Session key distribution phase. In order to facilitate future references, frequently used notations are listed below with their descriptions.

a) p, n: two large prime numbers;

b) F_p: a finite field;

c) $E(F_p)$: an elliptic curve over F_p defined by the equation $y^2 = x^3 + ax + b$, where $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0$;

d) G: the cyclic additive group consisting of points on $E(F_p)$ and a special point called infinite point;

e) P : a generator point of G with the order n;

f) ID_A: Identity of the user A;

g) pw_A: Secret password of the user A.

h) d_S : Secret key of the server S.

i) U_S : Public key of the server S, where $U_S = d_S \cdot P$.

j) U_A : Password-verifier of the user A, where $U_A = pw_A \cdot P$.

k) K_x: Secret key computed either using $K = pw_A \cdot U_S = (K_x, K_y)$ or $K = d_S \cdot U_A = (K_x, K_y)$.

l) $E_k(\cdot)$: Symmetric encryption (AES) with k.

m) $H(\cdot)$: A collision-resistant one-way secure hash function.

n) r_A / r_S: Random numbers chosen by the user/server from $[1, n-1]$ respectively.

o) $+/-$: Elliptic curve point addition/subtraction.

2.1. Registration Phase

In this phase, everyone who wants to register at the server should submit his identity and password-verifier to the server. The detail of the phase is described as follows.

1) The user A chooses his identity ID_A, password pw_A, computes the password-verifier $U_A = pw_A \cdot P$ and sends ID_A and U_A to the server S.

2) After receiving ID_A and U_A, S computes $V_A = E_x(U_A)$ and stores ID_A, V_A, and a $status-bit$ in a write protected file, where the $status-bit$ indicates the status of the user, i.e., when the user is logged-in to the server the status-bit is set to one, otherwise it is set to zero.

2.2. Password Authentication Phase

Once the user A wants to login to the server S, as shown in Fig. 2, he will perform the following login steps.

1) The user A inputs his identity ID_A and the password pw_A into the terminal. The user selects a random number $r_A \in [1, n-1]$, computes $R_A = r_A \cdot U_S$, $W_A = (r_A + pw_A) \cdot P$ and $h_1 = H(ID_A, R_A, W_A)$. Then A sends the message $M_1 = \{ID_A, W_A, h_1\}$ to S.

2) Upon receiving M_1, S uses its secret key x to decrypt V_A and gets $U_A = pw_A \cdot G$. Then S computes $R'_A = x \cdot (W_A - U_A)$ and verifies whether h_1 and $H(ID_A, R'_A, W_A)$ are equal. If they are not equal, S stops the session. Otherwise, S selects a random number $r_S \in [1, n-1]$, computes $R_S = r_S \cdot P$ and $h_2 = H(ID_A, R'_A, W_A, R_S)$. Then S sends the message $M_2 = \{R_S, h_2\}$ to A.

3) Upon receiving M_2, A checks whether h_2 and $H(ID_A, R_A, W_A, W_S)$ are equal. If they are not equal, A stops the session. Otherwise, A computes $K_A = r_A \cdot R_S = r_A \cdot r_S \cdot P$ and $h_3 = H(ID_A, K_A)$. At last, A sends the message $M_3 = \{h_3\}$ to S.

4) Upon receiving M_3, S computes $K_S = r_S \cdot (W_A - U_A) = r_A \cdot r_S \cdot P$ and checks whether $H(ID_A, K_S)$ and h_3 are equal. If they are not equal, S rejects the user login request. Otherwise, S granted the A's login request.

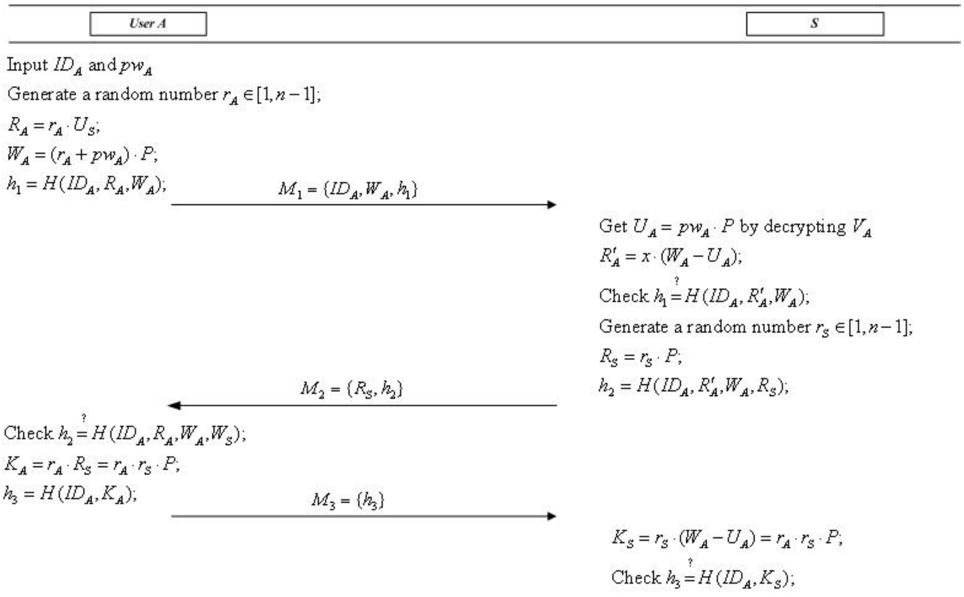
User A
S
Input ID_A and pw_A
Generate a random number $r_A \in [1, n-1]$;
$R_A = r_A \cdot U_S$;
$W_A = (r_A + pw_A) \cdot P$;
$h_1 = H(ID_A, R_A, W_A)$;
$M_1 = \{ID_A, W_A, h_1\}$
Get $U_A = pw_A \cdot P$ by decrypting V_A
$R'_A = x \cdot (W_A - U_A)$;
Check $h_1 \overset{?}{=} H(ID_A, R'_A, W_A)$;
Generate a random number $r_S \in [1, n-1]$;
$R_S = r_S \cdot P$;
$h_2 = H(ID_A, R'_A, W_A, R_S)$;
$M_2 = \{R_S, h_2\}$
Check $h_2 \overset{?}{=} H(ID_A, R_A, W_A, W_S)$;
$K_A = r_A \cdot R_S = r_A \cdot r_S \cdot P$;
$h_3 = H(ID_A, K_A)$;
$M_3 = \{h_3\}$
$K_S = r_S \cdot (W_A - U_A) = r_A \cdot r_S \cdot P$;
Check $h_3 \overset{?}{=} H(ID_A, K_S)$;

Figure 2. Password Authentication Phase of our Scheme

2.3. Password Change Phase

This phase will be invoked if the user wants to change his password from pw_A to pw'_A. The user A and the server S first execute steps 1) and 2) in subsection 2.2. Then the following steps will be executed.

3) Upon receiving M_2, A checks whether h_2 and $H(ID_A, R_A, W_A, W_S)$ are equal. If they are not equal, A stops the session. Otherwise, A inputs the new password pw'_A, computes $U'_A = pw'_A \cdot G$ and $K_A = r_A \cdot R_S = r_A \cdot r_S \cdot P$. At last, A sends $M_3 = \{E_{K_A}(ID_A \| U'_A)\}$ to S.

4) Upon receiving M_3, S computes $K_S = r_S \cdot (W_A - U_A) = r_A \cdot r_S \cdot P$ and uses it to decrypt $E_{K_A}(ID_A \| U'_A)$. Then S checks whether ID_A is included in the decryption result. If it is not included, S rejects the user's request. Otherwise, A accepts the request and replaces V_A with $V'_A = E_x(U'_A)$.

2.4. Session key distribution phase

Once the user A wants to login to the server S and generate a session key for future communication, the phase will be executed. The phase is similar with the password authentication phase described in subsection 5.2. The following two steps are added to 3) and 4) separately to generate the session key.

a) The user computes the final session key as $SK_A = K_A$.

b) The server computes the final session key as $SK_S = K_S$.

3. Security Analysis

The following security properties [30-32]: replay attack, password guessing attack, man-in-the-middle attack, stolen-verifier attack, modification attack, Denning-Sacco attack, mutual authentication, known-key security, session key security, and perfect forward secrecy, must be considered for the proposed scheme.

Theorem 1. Our scheme can resist the replay attacks.

Proof. A replay attack is an offensive action in which an adversary impersonates or deceives another legitimate participant through the reuse of information obtained in a scheme [30, 31]. Suppose an adversary A intercepts $M_1 = \{ID_A, W_A, h_1\}$ from A in Step (1) and replays it to impersonate A, where $R_A = r_A \cdot U_S$, $W_A = (r_A + pw_A) \cdot P$ and $h_1 = H(ID_A, R_A, W_A)$. However, A cannot compute a correct $h_3 = H(ID_A, K_A)$ and deliver it to S in Step (3) unless she can correctly guess password pw_A to obtain $r_A \cdot P$ and guess the right r_A from $r_A \cdot P$. When A tries to guess r_A from $r_A \cdot P$ or r_B from $r_B \cdot P$, she will face the DLP. On the other hand, suppose A intercepts $M_2 = \{R_S, h_2\}$ from S in Step (2) and replays it in order to impersonate A. For the same reason, if A cannot gain the correct r_A from $W_A = (r_A + pw_A) \cdot P$, A will find out that h_2 is not equivalent to his/her computed $H(ID_A, R_A, W_A, W_S)$. Then, A will not send $M_3 = \{h_3\}$ back to A in Step (3). Therefore, the proposed scheme can resist against the replay attacks.

Theorem 2. Our scheme can resist the password guessing attacks

Proof. A guessing attack involves an adversary –randomly or systematically trying long-term private keys (e.g., user passwords or server secret keys) one at a time, in a hope of finding the correct private key. Ensuring that long-term private keys are chosen from a sufficiently large space helps resist against exhaustive searches. Most users, however, select passwords from a small subset of the full password space. Such weak passwords with a low entropy are easily guessed by using so-called dictionary attacks [31].

An on-line password guessing attack cannot succeed, since S can choose appropriate trail intervals. On the other hand, in an off-line password guessing attack, the adversary A can try to find a weak password by repeatedly guessing possible passwords and verifying the correctness of the guesses based on information obtained in an off-line manner. In our scheme, A can gain knowledge of $M_1 = \{ID_A, W_A, h_1\}$, $M_2 = \{R_S, h_2\}$ and $M_3 = \{h_3\}$ in Steps (1), (2), and (3), respectively. In order to obtain the password pw_A of A; A first guesses password pw'_A and then computes $r'_A \cdot P = W_A - pw'_A \cdot P$. By using $r'_A \cdot P$ and $R_S = r_S \cdot P$, A will try to compute the session key $r'_A r_S P$. However, A has to break the CDHP to find the keying material $r'_A r_S P$ from $r'_A \cdot P$ and $r_S \cdot P$ to verify her guess.

Therefore, the proposed scheme can resist against the password guessing attacks.

Theorem 3. Our scheme can resist the man-in-the-middle attacks.

Proof. The man-in-the-middle attack is a form of active eavesdropping in which the adversary makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection where in fact the entire conversation is controlled by the adversary [31, 32]. A mutual password pw_A between A and S is used to prevent the man-in-the-middle attacks. The illegal adversary Eve cannot pretend to be A or S to authenticate since she does not own the mutual password pw_A. Therefore, the proposed scheme can resist against the man-in-the-middle attacks.

Theorem 4. Our scheme can withstand the stolen-verifier attack.

Proof: The stolen-verifier attack means that an adversary who steals the password verifier from S can use it directly to masquerade as a legitimate user in a user authentication process [31, 32]. Servers are always the target of attacks. The attacker A may acquire $V_A = E_x(U_A)$ stored in S. However, without knowing S's secret key x; A cannot forge a login request to pass the authentication, as U_A is hidden in $E_x(U_A)$ using S's secret key x, and thus the correctness of the guessed password pw'_A cannot be verified even if he is a legal user. Therefore, the proposed scheme can resist against the stolen-verifier attacks.

Theorem 5. Our scheme can resist the modification attacks.

Proof. A modification attack is an attempt by an adversary to modify information in an unauthorized manner. This is an attack against the integrity of the information[31]. The adversary A may modify the communication messages $M_1 = \{ID_A, W_A, h_1\}$, $M_2 = \{R_S, h_2\}$ and $M_3 = \{h_3\}$ being transmitted over an insecure network. However, although A can modify them, the proposed scheme can detect this modification attack, because it can verify not only the equality of $r_A r_S P$ computed by each party, but also the correctness of $M_1 = \{ID_A, W_A, h_1\}$ and $M_2 = \{R_S, h_2\}$ transmitted between two parties, by validating h_2 and h_3 in the proposed scheme. Therefore, the proposed scheme can resist against the modification attacks.

Theorem 6. Our scheme can resist the Denning-Sacco attacks.

Proof. The Dennig-Sacco attack works where an attacker compromises an old session key and tries to find a long-term private key (e.g., user password or server private key) or other session keys[30]. Although an adversary A can obtain the fresh session key $sk = r_A r_S P$, A cannot obtain the secret password S from $W_A = (r_A + pw_A) \cdot P$ because A will face the DLP to obtain r_A from $r_A r_S P$. Therefore, the proposed scheme can resist against the Denning-Sacco attacks.

Theorem 7. Our scheme can provide mutual authentication.

Proof. Mutual authentication means that both user and server are authenticated to each other within the same scheme [31, 32]. It is easy to say that there is no one could compute a valid h_2 without the knowledge pw_A and the secret key x, since he has to compute $R'_A = x \cdot (W_A - U_A) = x \cdot r_A \cdot P$ from $W_A = (r_A + pw_A) \cdot P$, $U_S = x \cdot P$ and will face to CDHP. Then user A could authenticate S by checking the volatility of h_2. We also know that there is no once can compute $K_A = r_A \cdot R_S = r_A \cdot r_S \cdot P$ from $W_A = (r_A + pw_A) \cdot P$ and $R_S = r_S \cdot P$ without the knowledge pw_A and random number r_A. Then S could authenticate A be checking the validity of h_3. Therefore, the proposed scheme can provide mutual authentication.

Theorem 8. Our scheme can provide known-key security.

Proof. Known-key security means that each run of an authentication and key agreement scheme between two communication entities (the user and the server) should produce unique secret keys; such keys are called session keys[30]. Knowing a session key $sk = r_A r_S P$ and the random values r_A and r_S are useless for computing the other session keys $sk' = r'_A r'_S P$, since without knowing r'_A and r'_S it is impossible to compute the session key sk'. Therefore, the proposed scheme provides the known-key security.

Theorem 9. Our scheme can provide session key security.

Proof. Session key security means that at the end of the key exchange, the session key is not known by anyone but only the two communication entities (the user and the server)[31, 32]. The session key $sk = r_A r_S P$ is not known by anyone but only A and S since the random values r_A and r_S are protected by the DLP and the secure one-way hash function. Nothing about this session key $sk = r_A r_S P$ is known to anybody but A and S. Therefore, the proposed scheme provides the session key security.

Theorem 10. Our scheme can provide perfect forward secrecy.

Proof. Perfect forward secrecy means that if a long-term private key (e.g., password) is compromised, this does not compromise any earlier session keys [30, 31]. If the password pw_A shared between A and S is compromised, it does not allow an adversary A to determine the session key $sk = r_A r_S P$ for the past sessions and decrypt them, since A still faces the CDHP to compute the session key $r_A r_S P$ from the two extracted values $r_A P$ and $r_S P$. Therefore, the proposed scheme satisfies the property of perfect forward secrecy.

4. Security and Performance Comparison

To the best of our knowledge, Islam et al.'s scheme [28] is superior to previously proposed schemes [3-14], then we will just compare our scheme with Islam et al.'s scheme here. It is necessary to the user and the server to generate session key for future communication, then we compare the performance of the session key distribution phase. Table 1 and Table 2 show the security and performance comparison between our scheme and Islam et al.'s scheme, respectively.

From Table 1, we know that Islam et al.'s scheme is vulnerable to password guessing attack and stolen-verifier attack. Then our enhanced scheme is superior to Islam et al.'s scheme [28] by supporting all security requirements. It is well known that point addition, hash operation and en/decryption operation may be ignored compared with pairings operation and scalar multiplication. Besides, pairings operation is more complicated than scalar multiplication. Then we can conclude that our scheme have better performance Islam et al.'s scheme. Then our scheme is more suitable for practical applications.

Table 1. Security Comparison

	Islam et al.'s scheme[28]	Our scheme
Resistance to replay attack	√	√
Resistance to password guessing attack	×	√
Resistance to man-in-the-middle attack	√	√
Resistance to stolen-verifier attack	×	√
Resistance to modification attack	√	√
Resistance to Denning-Sacco attack	√	√
Mutual authentication	√	√
Known-key security	√	√
Session key security	√	√
Perfect forward secrecy	√	√

Table 2. Performance Comparison

	Islam et al.'s scheme[28]		Our scheme	
Communication entity	*A*	*S*	*A*	*S*
Pairings operation	0	2	0	0
Scalar multiplication	4	3	3	3
Point addition	1	1	1	1
Hash operation	2	2	3	3
En/decryption operation	1	1	0	0

5. Conclusion

In this paper, we have proposed an improved scheme that addresses the known security problems. Compared with Islam et al.'s scheme, the proposed scheme overcomes the security weaknesses and has better performance. Therefore, the proposed scheme is well suited to the practical applications environment.

References

[1] L Lamport. Password Authentication with Insecure Communication. Communications of the ACM. 1981; 24(11): 770-772.

[2] MS Hwang, LH Li. A new remote user authentication scheme using smart cards. *IEEE Transactions* on *Consumer Electronics.* 2000; 46(1): 28–30.

[3] M Peyravian, N Zunic. Methods for protecting password transmission. *Computers & Security*. 2000; 19(5): 466-469.

[4] CC Lee, LH Li, MS Hwang. *A remote user authentication scheme using hash functions.* ACM Operating Systems Review. 2002; 36(4): 23-29.

[5] WC Ku, CM Chen, HL Lee. Weaknesses of Lee-Li-Hwang's Hash-based password authentication scheme. *ACM Operating Systems Review.* 2003; 37(4): 19–25.

[6] EJ Yoon, EK Ruy, KY Roo. A secure user authentication scheme using hash functions. *ACM Operating Systems Review*. 2004; 38(2): 62-68.

[7] WC Ku, MH Chaing, ST Chang. Weaknesses of Yoon-Ryu-Yoo's hash-based password authentication scheme, *ACM Operating Systems Review.* 2005; 39(1): 85-89.

[8] JJ Hwang, TC Yeh. Improvement on Peyravian-Zunics Password Authentication Schemes. *IEICE Transactions on Communications*. 2002; E85-B(4); 823–825.

[9] WC Ku, CM Chen, L Hui. Cryptanalysis of a Variant of Peyravian-zunic's Password Authentication Scheme. *IEICE Transactions on Communications.* 2002; E86-B(5): 1682-1684.

[10] CL Lin, T Hwang. A password authentication scheme with secure password updating. *Computers & Security.* 2003; 22(1): 68-72.

[11] M Peyravian, C Jeffries. Secure Remote User Access over Insecure Networks. *Computer Communications*. 2006; 29(5): 660-667.

[12] KA Shim, Security flaws of remote user access over insecure networks. *Computer communications.* 2006; 30(1): 117-121.

[13] YF Chang, CC Chang, YL Liu, Password Authentication without the Server Public Key*. IEICE Transactions on Communications*. 2004; E87-B(10): 3088-3091.

[14] L Zhu, S Yu, X Zhang. Improvement upon Mutual Password Authentication Scheme. *International seminar on Business and Information Management*. 2008; 400-403.

[15] ZH Shen. A new modified remote user authentication scheme using smartcards. *Applied Mathematics.* 2008; 23(3): 371-376.

[16] YL Jia, AM Jhou, MX Gao, A new mutual authentication scheme based on nonce and smartcards. *Computer Communications*. 2008; 31(10): 2205-2209.

[17] WS Juang, WK Nien. Efficient password authenticated key agreement using bilinear pairings. Mathematical and Computer Modelling. 2008; 47(11-12): 1238-1245.

[18] SK Kim, MG Chung. More secure remote user authentication scheme. *Computer Communication.* 2009; 32(6): 1018-1021.

[19] J Xu, WT Zhu, DG Feng, An improved smart card based password authentication scheme with provable security. *Computer Standards & Interfaces*. 2009; 31(4): 723-728.

[20] M Kumar. An enhanced remote user authentication scheme with smart card. *International Journal of Network Security*. 2010; 10(3); 175-184.

[21] CT Li, MS Hwang. An efficient biometrics-based remote user authentication scheme using smart cards*. Journal of Network and Computer Applications*. 2010; 33(1): 1-5.

[22] X.M. Wang, W.F. Zhang, J.S. Zhang, M.K. Khan, Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards, Computer Standards & Interfaces 29 (2007) 507–512.

[23] Y Chen, JS Chou, CH Huang. Comments on five smart card based password authentication schemes*. International Journal of Computer Science and Information Security.* 2010; 8(2): 129-132.

[24] M Joye, F Olivier. Side-channel analysis, Encyclopedia of Cryptography and Security. Kluwer Academic Publishers. 2005; 571-576.

[25] P Kocher, J Jaffe, B Jun. *Differential power analysis*. Proceedings of Advances in Cryptology-Crypto'99, LNCS, 1999: 388-397.

[26] TS Messerges, EA Dabbish, RH Sloan. Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*. 2002; 51(5): 541-552.

[27] JS Lee, YF Chang, CC Chang. A novel authentication scheme for multi-server architecture without smart cards, International *Journal of Innovative Computing, Information and Control*. 2008; 4(6): 1357-1364.

[28] SK Hafizul Islam, GP Biswas. Design of improved password authentication and update scheme based on elliptic curve cryptography. *Mathematical and Computer Modelling*. 2013; 57(11-12): 2703–2717.

[29] D He, S Wu, J Chen. Note on 'Design of improved password authentication and update scheme based on elliptic curve cryptography. Mathematical and Computer Modelling. 2012; 55(3-4): 1661–1664.

[30] D Denning, G Sacco. Timestamps in key distribution systems. *Communications of the ACM.* 1981; 24; 533–536.

[31] AJ Menezes, PC Oorschot, SA Vanstone, Handbook of Applied Cryptograph, CRC Press, New York, 1997.

[32] EJ Yoon, WH Kim, KY Yoo. Robust and simple authentication scheme for secure communication on the web. ICWE 2005. *Lecture Notes in Computer Science*, Springer-Verlag. 2005; 3579: 352–362.