Mutual SIP Authentication Scheme Based on ECC

Samaneh Sadat Mousavi Nik and Mehdi Shahrabi

***Abstract*—Session Initial Protocol (SIP) has received much attention and increasingly used for administrating Voice over IP (VoIP) phone calls and in current Internet protocols such as Hyper Text Transport Protocol (HTTP) and Simple Mail Transport Protocol (SMTP) as a signaling protocol. SIP is a based on HTTP to establish multimedia sessions in both wire line and wireless world. But the authentication mechanism proposed in SIP is based on HTTP Digest authentication that this scheme vulnerable against some attacks, such as off-line password guessing attacks, replay attacks, impersonate attacks and etc. So, many researches proposed various schemes to secure the SIP authentication. In the year 2012, Tang *et al.* proposed a SIP authentication using elliptic curve cryptography (ECC), but their scheme is insecure against off-line password guessing and DoS attacks. We proposed an ECC-based authentication scheme for SIP to overcome such security problems and analysis of security of the ECC-based protocol indicates that our scheme is appropriate for the applications with higher security requirement.**

***Index Terms*—SIP, elliptic curve cryptography, authentication, vulnerability, security, mutual.**

I. Introduction

Session Initiation Protocol (SIP) proposed by Internet Engineering Task Force (IETF) in 1999, for the IP-based telephony [1], [2]. SIP is a text based protocol that can be used for controlling multimedia communication sessions such as voice and video calls over Internet protocols such as Hyper Text Transport Protocol (HTTP) and Simple Mail Transport Protocol (SMTP) [3] also SIP is the one important protocol because of the widespread application of the voice over IP (VoIP) in the Internet so the security of SIP is becoming too important [4].

SIP is a request-response protocol when a user wants to access a SIP service, at the first she/he has to authenticate with SIP server but the original authentication scheme for SIP doesn't provide enough security because it's based on HTTP Digest authentication noted in RFC2617 [5].

To overcome these vulnerabilities, different SIP authentication schemes have been proposed, especially based on Elliptic curve cryptography (ECC). In 2005,Yang *et al.* found that the original SIP authentication scheme was vulnerable to off-line password guessing attack and server-spoofing attack [6] so they proposed scheme was based on Diffie-Hellman key exchange algorithm [7], which depended on the difficulty of Discrete Logarithm Problem (DLP) [8] but Yang *et al.*'s scheme was vulnerable to stolen-verifier attack, off-line password guessing attack, and Denning-Sacco attack [9] and Their scheme was high computation cost [10]-[12]. In the same year, based on Yang *et al.*'s scheme, Durlanik *et al.* [10] introduced another SIP authentication by using Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm but this scheme in comparison with Yang *et al.*'s scheme reduced the execution time and memory requirements. However, their scheme still vulnerability from off- line dictionary attack and Denning-Sacco attack [13]. In 2008, Tsai [12] proposed SIP authentication scheme based on random nonce. In this scheme all the communication messages were computed with one-way hash function and exclusive-or operation so computation cost reduce highly. But this scheme vulnerable to off-line password guessing, Denning-Sacco and stolen-verifier attacks; furthermore, it did not provide any key agreement, known-key secrecy and perfect forward secrecy (PFS) [14]-[17]. In 2009, Wu *et al.* [18] suggested an SIP authentication scheme based on elliptic curve cryptography (ECC). This scheme achieves authentication and a shared secrecy at the same time. Wu *et al.*'s scheme provides provable security in the Canetti–Krawczyk (CK) security model [19] and it's suitable for applications that require low memory and rapid transactions. But Wu *et al.*'s SIP authentication schemes are still vulnerable to off-line password guessing attacks, Denning-Sacco attacks, and stolen-verifier attacks [8], [16]. In 2009, Yoon *et al.* proposed another authentication for SIP using ECC in [17]. Unfortunately, the scheme was vulnerable to password guessing attack and stolen-verifier attack. The attack method could be referred to [20]. In 2010, Yoon *et al.* proposed the third and fourth ECC-based authentication scheme for SIP [21], [22]. But these schemes were vulnerable to offline password guessing and stolen-verifier attacks [20]. In 2011, Arshad *et al.* proposed SIP authentication scheme based on ECC [14]. But Arshad *et al.*'s authentication scheme was vulnerable to off-line password guessing attack [23]. In 2012, Tang *et al.* proposed a secure and efficient authentication scheme based on Elliptic Curve Discrete Logarithm Problem (ECDLP) for SIP. In this paper, we demonstrate the Tang *et al.*'s authentication scheme vulnerable to off-line password guessing attack and DoS attack by using modification attack and registration attack and then propose a secure SIP authentication scheme based on ECC in order to solve those security problems. The proposed SIP authentication scheme can provide high security and executes faster than previously proposed schemes.

The remainder of this paper is outlined as follows. Section II reviews the original SIP authentication procedure. Section III introduces of Tang *et al.*'s scheme and discusses attack on

Manuscript received August 29, 2013; revised November 25, 2013.

Samaneh Sadat Mousavi Nik is with Payam Noor University, Mashhad. She was with the Department of Engineering , Security in Information Technology, University of Tehran Kish International Campus, Iran (Corresponding Author, e-mail: samaneh_mousavi@alumni.ut.ac.ir),

Mehdi Shahrabi is with the Department of Engineering, Amirkabir University of Technology- Tehran Polytechnic (e-mail: mshahrabi@aut.ac.ir)

it and in Section IV proposed ECC-based mutual authentication scheme for SIP is presented. In Section V discuss the security and efficiency of the proposed scheme, In Section VI, evaluate the performance of the proposed scheme. And Section VII is the conclusion.

II. SIP Authentication Procedure

The common authentication scheme for SIP is Digest Access Authentication (DAA) [5].

DAA security is based on the challenge-response pattern [6]. Client pre-shares a password with the server before the authentication procedure starts. Fig. 1 shows procedure of the DAA mechanism in SIP.

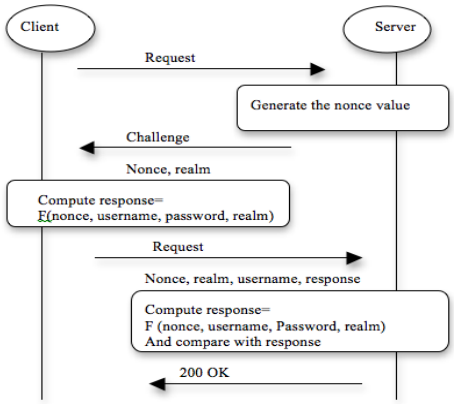

Fig. 1. The SIP digest access authentication method during a SIP REGISTER transaction.

III. SIP Authentication Scheme by Tang *et al.*

This section reviews Tang *et al.*'s SIP authentication scheme [23]. Then shows that the scheme is vulnerable to off-line password guessing and Dos attacks. Tang *et al.*'s scheme consists of four phases: system setup phase, registration phase, login and authentication phase, and password change phase.

A. Tang et al.'s Scheme

Tang *et al.* propose an enhanced ECC-based SIP authentication scheme in order to strength Arshad *et al.*'s scheme. Notations used in this paper are defined in Table I.

TABLE I: Notations and Their Explanations[23]

Ui , U :	the ith user or user
IDi , username:	the identity of user Ui
PWi:	Password of user
S:	the remote server
Ks:	the secret key of the server
SK:	a session key
Q = Ks.P:	the public key of the server
h(.):	a strong cryptographic one-way hash function
H(.):	a function which makes a point map to another point on elliptic curve
ll:	the string concatenation operation
⊕:	the exclusive-or operation
⇒:	a secure channel
→:	a common channel
A?=B:	compares whether A equals B
D:	a uniformly distributed dictionary of size lDl

1) System setup phase

First the members and the server agree on the EC parameters Then server selects a secret key Ks, computes $Q = Ks.P$ and keeps secret Ks and publishes p, a, b, P, n, h, Q [23].

2) Registration phase

In this phase:

- The user chooses his or her identity ID_i and password PW_i, then through a pre-established secure channel, such as Virtual Private Network (VPN) or Secure Sockets Layer (SSL) sends them to the server.
- The server computes $V_i = h(ID_i \| Ks) \oplus PW_i$ and stores (ID_i, V_i) in its database.

3) Login and authentication phase

Fig. 2 illustrates Tang *et al.*'s SIP authentication scheme. When a legal SIP client *U* wants to login the SIP server *S*, the authentication scheme between *U* and *S* proceeds as follows.

4) Password change phase

In this phase user can change his or her password. Fig. 3 shows the password change phase.

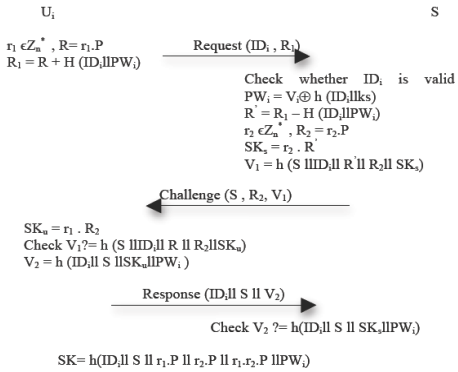

Fig. 2. Login and authentication phase[23]

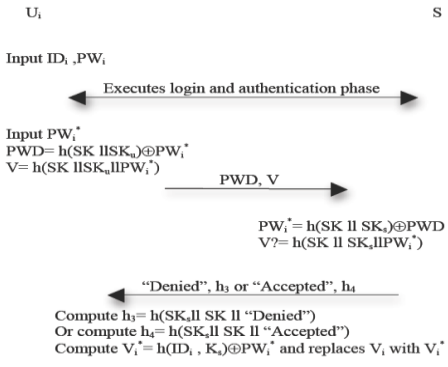

Fig. 3. Password change phase[23]

B. Attacks on Tang et al.'s Scheme

In this section, we will show that Tang *et al.*'s scheme is vulnerable to off-line password guessing attack and DoS attack.

1) Scenario one: off-line password guessing attack

Off-line password guessing attack works when an attacker tries to find a long-term private key (pw) of *Ui*. In Tang *et al.*'s SIP authentication scheme, the off-line password guessing attack is possible.

- An attacker records Tang *et al.*'s SIP authentication scheme between the SIP client and the server (use R_1, R_2 and V_2 values).
- By performing the following can run off-line password guessing attack.

1) An attacker selects a candidate password PWi* from the password dictionary *D*.

2) Attacker Calculate H (ID$_i$llPW$_i^*$) then $R_1^{'}$ =R_1 – H ($ID_i llPW_i^*$) = R + H ($ID_i llPW_i$) – H ($ID_i llPW_i^*$) output of this step is R.

3) Attacker computes Sku* = $r_1.R_2$ and V_2^* = h (ID_i*ll S llsk*$_u^*$ llpw$_i^*$)

4) Finally compares V_2* with V_2. If they are equal, attacker guesses the correct password of U. If not, the attacker repeats the above process until V_2* = V_2.

2) Scenario two: DoS attack

DoS attacks, implement by registration attacks and modification attacks.

a) Registration attacks:

During the SIP REGISTER handshake between the UA and the SIP server, authentication process is performed. In this section indicate the shortcomings of Tang *et al*.'s scheme authentication and recommend which value it requires to be protected.

During the authentication, UA's IP-address is sent in clear and is not protected by Tang *et al*.'s scheme authentication. Therefore an attacker can modify the hostname or IP-address in real-time using NetSED (see Fig. 4). NetSED, modifies network packets in real time based on a regular expression. Then UA's phone number with the attackers IP address is registered. So After a successful authentication, the attacker's hostname or IP-address is registered in the SIP server. Therefore all requests to the valid UA will be diverted to a hostname or IP-address set by an attacker. Finally, a valid user is unreachable and server will not detect that anything is wrong, so when server receives a call to valid UA, the call will be forwarded to the attackers registered IP address.

b) Modification attacks

When SIP is deployed by underling cryptographic protection mechanism like Tang *et al*.'s scheme authentication, implemented the typical man in the middle and impersonation attacks between a caller and server are difficult. But in Tang *et al*.'s scheme authentication mechanism, there isn't any protection in the final phase (see Fig. 4) so after successful authentication when server wants to send 200 OK to the UA the attacker able to modify this message to Busy. The attacker can fraud UA and UA imagine that the registration process was unsuccessful.

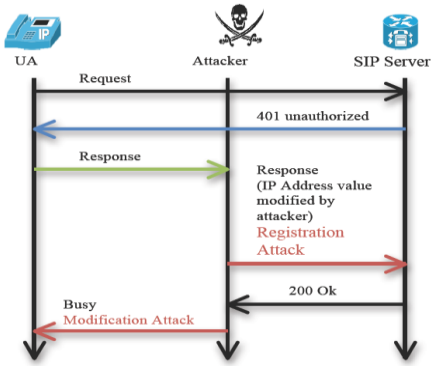

Fig. 4. DoS attack

IV. Proposed SIP Authentication Scheme

We propose a new secure SIP authentication scheme based on elliptic curve cryptography (ECC) to overcome the security problems. This scheme is in order to Tang *et al*.'s scheme.

The proposed scheme exploits speed and security jointly. The proposed scheme consists of four phases: system setup phase, registration phase, login and authentication phase, and password change phase.

A. System Setup Phase

U and S agree on the EC parameters. The server selects a secret key Ks, computes Q = Ks .P, keeps secret Ks and publishes p, a, b, P, n, h, Q.

B. Registration Phase

In this phase:

- The user chooses his or her identity ID_i and password PW$_i$, then through a pre-established secure channel, such as Virtual Private Network (VPN) or Secure Sockets Layer (SSL) sends them to the server.
- The server computes V_i = h ($ID_i llKs$)⊕PW_i and stores (ID_i, V_i) in its database.

This phase is the same Tang *et al*.'s scheme.

C. Login and Authentication Phase

When a legal SIP client U wants to login the SIP server S, the authentication scheme between U and S proceeds. We indicated that Tang *et al*.'s scheme is vulnerable to off-line password guessing attack, registration attack and modification attack for overcome these security problems, Fig. 5 illustrates the new proposed SIP authentication scheme.

1) U_i→ S: REQUEST (ID_i,IP_i, R_1)

U_i selects a random nonce r$_1$ ϵ Z$_n^*$ then computes R = r_1 . P, R_1= R + H(IP$_i$llPW$_i$). And then sends message REQUEST (ID_i ,IP_i , R_1) to the server S.

2) S →U_i: CHALLENGE (S, R_2^*)

First S checks ID_i is exist in database. If yes, S computes PW_i= V_i⊕h($ID_i llKs$), $R^{'}$= R_1 - H($IP_i llPW_i$) = r_1 . P. And then S selects a random nonce r$_2$ ϵ Z$_n^*$, computes R_2 = r_2. P,

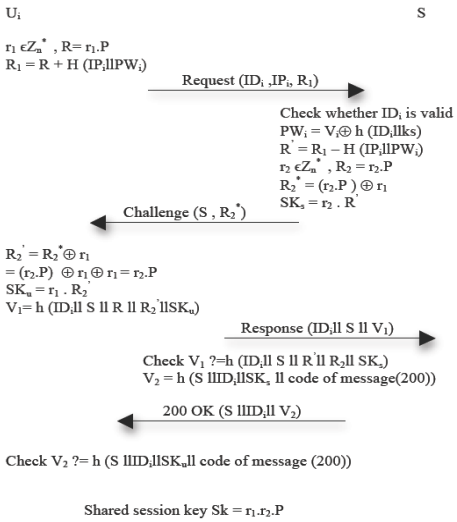

Fig. 5. Proposed Login and authentication phase

R_2^* = (r_2.P) ⊕ r_1 , SK_S = r_2 . $R^{'}$= r_1 .r_2. P, and sends CHALLENGE (S , R_2^*)to U_i.

3) U_i→ S : RESPONSE (ID_ill S ll V_1)

U_i computes $R_2^{'}$ = R_2^*⊕ r_1 = (r_2.P) ⊕ r_1⊕ r_1 = r_2.P ,SK_u = r_1.$R_2^{'}$,V_1= h ($ID_i ll$ S ll R ll $R_2^{'}$llSK_u) and sends RESPONSE ($ID_i ll$ S ll V_1) to server.

4) S →U_i : 200 Ok (S llID$_i$ll V_2)

Upon receiving the response message, *S* checks V_1 is equal to h(ID$_i$ll S ll R$_2$ll SK$_s$).If the result is equal S authenticates the identity of U_i . Then *S* computes $V_2 = h$ (S llID$_i$llSK$_s$ ll code of message(200)) and sends message 200 OK (*S llID$_i$ll* V_2) To U_i.

5) When U_i received 200 OK message, U_i checks V_2 is equal to h (S llID$_i$llSK$_u$ll code of message (200)). If the result is equal U_i authenticates the identity of S.

Shared session key $Sk = r_1.r_2.P$

D. Password Change Phase

In this phase user can change his or her password. Fig. 3 shows the password change phase. This phase is the same Tang *et al*.'s scheme.

V. Security Analysis

This section analyzes a security of the proposed SIP authentication scheme.

A. Password Guessing Attacks

Off-line password guessing attack: If Eve try to find a *PW* by gain information in an off-line manner cannot success because In our scheme, all knowledge Eve can gain are $R_1 = R + H(IP_i llPW_i)$, $R_2^* = (r_2.P) \oplus r_1$, V_1 and V_2 . Therefore if Eve guessing possible password and computes $H(IP_i ll\ PW)$, it doesn't have any information to compare the guess password is correct or not and also Eve cannot compute SK because it's difficult Eve breaks the ECDLP and ECDHP, in addition both r_1 and r_2 values are protected too (see R_1 and R_2^*).

On-line password guessing attack: The secret key K_s is a high entropy number and cannot be guessed by anyone so Eve cannot make a successful guess of the right password from V_i. Therefore, the proposed scheme can resist against the password guessing attacks.

B. Replay Attacks

The proposed scheme can resist the replay attacks. If an attacker replays REQUEST to impersonate *U* in Step (1), in Step (3), Eve cannot compute a correct session key sk and deliver it to *S*. On the other hand if an attacker replays CHALLENGE to impersonate *S* in step (2), Eve cannot compute message 200 OK in step (4) and deliver it to *U* so the proposed scheme can resist against the replay attacks.

C. Man-in-the-Middle Attacks

The proposed scheme can resist against the man-in-the-middle attacks because this scheme based on mutual authentication and PW$_i$ of U_i and the secret key K_s of *S* are used to prevent the man-in-middle attack.

D. Stolen-Verifier Attacks

The proposed scheme can resist against the stolen-verifier attacks because server computes $V_i = h(ID_i llK_S) \oplus PW_i$ and stores (ID_i, V_i) in its database so if attacker Eve steals verifier from the database of the server ,Eve cannot make a successful guess of the right password from *Vi* .because K_s is a high entropy number.

E. Impersonation Attacks

The proposed scheme can resist against the impersonation attacks. In this scheme attacker Eve cannot masquerade as server because doesn't have K_s and on the other hand Eve cannot masquerade as *U* because doesn't have knowledge about PW.

F. Modification Attacks

The proposed scheme can resist against the modification attacks. In this scheme all steps carry information related authentication so if attacker Eve modify these messages when U and S check the correction of the receive message they can detect the modification of message so reject the message.

G. Denning-Sacco Attacks

The proposed scheme can resist against Denning-Sacco attacks. Assume that attacker Eve may find fresh session key SK for some reasons. But Eve cannot detect PW$_i$ and server's secret key K$_s$ because SK= r$_1$.r$_2$.P and it's ECDHP so Eve cannot compute.

H. Registration Attacks

The proposed scheme can resist against registration attacks. In our scheme by hashing IP address of U_i in phase (1), we protected this value.

I. Known-Key Security

Our scheme provides Known-key security, means that during authentication between U_i and *S*, they should produce unique secret session key by random values $r_1$and r_2.

J. Session KEY Security

Our scheme provides session key security because of ECDLP, ECDHP and secure one-way hash function therefore just U_i and S can compute the session key at the end of the key exchange.

K. Perfect Forward Secrecy

Our scheme provides PFS means that, if long-term private keys such as user's password PW_i and secret key K_s of server are compromised, there isn't any effect on the secrecy of previous session keys. Because of ECDHP and attacker Eve cannot compute $Sk = \alpha\beta P$ from R_1 and R_2^*.

L. Mutual Authentication

Our scheme provides mutual authentication means that during authentication mechanism both the user and the server are authenticated each other.

The security properties of the previously reported schemes [6], [10], [12], [14], [21], [23] and the proposed scheme are summarized in Table II.

VI. Performance Comparisons

The computation costs of our proposed scheme and the previously schemes [6], [10], [12], [14], [21], [23] are shown in Table III. The proposed SIP authentication scheme requires four PM (elliptic curve scale multiplication), two HP (hash-to-point function), two PA (point addition) and five H (hash function operations) during the protocol execution. Our proposed scheme is efficient authentication schemes for Session Initiation Protocol.

The proposed SIP authentication scheme requires elliptic curve scale multiplication computations and hash-to-point operations to resist the password guessing attack and provide known-key secrecy and PFS.

TABLE II: COMPARISONS OF THE SECURITY PROPERTIES OF DIFFERENT SCHEMES

	Durlanik[10]	Yang [6]	Tsai [12]	Yoon [21]	Arshad [14]	Tang[23]	Ours
Impersonation attack	Insecure	Insecure	Insecure	Secure	Insecure	Secure	Secure
Password guessing attack	Insecure	Insecure	Insecure	Insecure	Insecure	Insecure	Secure
Denning Sacco attack	Insecure	Insecure	Insecure	Secure	Secure	Secure	Secure
Stolen-verifier attack	Not applicable	Insecure	Insecure	Insecure	Secure	Secure	Secure
Registration attack	Insecure	Insecure	Insecure	Insecure	Insecure	Insecure	Secure
Mutual authentication	Provided	Provided	Provided	Provided	Provided	Provided	Provided
Session key security	Provided	Not applicable	Provided	Provided	Provided	Provided	Provided
Known key secrecy	Provided	Not applicable	Not provided	Provided	Provided	Provided	Provided
Perfect forward secrecy	Provided	Not applicable	Not provided	Provided	Provided	Provided	Provided

TABLE III: COMPARISON OF COMPUTATION

	Durlanik[10]	Yang [6]	Tsai [12]	Yoon [21]	Arshad [14]	Tang [23]	Ours
Exponentiation	**0**	**4**	**0**	**0**	**0**	**0**	**0**
Scale multiplication	**4**	**0**	**0**	**6**	**5**	**4**	**4**
Point addition	**0**	**0**	**0**	**3**	**0**	**2**	**2**
Hash-to-point	**0**	**0**	**0**	**0**	**0**	**2**	**2**
Hash function	**6**	**8**	**7**	**4**	**8**	**7**	**5**
Exclusive or	**4**	**4**	**3**	**0**	**2**	**1**	**3**
Security	ECDLP	DLP	HASH	ECDLP	ECDLP	ECDLP	ECDLP

VII. CONCLUSIONS

This paper indicates the vulnerabilities of Tang *et al*.'s authentication schemes for session initiation protocol (SIP) to off-line password guessing attacks, registration attacks and modification attacks. In order to resolve the shortcomings in their scheme, we proposed a new secure and efficient SIP authentication scheme. Our scheme based on ECC, resists the mentioned attacks and needs to compute four elliptic curve scale multiplications and two hash-to-point function operations during a protocol run so by using this method can decrease computational time for authentication phase in SIP. At the end, our scheme maintains high efficiency compared with previous ECC-based authentication schemes but it's essential to generate new method with low computational time for portal device such as mobile.

REFERENCES

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnstone, J. Peterson, and R. Sparks, *SIP: Session Initiation Protocol*, IETF, 2002.

[2] M. Thomas, *SIP Security Requirements*, IETF Internet Draft, 2001.

[3] L. Veltri, S. Salsano and D. Papalilo, "SIP security issues: the SIP authentication procedure and its processing load," *IEEE Netw*., vol. 16, pp. 6, pp. 38–44, 2002.

[4] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, and S. Ehlert, "Survey of security vulnerabilities in session initiation protocol," *IEEE Commun. Surv. Tutorials*., vol. 8, no. 3, pp. 68–81, 2006.

[5] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, "HTTP authentication: basic and digest access authentication," IETF RFC2617, 1999.

[6] C. C. Yang, R. C. Wang and W. T. Liu, "Secure authentication scheme for session initiation protocol," *Comput Secur*., vol. 24, pp. 381–386, 2005.

[7] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644–654, 1976.

[8] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptograph*, CRC Press, 1997.

[9] D. Denning and G. Sacco, "Timestamps in key distribution systems," *Commun ACM*, vol. 24, pp. 533–536, 1981.

[10] A. Durlanik and I. Sogukpinar, "SIP Authentication Scheme using ECDH," *World Academy of Science, Engineering and Technology*, vol. 8, pp. 350–353, 2005.

[11] D. B. He, J. H. Chen, and R. Zhang, "A more secure authentication scheme for telecare medicine information systems," *J. Med Syst.*, vol. 36, issue 3, pp. 1989-1995, 2011.

[12] J. L. Tsai, "Efficient nonce-based authentication scheme for session initiation protocol," *Int J NetwSecur*., vol. 8, no. 3, pp.312–316, 2009.

[13] E. J. Yoon and K. Y. Yoo, "Cryptanalysis of DS-SIP authentication scheme using ECDH," in *Proc. 2009 International Conference on New Trends in Information and Service Science*, 2009, pp. 642–647.

[14] R. Arshad and N. Ikram, "Elliptic curve cryptography based mutual authentication scheme for session initiation protocol," *Multimed Tool Appl*. Vol. 66, issue 2, pp. 165-178, 2013.

[15] T. H. Chen, H. L. Yeh, P. C. Liu, H. C. Hsiang, and W. K. Shih, "A secured authentication protocol for SIP using elliptic curves cryptography," *Communications in Computer and Information Science*, vol. 119, pp. 46–55, 2010.

[16] C. L. Lin and T. Hwang, "A password authentication scheme with secure password updating," *ComputSecur*., vol. 22, no. 1, pp. 68–72, 2003.

[17] E. J. Yoon and K. Y. Yoo, "A new authentication scheme for session initiation protocol," in *Proc. 2009 International Conference on Complex, Intelligent and Software Intensive Systems*, pp. 549–554, 2009.

[18] L. Wu, Y. Zhang and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC," *Computer Standards and Interfaces*, vol. 31, no. 2, pp. 286–291, 2009.

[19] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels", in *Proc. International Conference on the Theory and Application of Cryptographic Techniques Innsbruck*, Austria, May 6–10, 2001, pp. 453–474.

[20] Q. Xie, "A new authenticated key agreement for session initiation protocol," *Int J Commun Syst*. vol. 25, issue 1, pp. 47-54, 2011.

[21] E. J. Yoon and K. Y. Koo, "Robust mutual authentication with a key agreement scheme for the session initiation protocol," *IETE Tech Rev*., vol. 27, no. 3, pp.203–213, 2010.

[22] E. J. Yoon and K. Y. Yoo, "A three-factor authenticated key agreement scheme for SIP on elliptic curves," in *Proc. the 2010 Fourth International Conference on Network and System Security*, pp. 334–339.

[23] H. Tang and X. Liu, "Cryptanalysis of Arshad *et al*.'s ECC-based mutual authentication scheme for session initiation protocol," *Multimed Tools Appl*. 2012.

Samaneh Sadat Mousavi Nik received the B.Sc. Degree in Software Engineering from the Islamic Azad University of Quchan, Iran, in September 2007. She received her Master of Science degree from the University of Tehran-Kish international campus, Iran, in September 2012. She is currently lecturing Payam Noor University, Mashhad, Iran. Her research interests include information/network security, especially network protocols, cryptography, wireless networks.

Mehdi Shahrabi is a Master of Science student at the Amirkabir University of Technology- Tehran Polytechnic. He received the B.Sc. Degree in Information Technology from the Iran University of science and Technology of Tehran, Iran, in February 2010.

His research interests include information/network security, especially wireless networks.