Indonesian Journal of Electrical Engineering and Computer Science
Vol. 4, No. 1, October 2016, pp. 231 ~ 239
DOI: 10.11591/ijeecs.v4.i1.pp231-239

SIP Authentication Protocols Based On Elliptic Curve Cryptography: Survey and comparison

Mourade Azrour*, Mohammed Ouanan, Yousef Farhaoui
Moulay Ismail University, Faculty of sciences and Techniques,
Department of Computer Science, M2I Laboratory, ASIA Team, Errachidia, Morocco
*Corresponding author, email: azrour.mourade@gmail.com

Abstract

Session Initiation Protocol (SIP) is the most popular signaling protocol using in order to establish, modify and terminate the session multimedia between different participants. It was selected by the Third Generation Project Partnership (3GPP) as a multimedia application protocol in 3G mobile networks. SIP is the protocol currently used for signaling ToIP calls. The security of SIP is becoming more and more important. Authentication is the most important security service required by SIP. To ensure a secured communication, many SIP authentication protocols have been proposed. This work provides an overview of the proposed schemes based on elliptic curve cryptography. Those proposed schemes are analyzed in security consideration and the computational cost.

Keywords*: Session Initiation Protocol, security, authentication protocol, Elliptic Curve Cryptography*

Copyright © 2016 Institute of Advanced Engineering and Science. All rights reserved.

1. Introduction

Telephony over IP (ToIP) is a service that allows you to transfer voice communications flow on IP (Internet Protocol). This is the application that will require the IP infrastructure as the standard for all types of information or media. The Session Initiation Protocol (SIP) is a signaling protocol used to manage, establish and terminate the communication sessions between two or more participants. SIP is not limited to telephone calls, but it can be used for multimedia conferencing [1], instant messaging and online games,... View this popularity and use in public networks, SIP security becomes more and more important.

Authentication is the most security service required for SIP. The original SIP authentication protocol is HTTP Digest Authentication [2]. However, this protocol was found vulnerable to deferent attacks. In order to reinforce SIP authentication, a large community has been participated by proposing different protocols based on various mechanisms. In this paper we have analysed the proposed protocols based on security offred and total ranning time; the comparison between those protocols can helped as to determinate based on elliptic curve cryptography.

The remainder of this paper is organized as follows. Section 2 delivers general information on the architecture and the original SIP authentication protocol. In section 3, we analyze the performance security of proposed protocols. A comparison between the proposed protocols in terms of security and computational cost consideration are presented in section 4. Finally, section 5 concludes this research.

2. Background on SIP Protocol

SIP was initiated by the group MMUSIC (Multiparty Multimedia Session Control); then it was taken over and maintained by the SIP Group of the IETF. The first works were started on 1995, which resulted in a first version of SIP with the publication of RFC 2543 [3] in 1999; then a second version of SIP was published in 2002 to correct some defects of the previous version. This latest version is still effective through RFC 3261 [4].

SIP is a text-based protocol built on the basis of protocols such as HTTP or SMTP. The exchanges are in the form of dialogues (peer-to-peer relationships between agents) that include transactions (request/response). It is a widely used protocol, mainly for telephony type

Received April 13, 2016; Revised July 29, 2016; Accepted August 1, 2016

applications on IP. SIP belonged to the application layer of the OSI model. It provides mechanisms for opening, maintaining and closing an interactive session of communication between users.

2.1. SIP Architecture

The architecture of SIP consists of a proxy server, redirect server, registrar server, location server, and user agents. The role of each component is described as follows.

1. User Agent Client (UAC): generates SIP requests before they were sent.
2. User Agent Server (UAS): generates answers to SIP requests (accepting, refusing, or redirecting).
3. User Agent (UA): it can be a SoftPhone (software) or HardPhone (IP phone). It is able to generate, send and receive SIP requests. It can act at the same time as a UAC and UAS.
4. Registrar Server: handles the registration of SIP terminals. This is a server that accepts SIP REGISTER requests.
5. Proxy Server: it is a server which is connected to fixed or mobile terminals (UA). It plays the role of a server and client.
6. Redirect Server: it is a server that accepts SIP requests, translates the SIP address of a destination to IP address and returns them to the client.
7. Location server: It provides the proxy server, redirect server, and register server, it allows for them to look up or register the location of the user agent.

2.2. Authentication HTTP Digest

The authentication of SIP is the most security service recommended by the IETF (Internet Engineering Task Force). The messages exchanged between the server and the clients during authentication procedure are illustrated in Figure 1 and they are described as following:

1. Step 1. Client → Server : REQUEST
   The client sends a REQUEST to the server.
2. Step 2. Server → Client : CHALLENGE (nonce, realm)
   The server generates nonce. Then it sends back CHALLENGE that includes a nonce and realm to the client.
3. Step 3. Client → Server: RESPONSE (nonce, realm, username, response)

After receiving CHALLENGE from the server the client computes the response by using received nonce, username, secret password, and realm. response=F(nonce, username, password, realm). F(.) is a one-way hash function. Next, the client sends back to the server the message RESPONSE which contains the computed response, username, nonce and realm.

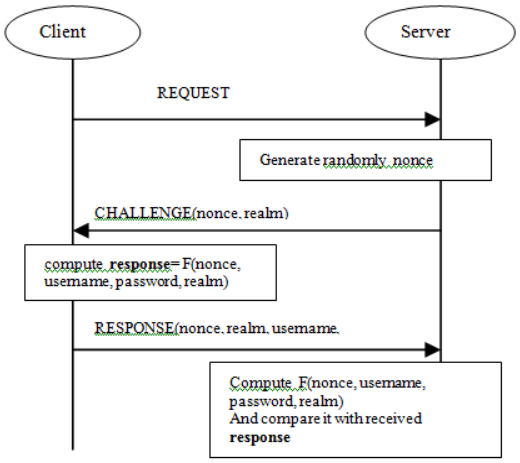


Figure 1. HTTP Digest Authentication

4. Step 4.

According to username the server extracts the client's password. Then the server verifies wither nonce is correct or not. If it is correct, the server computes F(nonce, username, password, realm) and uses it to compare it with the received response. If they match, the server authenticates the identity of the client.

2.3. Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) was introduced by Neal Koblitz in 1987 [5]. ECC proposed as an alternative to established public-key systems such as DSA and RSA. ECC have lately received a lot of attention in information security. The main reason for the attractiveness of ECC is the fact that there is no sub-exponential algorithm known to solve the discrete logarithm problem on a properly chosen elliptic curve. This means that ECC uses the keys of small size but offer the same levels of security offered by the Diffie-Hellman key large sizes. Some benefits of having smaller key sizes include faster computations, and reductions in processing power, storage space and bandwidth. This makes ECC ideal for constrained environments such as cellular phones and smart cards.

The elliptic curve is a cubic equation of the form in (1).

$$E: y^2 + axy + by = x^3 + cx^2 + dx + e \quad (1)$$

Where a, b, c and e are real numbers.

In cryptosystem, the elliptic curve equation is defined as the form in (2) over a prim finite field F_p, where $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0 \pmod p$. Given an integer $k \in F_p^*$ and a point $P \in E_p(a, b)$, the scalar multiplication kP over $E_p(a, b)$ can be computed as in (3).

$$E_p(a, b): y^2 = x^3 + ax + b \pmod p \quad (2)$$

$$kP = P + P + \cdots + P_{(k \text{ times})} \quad (3)$$

Definition 1. Given two points P and Q over $E_p(a, b)$, the elliptic curve discrete logarithm problem (ECDLP) is to find an integer $k \in F_p^*$ such as $Q = kP$.

Definition 2. Given three points P, sP and kP over $E_p(a, b)$ for $s, k \in F_p^*$, the computational Diffie-Hellman problem (CDHP) is to find the point skP over $E_p(a, b)$.

Definition 3. Given two points P and $Q = sP + kP$ over $E_p(a, b)$ for $s, k \in F_p^*$, the elliptic curve factorization problem (ECFP) is to find two points sP and kP over $E_p(a, b)$.

3. Analysis of Proposed SIP Authentication Protocols Based on Elliptic Curve Cryptography

In 2005, Yang et al., [6] demonstrated that the original SIP authentication protocol does not provide the necessary security, because it is vulnerable to Off-line password guessing attack and stolen verifier attack. For this, they proposed a new SIP authentication protocol that is based on the Diffie-Hellman Key Exchange [7], which depends on the difficulty of the Discrete logarithm problem. After a comparison with HTTP Digest Authentication and Key Exchange Encrypted (EKE), they motioned that their protocol is secure against Off-line password guessing attack, server spoofing attack and replay attack.

However the protocol of Yang et al. [6] needs maintenance and configuration of the passwords table. In addition, it functions on the discrete logarithm problem which need an important computation time. Therefore, it is not desirable for applications with low memory and limited computing capabilities [8].

In 2006, Huang et al., [8] propose a new protocol based only on hash functions. Then, they compare the computational complexity of their protocol with the Yang et al., protocol. So they concluded that their protocol is the fastest. Furthermore Jo et al. [9] demonstrated that the protocol of Yang et al., and the protocol of Huang etet al al. are both vulnerable to Off-line password guessing attack.

To overcome this weakness, Durlanik and Sogukpinar [10] based on the Yang et al.'s protocol to propose another SIP authentication protocol using the Elliptic Curve Cryptography

Diffie-Hellman (ECCDH). They demonstrated that their protocol reduces the computation time if it is compared with Diffie-Hillman. In addition, it allows the use of small size key but offer the same security offered by the Diffie-Hellman large key size. Consequently, this protocol offers an advantage in terms of computing time and in memory spaces. However Yoon et al., [11-12] introduced that the protocol of Durlanik and Sogukpinar cannot resist the stolen verifier attack and Denning-Sacco attack.

In 2008, Wu et al., [13] proposed a new SIP authentication and key exchange protocol based on elliptic curve cryptography (ECC). This protocol provides authentication and exchange of the session key at the same time. Wu et al., demonstrated that their protocol provides several security services such as confidentiality, integrity, authentication, access control and perfect forward secrecy. Then, they showed that it is secure against man-in-the-middle attack, replay attack, Off-line password guessing attack and server spoofing attack. However, this protocol is vulnerable to Off-line password guessing attack, Denning-Sacco attack and stolen verifier attack [14].

In 2008, Tsai [15] proposed an authentication protocol for SIP based on random nonce. In this protocol all communication messages are encrypted and decrypted by one-way hash functions, and a bit-wise exclusive-or (XOR) operation. As result, the calculation time is reduced when computation cost is compared with the existing protocols. For this, it is desirable for applications with low computing capacity. However, Yoon and Yoo [16] found that Tsai's protocol is vulnerable to Off-line password guessing attack, server spoofing attack and stolen verifier attack. In addition, it does not provide key exchange secrecy, key known secrecy and perfect forward secrecy.

In 2009, Yoon and Yoo [16] proposed a new secure authentication protocol based on elliptic curve cryptography discrete logarithm problem. They demonstrated that their protocol is quicker when it is compared with previous proposed protocols. Moreover, it is secure against the man-in-the-middle attack, Off-line password guessing attack, replay attack, modification attack, Denning-Sacco attack and stolen verifier attack. In addition, it provides mutual authentication, known key secrecy, session key secrecy and perfect forward secrecy. However, Liu and Koenig [17] demonstrated that this protocol is vulnerable to Off-line password guessing attack and partition attack.

In 2010, Yoon et al., [11] based on weakness of Sogukpinar and Durlanik protocol and on the problems of Wu et al., protocol to propose another authentication protocol based on ECC. However, this protocol is vulnerable to Off-line password guessing attack and stolen verifier attack [18].

In 2011, Arshad and Ikram [19] demonstrated that Tsai et al., protocol is vulnerable to Off-line password guessing attack and stolen verifier attack, and it does not provide key known secrecy and perfect forward secrecy. As result, Arshad and Ikram presented an authentication protocol for SIP based on ECC. They showed that their protocol is secure against Off-line password guessing attack, modification attack, stolen verifier attack, server spoofing attack and man-in-the-middle attack. Furthermore, it provides known key secrecy, session key secrecy and perfect forward secrecy. After a comparison of their protocol with Yang et al., protocol and Tsai's protocol, Arshad et al. concluded that their protocol is the more efficient.

In 2012, Xie [18] showed that the protocol of Yoon and Yoo is insecure against stolen verifier attack and Off-line password guessing attack. Based on these attacks Xie proposes a new SIP authentication protocol. Then, he demonstrated that his protocol is more secure, and it is faster when it compared with existing protocols. However Xie's protocol is shown vulnerable to Off-line password guessing attack and impersonation attack [20].

In 2012, Tang et al., [21] noted that the protocol introduced by Arshad and Ikram is not secure against attack Off-line password guessing. In order to deal with this problem, they suggested another secure and efficient SIP authentication protocol based on ECDLP. In the same year Sadat et al., [22] show that the Tang et al.'s protocol suffers from Off-line password guessing attack, registration attack and modification attack. Then, they also introduced a new protocol based on ECDLP.

In 2013, Farash et al., [20] noted that the protocol proposed by Xie is defenseless to Off-line password guessing attack and to impersonation attack. Therefore they presented another authentication protocol SIP. Then they demonstrated that their protocol can resist to Off-line password guessing attack, stolen verifier attack, Denning-Sacco attack, man-in-the-middle attack and replay attack.

In 2014, Sadat Nik and Shahrab [23] proposed a mutual SIP authentication Scheme Based on ECC, then they demonstrated that their proposed scheme can resist to modification attack, Denning Sacco attack, registration attack, replay attack, man-in-the-middle attack, and stolen verifier attack.

The previous SIP authentication protocols proposed are based on the password verification using several mechanisms. Then, the password must be shared between the client and the server. The server store this password or its verifier in the database wish must be maintained and protected. Therefore, these protocols are vulnerable to verifier stolen attack. In addition to this attack these protocols suffer from the problem of managing of password's database, which often occupies a large memory space. In 2013, these problems begin to solve when a first SIP authentication protocol using the Smart Card was proposed by Zhang et al. [24]. Zhang et al., have demonstrated that their protocol offers several advantages such as mutual authentication, session key secrecy and password updating. In addition, it is secure against replay attacks, server spoofing attack, stolen verifier attack, man in the middle attack, and offline password guessing attack. Despite this, the protocol is proven vulnerable to user impersonation attack in [25, 27, 29]. In order to solve this attack, Zhang et al., propose a year after their second protocol [25].

Irshad et al., [26] have noted that the lack of timestamp in the protocol of Zhang et al., [24] can be a source of the attack Denial of Service (DoS). Moreover, the use of a single server secret to protect information during authentication can expose the whole system if compromised. However, the protocol can be made more robust if server uses two secrets instead of one. Also, they said that the number of messages exchanged during authentication can be reduced by two instead of three messages. Consequently, Irshad et al. propose a new authentication protocol for SIP based on the Elliptic Curve Cryptography and using the Smart Card. This protocol consists of four phases which are system setup phase, registration phase, authentication phase and password exchange phase. The first, the two and the last phases are almost similar to the phases of Zhang et al., [24]. However, the authentication phase is completed in a single round-trip instead of a round-trip and half. Next, Irshad et al. demonstrate that their protocol is resistant to known attacks.

Wu et al., [27] also showed that the protocol of Zhang et al., [24] is vulnerable to user impersonation attack. This attack is applied by a legitimate user having valid Smart Card, but who tries to connect to the server under the name of his victim. The attacker in this case uses his smart card and his valid password but he successfully connected using the name of another legitimate client. Based on the work presented by He et al., in [28] Wu et al., proposed a new SIP authentication protocol which consists of four phases: system setup, registration, authentication, and password exchange. They justified that their protocol resists to the following attacks: replay attack, server spoofing, stolen verifier attack, man-in-the-middle attack, Offline password guessing attack, and modification attack. Furthermore, it provides mutual authentication and perfect forward secrecy

In 2014, Jiang et al., [29] proposed a new SIP authentication protocol. This protocol is composed of three phases: system setup phase, registration phase, authentication phase, and password exchange phase. Jiang et al., have demonstrated that their protocol is secure against known attacks and it is faster if compared with the protocol of Zhang et al.

In the same year, Tu et al., [30] also found that the protocol of Zhang et al., [24] is vulnerable to the user impersonation attack using the same principle used by Wu et al., [27]. In order to overcome this problem they proposed a new protocol that consists of four phases such as Zhang et al., protocol. Tu et al., proved that their protocol is secure against replay attack, server spoofing attack, stolen verifier attack, the man- in-the-middle attack, Offline password guessing attack, and modification attack. After a comparison between the computing time of their protocol and Zhang et al., protocol computing time, Tu et al., reduced that the authentication phase of their protocol reduce the computing time cost to 75% compared to the same Zhang et al., phase. Despite these advantages, Tu et al., protocol is demonstrated vulnerable to many attacks by Farash et al., [31], Mishra et al., [32] and Zhu et al., [33].

Mishra et al., [32] discovered that the protocol of Tu et al. cannot resist server spoofing attack, user impersonation attack and the man-in-the-middle attack. Consequently, they proposed a new SIP authentication protocol that is proven secure against known attacks. A year later, Zhu et al., [33] shown that the protocol of Tu et al., is vulnerable to user impersonation

attack and server spoofing attack. Then they proposed a new protocol that can withstand attacks found in the protocol of Tu et al.

Farah et al., [30] also showed that the Tu et al.'s protocol is vulnerable to user impersonation attack. In order to overcome the weakness Farash et al., proposed their SIP authentication protocol. However, in 2015, Chaudhry et al., [34] demonstrated that the Farash et al., protocol is defenseless to replay attack and Denial of Service attack. As result, they proposed a new protocol and they have proven to be secure against known attacks.

Kumaris et al., [35] noticed that Farah et al., protocol puts up with impersonation attack, offline password guessing attack, lacks user anonymity and session-specific temporary information attack. Based on these attacks Kumari et al., proposed a new protocol that can resist user impersonation attack, Off-line password guessing attack, replay attack and man-in-the-middle. In addition, it can provide mutual authentication and perfect forward secrecy.

In 2014, Arshad et al., [36] Showed that Irshad et al., protocol suffer from user impersonation attack. In order to force the authentication of SIP, Arshad et al., Proposed a new SIP authentication protocol. They have proven that their protocol is resistant to various attacks, as it is faster when compared with existing protocols. However, in 2016, Lin et al., [37]. Have discovered that Arshad et al., protocol is not secure enough because it does not withstand server spoofing attack, denial of service attack and insider privilege attack. To overcome this problem Lin et al. proposed a new protocol that is more secure and allows to users to update their password using a new method.

4. Comparison And Cost Analysis

The effectiveness of a protocol meant resistance to known attacks and quick execution. In this section we present the results of the comparison between the authentication protocols SIP, in terms of security and in terms of computing time cost.

4.1. Security comparison

Table 1 shows the results of the comparison between the proposed protocols depending on the type of attack. As can be seen; protocols that based on elliptic curve cryptography are the most resistant to known attacks.

Table 1. Security performance

ATTACKS	EXP		HASH FUNCTIONS		ELLIPTIC CURVE CRYPTOGRAPHY															
					With table of passwords			Without table of passwords (Using Smart card)												
	[4]	[11]	[6]	[14]	[8]	[12]	[11]	[21]	[17]	[19]	[23]	[28]	[29]	[30]	[31]	[32]	[23]	[34]	[35]	[36]
Stolen verifier	No	-	No	No	No	No	No	YES	YES	YES	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Denning Sacco	No	-	No	No	No	No	YES	YES	YES	YES	Yes	-	-	Yes	Yes	-	-	-	-	-
password guessing	No	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	No	Yes	-	Yes	Yes	Yes	Yes
Replay	No	No	YES	YES	YES	YES	YES	YES	YES	YES	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Man in the middle	No	No	-	-	YES	YES	YES	YES	YES	YES	Yes	-	No	Yes	Yes	-	-	-	-	-
Server spoofing	No	No	-	YES	-	YES	-	YES	-	YES	No	No	No	Yes	Yes	Yes	Yes	-	No	Yes
Impersonation	-	-	YES	YES	No	-		No	No	YES	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes

4.2. Computation Time Cost Comparison

The time computation of a protocol is generally dependent on the complexity or simplicity of the calculation. So to calculate total running time of a protocol, we must firstly know the running time of each function used. Then, calculate the number of times these functions are used. Due to the importance of this issue, some researchers have focused on reducing the necessary time for creating the session in progress, for example in [38].

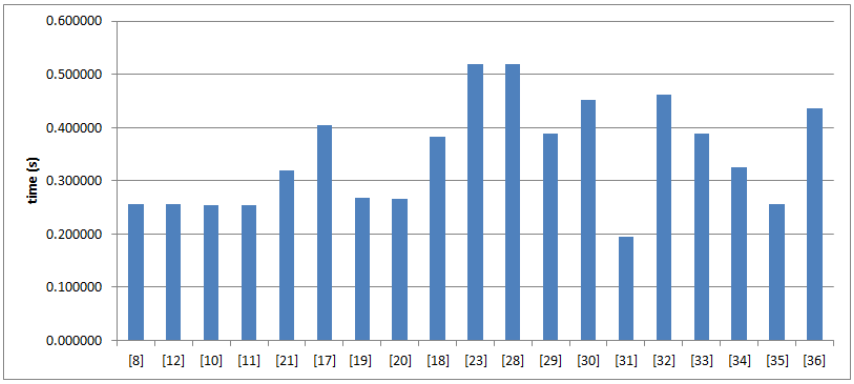
In our paper we can compare the speed of protocols by comparing the running time of each one or by comparing the number and the time execution of each function used. Table 2 shows result of computational cost comparison of authentication phases.

Table 2. Computational cost comparison of authentication phases

	[1]	[6]	[14]	[4]	[8]	[12]	[10]	[11]	[21]	[17]	[19]	[20]	[18]	[23]	[28]	[29]	[30]	[31]	[32]	[33]	[34]	[35]	[36]
H	2	8	7	8	6	6	4	5	8	6	7	5	8	10	9	8	10	11	11	9	10	8	11
HP	0	0	0	0	0	0	0	0	0	0	2	2	0	0	0	0	0	1	0	0	0	0	0
AEC	0	0	0	0	0	0	0	0	0	1	2	2	0	2	2	1	1	0	1	1	1	0	0
MEC	0	0	0	0	4	4	4	4	5	6	4	4	6	8	8	6	7	3	7	6	5	4	6
SKE	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	3
SKD	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	3

H: one-way hash function; **XOR** : exclusive-or operation. **HP**: hash of point operation. **AEC**: elliptic curve point addition operation. **MEC**: elliptic curve point multiplication operation. **SKE** : symmetric encryption algorithm. **SKD** : symmetric decryption algorithm

According to H. F. Zhu [39] the computational time of a one-way hashing operation, a symmetric encryption/decryption operation, and elliptic curve point multiplication operation operation is 0.0005s, 0.0087s and 0.063075s respectively. In Figure 2 shows the total running times of different protocols.



5. Conclusion

Authentication is the most security service required by SIP. Different protocols have been proposed to overcome the original SIP authentication protocol problems. Performance and vulnerabilities of proposed protocols are analyzed in this work. As result, we conclude that the protocols that are based on elliptic curve cryptography are the most resistant to known attacks. Furthermore; we noticed that the send of password during authentication either in hashed or concatenated with other public values can be the source of the Off-line password guessing attack. Then, we need to think about another method that can secure authentication of SIP against this attack. So our future work will focus on developing a new method to strengthen the authentication of SIP.

References

[1] Shanshan Peng. Audio and Video Communication Software Design Based on SIP. 2014; 12(11).

[2] J Franks, P Hallam-Baker, J Hostetler, S Lawrence, P Leach, A Luotonen, L Stewart. HTTP Authentication: Basic and Digest Access Authentication. *Internet Engineering Task Force.* 1999: 2617.
[3] M Handley, H Schulzrinne, E Schooler, J Rosenberg. SIP: Session Initiation Protocol. 1999.
[4] J Rosenberg, H Schulzrinne, G Camarillo, A Johnston, J Peterson, R Sparks, M Handley, E Schooler. SIP: Session Initiation Protocol. *Internet Engineering Task Force.* 2002.
[5] N Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation.* 1987; 48(177): 203-209.
[6] Chou-Chen Yang, Ren-Chiun Wang, Wei-Ting Liu. Secure authentication scheme for session initiation protocol. *Computers & Security.* 2005; 24: 381-386.
[7] W Diffie, M Hellman. New directions in cryptology. *IEEE Transaction on Information Theory.* 1976; 22(6).
[8] H Huang, W Wei, GE Brown. *A new efficient authentication scheme for session initiation protocol.* In Proceedings of the 9th Joint Conference on Information Sciences. 2006.
[9] H Jo, Y Lee, M Kim, S Kim, D Won. *Of-line password guessing attack to Yang's and Huang's authentication schemes for session initiation protocol.* In Proceedings of the 5th International Joint Conference on INC, IMS and IDC (NCM '09). 2009: 618-621.
[10] Durlanik A, Sogukpinar I, SIP Authentication Scheme using ECDH. *World Enformatika Socity Transations on Engineering Computing and Technology*. 2005; 8: 350-353.
[11] Yoon EJ, Yoo KY. *Cryptanalysis of DS-SIP authentication scheme using ECDH.* In 2009 International Conference on New Trends in Information and Service Science. 2009: 642-647.
[12] EJ Yoon, KY Yoo, C Kim, YS Hong, M Jo, HH Chen. A secure and efficient SIP authentication scheme for converged VoIP networks. *Computer Communications.* 2010; 33(14): 1674-1681.
[13] L Wu, Y Zhang, F Wang. A new provably secure authentication and key agreement protocol for SIP using ECC. *Computer Standards and Interfaces*. 2009; 31(2): 286-291.
[14] Eun-Jun Yoon, Kee-Young Yoo. *Cryptanalysis of NAKE Protocol based on ECC for SIP and Its Improvement.* Second International Conference on Future Generation Communication and Networking Symposia. 2008.
[15] JL Tsai. Efficient nonce-based authentication scheme for session initiation protocol. *International Journal of Network Security*. 2009; 8(3): 312-316.
[16] Yoon EJ, Yoo KY. *A new authentication scheme for session initiation protocol.* In 2009 International Conference on Complex, Intelligent and Software Intensive Systems, CISIS '09. 2009: 549-554.
[17] FW Liu, H Koenig. *Cryptanalysis of a SIP authentication scheme.* In 12th IFIP TC6/TC11 International Conference, CMS 2011. 2011; 7025: 134-143.
[18] Q Xie. A new authenticated key agreement for session initiation protocol. *International Journal of Communication Systems.* 2012; 25(1): 47-54.
[19] R Arshad, N Ikram. Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. *Multimed Tools Appl.* 2013; 66(2): 165-178.
[20] Farash et al. An Enhanced Authenticated Key Agreement for Session Initiation Protocol. Information Technology and Control. 2013; 42(4).
[21] H Tang, X Liu. Cryptanalysis of Arshad et al.'s ECC-based mutual authentication scheme for session initiation protocol. *Multimedia Tools and Applications.* 2013; 65(3): 165-178.
[22] Sadat, et al. Proposed SecureSIP Authentication Scheme based on Elliptic Curve Cryptography. *International Journal of Computer Applications*. 2012; 58(8).
[23] SSM Nik, M Shahrab. Mutual SIP Authentication Scheme Based on ECC. *International Journal of Computer and Electrical Engineering.* 2014; 6(2).
[24] L Zhang, S Tang, Z Cai. Efficient and flexible passwordauthenticated key agreement for voice over internet protocolsession initiation protocol using smart card. *International Journal of Communication Systems*. 2013; 27(11): 2691-2702.
[25] L Zhang, S Tang, Z Cai. Cryptanalysis and improvement of password-authenticated key agree-ment for session initiation protocol using smart cards. Secur Commun Netw. 2014.
[26] A Irshad, M Sher, E Rehman, ChS Ashraf, MU Hassan, A Ghani. A single round-trip SIP authentication scheme for voice over internet protocol using smart card. *Multimed Tools Appl*. 2013.
[27] K Wu, P Gong, J Wang, X Yan, P Li. An Improved Authentication Protocol for Session Initiation Protocol Using Smart Card and Elliptic Curve Cryptography. Romanian Journal of Information Science and Technology. 2013; 16(4): 324-335.
[28] He D, Chen J, Hu J. An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security. *Information Fusion*. 2012; 13(3): 223-230.
[29] Q Jiang, J Ma, Y Tian. Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol of zhang et al. *International Journal of Communication Systems*. 2014; 28(7).
[30] H Tu, N Kumar, N Chilamkurti, S Rho. An improved authentication protocol for session initiation protocol using smart card. *Peer-to-Peer Networking and Applications*. 2014: 1936-6442.
[31] MS Farash. Security analysis and enhancements of an improved authentication for session initiation protocol with provable security. Peer-to-Peer Netw. Appl.

[32] D Mishra, AK Das, S Mukhopadhyay. A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card. *Peer-to-Peer Netw. Appl*.
[33] W Zhu, J Chen, D He. Enhanced authentication protocol for session initiation protocol using smart card. *Int. J. Electronic Security and Digital Forensics*. 2015; 7(4).
[34] SA Chaudhry, K Mahmood, H Naqvi, Mu Sher. *A secure authentication scheme for session initiation protocol based on elliptic curve cryptography*. 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications. Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. 2015.
[35] S Kumari, SA Chaudhry, F Wu, X Li, MS Farash, MK Khan. An improved smart card based authentication scheme for session initiation protocol. *Peer-to-Peer Netw. Appl*. 2015.
[36] H Arshad, M Nikooghadam. An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC. *Multimed Tools Appl*. 2014.
[37] H Lin, F Wen, C Du. An anonymous and secure authentication and key agreement scheme for session initiation protocol. *Multimed Tools Appl. Multimed Tools Appl*. 2016.
[38] A Montazerolghaem, S Hosseini-Seno, MH Yaghmaee, R Budiarto. *High Load Diminution by Regulating Timers in SIP Servers.* Proceeding of International Conference on Electrical Engineering, Computer Science and Informatics (EECSI 2014). Yogyakarta, Indonesia. 2014.
[39] HF Zhu. Sustained and authenticated of a universal construction for multiple key agreement based on chaotic maps with privacy preserving. *Journal of Internet Technology.* 2016; 17(5): 1-10.