Paper

A New Efficient Authenticated and Key Agreement Scheme for SIP Using Digital Signature Algorithm on Elliptic Curves

Asma Jebrane, Ahmed Toumanari, Naîma Meddah, and Mohamed Bousseta

Ibn Zohr University, Agadir, Morocco

Abstract—Voice over Internet Protocol (VoIP) has been recently one of the more popular applications in Internet technology. It benefits lower cost of equipment, operation, and better integration with data applications than voice communications over telephone networks. However, the voice packets delivered over the Internet are not protected. The session initiation protocol (SIP) is widely used signaling protocol that controls communications on the Internet, typically using hypertext transport protocol (HTTP) digest authentication, which is vulnerable to many forms of attacks. This paper proposes a new secure authentication and key agreement scheme based on Digital Signature Algorithm (DSA) and Elliptic Curve Cryptography (ECC) named (ECDSA). Security analysis demonstrates that the proposed scheme can resist various attacks and it can be applied to authenticate the users with different SIP domains.

Keywords—authentication, key agreement, session initiation protocol, VoIP.

1. Introduction

Voice over IP (VoIP) networks attract great attention since they can provide low cost, deployment and maintenance, flexible implementation, and new applications than conventional telephones [1]. The session initiation protocol (SIP) is an application-layer signaling protocol based on HTTP-like request/response exchange for initiating, managing and terminate voice session. Authentication is an important security requirement when a user wants to access the SIP services. However, the original authentication scheme for SIP does not provide strong security, because it works based on HTTP-digest authentication [2], which is vulnerable to several attacks such as impersonation attacks, offline password guessing attacks and server spoofing attacks etc. Therefore, with the widespread use of VoIP in worldwide, the security of SIP has received much attention from several studies.

The remainder of this paper is outlined as follows. The related work is shown in Section 2. Section 3 provides some basic preliminaries and notations used in this paper. Section 4 shows proposed scheme. Section 5 analyzes presented solution. Section 6 shows the performance and functionality comparisons with other related works. The conclusion is given in Section 7.

2. Related Work

Since Elliptic Curve Cryptography (ECC) provides a smaller key size than any other cryptosystem and has faster computations than half of other public key systems [3]. Several protocols for SIP server based on ECC have been proposed to strength the security and performance of VoIP communication.

In [2] Yang pointed out that HTTP digests authentication protocol is vulnerable to offline password guessing attacks, and the spoofing attacks. They proposed a SIP authentication protocol based on Diffie-Helman key exchange protocol. Unfortunately Yang's protocol still suffered from the replay attack. In [4] the authors produced a new secure authentication and key agreement protocol called NAKE to solve the existing problems in the original proposal. The scheme assumes that the communication parties must share a common secret number k, but an adversary can easily launch the forgery-attack to act as the server or the user client.

In [5] Yoon *et al*. demonstrates that proposed SIP authentication schemes are not secure against attacks such as offline password guessing attack, Denning-Sacco attacks and stolen verifier attacks. They propose a new SIP authentication scheme in a converged VoIP network based on ECC in order to overcome security problems. However, Yoon *et al*. protocol was still not suitable for different SIP domains. In [6] Wang and Zhang proposed a new authentication and key agreement mechanism (SAKA) based on certificate-less public key cryptography, to conquer many forms of attacks in SIP authentication. The proposed protocol suffers from heavy computation cost. Also, Zhang *et al*. in [7] proposed an efficient authentication for SIP using smart card based on ECC. The proposed protocol can resist various attacks and provides efficient password updating.

Recently Arshad and Ikram [8] proposed an authentication protocol based on elliptic curve discrete logarithm problem for SIP. However, their protocol suffered from off-line pass-

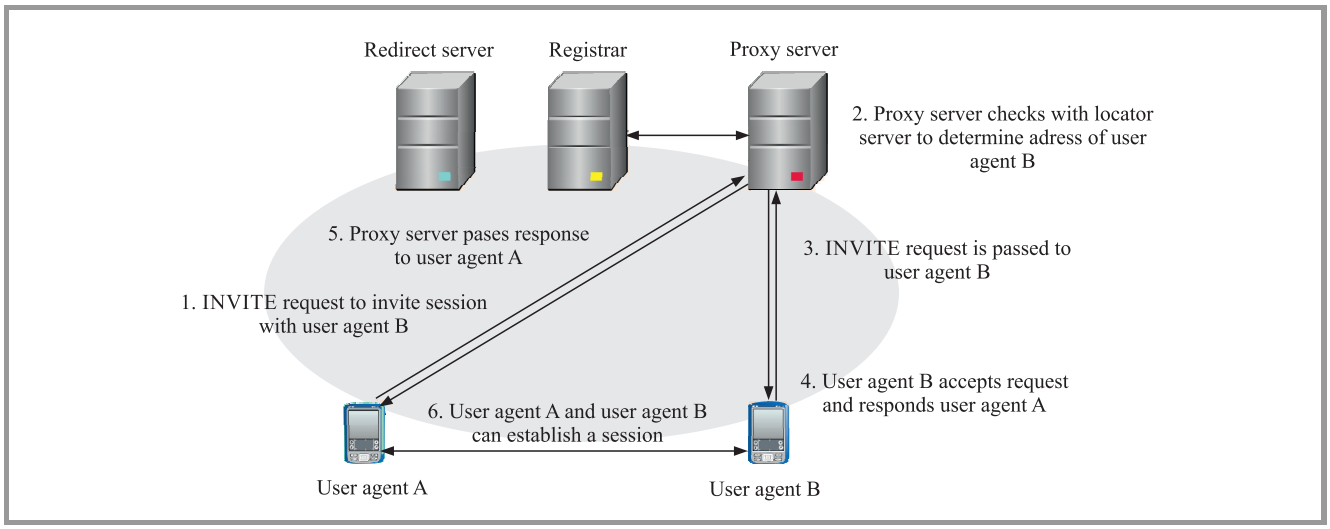


Fig. 1. SIP architecture.

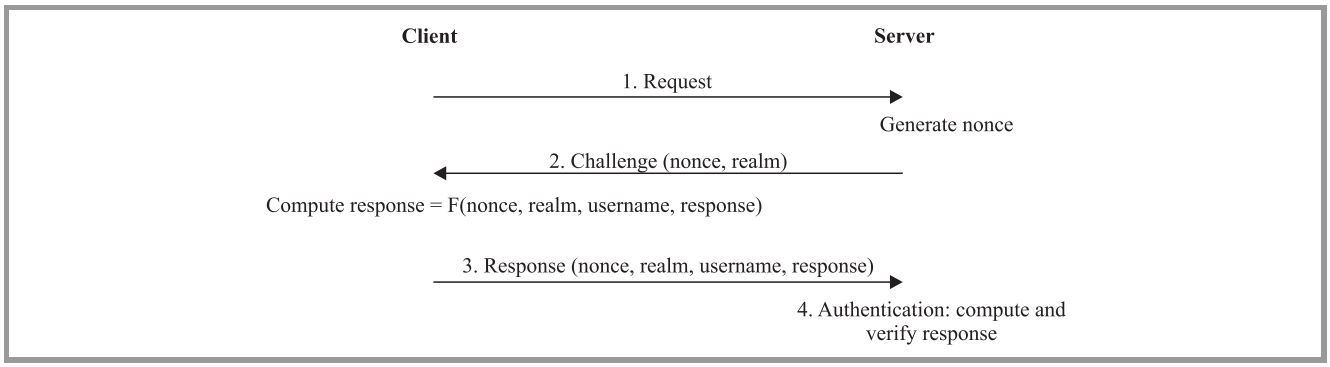


Fig. 2. SIP authentication.

word guessing attacks, for that Yel et al. in [3] adopted the smart card to construct an authentication protocol based on ECC for SIP. Liping *et al*. [9] confirm that Yel's protocol involved the time synchronization problem.

3. Preliminaries

In this section, the SIP architecture and SIP authentication procedure are introduced. Then, we briefly review the fundamentals of ECC and digital signature logarithm on ECC (ECDSA).

3.1. SIP Architecture

The SIP is a general purpose application layer signaling protocol [10] that is used to create, modify and terminate multimedia session such as VoIP calls. The SIP architecture is composed of a user agent client, proxy server, redirect server, register server and location server [8] (Fig. 1). The user agent is a logical entity such as a caller or a callee. Proxy server forwards a request and response between a caller and callee. Redirect server accepts requests and replies to the client with a response message. Location server maintains information on the current location of the user agent.

3.2. SIP Authentication Procedure

SIP authentication scheme works similarly to HTTP digest authentication [11], in which a nonce value is used in challenging the target. The response includes a checksum of the username, password, and nonce value [6]. Here is an example flow of authentication mechanism in SIP (Fig. 2).

1. **client** → **server**: Request. The client sends a request to the server.
2. **server** → **client**: Challenge(nonce, realm). Server generates a challenge that includes a nonce and client's realm.
3. **client** → **server**: Response(nonce, realm, username, response). The client computes the response = F(nonce, realm, username, response). Then the client sends the Response to the server.
4. According to the username, the server extracts the client's password. Then the server verifies whether the nonce is correct. If is, the server computes

F(nonce, username, password, realm) and use it to make a comparison with the response. If they match, the server authenticates the identity of the client.

3.3. Elliptic Curve Cryptography (ECC)

An elliptic curve is a cubic equation of the form: $E : y^2 + axy + by = x^3 + cx^2 + dx + e$, where a, b, c, and e are real numbers. Let F_p denote the finite of points where p is a large prime number and containing x, y. We focus on the finite field of ECC, the mathematical equation of ECC to be of form:
$E : y^2 = (x^3 + ax + b) \bmod p$ with a, $b \in F_p$ satisfying $(4a^3 + 27b^2) \bmod p \neq 0$. The arithmetic of elliptic curve discrete logarithm problem (ECDLP) is given points Q and P. Where Q, $P \in F_p$, and compute $Q = \alpha \times P$ it is hard to determine α given Q and P. In view of shortness, we omit the details and refer to [8], [12].
A key exchange between e.g. Alice and Bob can be accomplished as follows:

- Alice generates a random integer $a \in Z_p^*$ and compute $K_A = a \times P$ and sends K_A to Bob.
- Bob generates a random integer $b \in Z_p^*$ and compute $K_B = b \times P$ and sends K_B to Alice.
- Alice can compute shared key $SK_A = a \times K_B = a \times b \times \times P$ and Bob can compute shared key $SK_B = b \times K_A = b \times a \times P$

In this manner if we would like to find $SK_A = SK_B$, to break this scheme, we would face ECDLP, which is a hard and complex mathematical problem.

3.4. Digital Signature Algorithm Using Elliptic Curve (ECDSA)

In procedure for generating signature using the ECDSA to sign a message m an entity A with domain parameters (E, P, n, a, b, h) and associated key pair(d, Q) the following procedure is used:

1. select a random or pseudorandom integer k,
2. compute $kP = (x_1, y_1)$ and $r = x_1 \bmod n$; if $r = 0$ go to step 1.
3. compute $k^{-1} \bmod n$,
4. compute $e = h(m)$,
5. compute $s = k^{-1}(e + d.r) \bmod n$; if $s = 0$ then go to step 1.
6. A's signature for the message m is (s, r).

4. Proposed Authentication Scheme

In this section, a new authenticated key agreement of protocol SIP using ECDSA is proposed. The proposed scheme achieves mutual authentication between different SIP domains, the public key is computed directly from the signature of third trust party (TTP) on the user's identity. The proposed scheme comprises four phases: initialization, registration, mutual authentication, and the password change. The notations adopted through this paper are summarized in Table 1. The whole process is summarized in Table 2.

Table 1
Notations used in this paper

Notation	Definition
S	Server
Alice	A legal user
ID_A	User identity
ID_S	SIP server identity
PW_A	User password
TA	Trust authority
(s_T, PK_T)	TA key pair
P	A generator point with order n over $E_p(a,b)$
SK	Shared session key
h(.)	Secure one way hash function
$\|\|$	Concatenation operation
$A \longrightarrow B : M$	A sends a message M to B

4.1. Initialization Phase

A trusted authority (TA) was defined in each SIP domain to issue the private keys to the entities in the same domain. All entities have agreed upon a high elliptic curve E defined over a finite field, which is used with a base point generator P of prime order n. TA selects a random number $s_T \in Z_p^*$ as his private key, and then computes his public key PK_T ($PK_T = s_T \times P$). Then TA keeps s_T and publishes the system parameters (PK_T, P,n, G, h).
Each eligible server S_i selects a random k_i, computes $K_i = k_i \times P$ and sends (SID_i, K_i) to TA. TA chooses a random number t, compute $x = t \times P$ and compute the signature parameters (r_i, s_i) as follows:

$$\begin{cases} r_i = x \bmod n \\ s_i = t^{-1}\left(h(ID_i \,\|\, R_i) + s_T \cdot r_i\right) \end{cases}$$

then compute the parameters:

$$\begin{cases} R_i = r_i \times K_i \\ S_i = s_i \times x \end{cases}$$

Next, TA sends (R_i, S_i) to the server over a secure channel, upon receiving (R_i, S_i) the server computes his secret key $S_{key} = S_i \times k_i$ and his public key $P_{key} = S_{key} \times P$.

Table 2
Authenticated key agreement phase

Alice	TA
Registration phase: Chooses (ID_A, PW_A) Select a random k and compute $K_A = k \times P$ Sends (ID_A, PW_A, PW_A) to TA $\rightarrow$	Selects a random t and compute $x = t \times P$ Compute the signature parameters(r_A, s_A) Compute $\overline{s}_A = s_A \times x$ and $R_A = r_A \times K_A$ Compute : $C_2 = h(PW_A \| R_A)$ $m_A = \overline{s}_A + C_2$ $PK_A = [h(ID_A \| R_A).P.K_A + PK_T.R_A]$ smartcard (R_A, m_A, PK_A)
Input (ID_A, PW_A) Compute $s_A = m_A - c_2$ $sk_A = s_A \times k$ check if $(s_A \times P) = ?PK_A$ if yes $m_A^{new} = m_A \times k$	
Alice	SIP server
Mutual authentication phase: Input (ID_A, PW_A) Compute $s_A = m_A - c_2$ Check if $(s_A \times P) = ?PK_A$ Select a random a and compute $T_A = a \times P$ Sends (ID_A, R_A, K_A, T_A)	Generate a random b Compute $T_s = b \times P$ Compute PK_A Obtain the shared key: $SK_s = b \times PK_A + S_s \times T_A$ $C_2 = h(SK_s)$ $Auth_s = h(nonce \| realm \| ID_A \| ID_s \| T_A \| T_s \| c_2)$ Send CHALLENGE $\langle R_s, T_s, Auth_s, realm \rangle$
Compute $PK_s = [h(ID_s \| R_s).P.K_s + PK_T.R_s]$ $SK_A = a.PK_s + sk_A.T_A$ $c_3 = h(SK_A)$ $Auth_s = ?h(nonce \| realm \| ID_A \| ID_s \| T_A \| T_s \| c_3)$ $Auth_A = h(nonce + 1 \| realm \| ID_A \| ID_s \| T_A \| T_s \| c_3)$ Send RESPONSE $\langle nonce, realm, Auth_A \rangle$	Verify $Auth_A = h(nonce + 1 \| realm \| ID_A \| ID_s \| T_A \| T_s \| c_2)$
Shared key: $SK_A = a \times T_s = a \times b \times P$	$SK_s = b \times T_A = b \times a \times P$

4.2. Registration Phase

When a new user (Alice) wants to register with the server S, it performs the following process with TA to complete the registration process:

- Step R_1. Alice first selects her identity ID_A, password PW_A, and a random number k. Next, computes $K_A = k \times P$. Then, Alice sends $\{ID_A, PW_A, K_A\}$ to TA over a secure channel.
- Step R_2. After receiving the information, TA generates a random value t and computes $x = t.P$, the signature parameters (r_A, s_A) for Alice using previous equations. Next, TA computes the following parameters using her secret key s and the received message from Alice: $\overline{s}_A = s_A \times x$, $R_A = r_A \times K_A$, $c_1 = h(PW_A \parallel R_A)$, $m_A = \overline{s}_A + c_1$. Now the public key of Alice (PK_A) with the following equation:

$$PK_A = [h(ID_A \| R_A).P.K_A + PK_T.R_A].$$

In the end, TA personalizes a smart card with the secret parameters (m_A, R_A, PK_A, K_A) and delivers it to Alice through a secure channel.

- Step R_3. Upon receiving the smart card, Alice inputs (ID_A, PW_A, k) and the smart card computes $\overline{s}_A = m_A - c_1$ and $s_A = \overline{s}_A.k$. Next, check if $(s_A \times P)$ is equal to PK_A. If yes, the smart card update m_A to the new value $m_i^{new} = m_i \times k$ and terminate the registration phase.

4.3. Mutual Authentication Phase

Assume that Alice wants to communicate with the remote SIP server she must enter her user name ID_A and her password PW_A.
During the authentication process, Alice and the SIP server S perform the following steps to achieve mutual authentication and key negotiation.

Step 1 – Alice → server: Request $\langle ID_A, R_A, T_A \rangle$
First, Alice inputs her identity ID_A and password, then randomly chooses a number $a \in Z_p^*$ for computing $T_A = a \times P$, after that, she sends the request $\langle ID_A, R_A, T_A \rangle$ to the server S over a public channel.

Step 2 – server → Alice: Challenge $\langle R_s, T_s, Auth_s, realm \rangle$.
The server receives the REQUEST $\langle ID_A, R_A, T_A \rangle$ message and performs the following operations to challenge Alice:

- generate a random value b and compute $T_s = b \times P$,
- using received parameters ID_A, R_A compute the public key PK_A of Alice $PK_A = [h(ID_A \| R_A).P.K_A + PK_T.R_A]$,
- obtain the shared session key $SK_s = b.P + S_s.T_A$,
- calculate $c_2 = h(SK_s)$,
- generate the authentication information $Auth_s = h(nonce \| realm \| ID_A \| ID_s \| T_A \| T_s \| c_2)$. After that, the server sends the Challenge $\langle R_s, T_s, Auth_s, realm \rangle$ message to Alice.

Step 3 – Upon receiving the Challenge message, Alice computes the public key of the server and session key with the equations:
$PK_s = [h(ID_s \| R_s).P.K_s + PK_T.R_s]$,
$SK_A = a.PK_s + S_.T_A$.
Then, check the validity of the received message $Auth_s$ with the computed value $h(nonce \| realm \| ID_A \| ID_s \| T_A \| T_s \| c_3)$.

Step 4 – Alice → server: Response $\langle nonce, realm, Auth_A \rangle$.
After the server authentication phase, Alice computes $c_3 = h(SK_A)$ and calculates the response value $Auth_A = h(nonce \| realm \| ID_A \| ID_s \| T_A \| T_s \| c_2 \| c_3)$. Then send Response message $\langle nonce, realm, Auth_A \rangle$ to the server.

Step 5 – After receiving the message Response $\langle nonce, realm, Auth_A \rangle$, the SIP server S checks whether the following equation holds $Auth_A = h(nonce + 1 \| realm \| ID_A \| ID_s \| T_A \| T_s \| c_2)$. If yes, the server S assures the legality of Alice. Otherwise, it stops the authentication process.

After finishing mutual authentication between the server S and Alice, both of them can compute session key with the following equations:
$SK_A = a \times T_s = a \times b \times P$.
$SK_s = b \times T_A = b \times a \times P$.

4.4. Password Changing Phase

During the password changing phase, Alice can change her PW_A freely and securely, without any interaction with TA. The smart card can change password itself after performing the following steps:

Step 1. Alice inputs the original ID_A and PW_A, to the smart card and computes $s_A = m_i - h(PW_A \| K_A)$ check whether $(s_A \times P)$ is equal to PK_A stored in the smart card. If not, the request is rejected.

Step 2. Alice enter PW_A^{new} to compute $m_A^{new} = s_A + h(PW_A^{new} \| K_A)$ after that, the password is updated successfully.

5. Discussion

In this section, we evaluate a security and performance analysis of proposed SIP authentication scheme. The evaluation is divided into two parts: security analysis and comparison with other related approaches in terms of functionality and computational cost.

5.1. Security Analysis

Replay attack. Suppose an attacker Bob replays a request message $(ID_A, R_A, K_A^*, T_A^*)$ and response message $(none^*, realm, Auth_A^*)$ to impersonate Alice. In the proposed scheme, the SIP server will detect this replay and believe Bob to be illegal, this is because Bob cannot construct a valid $Auth_s$.

Offline password guessing attack. In proposed scheme, the password is stored in the smart card, thus, an adversary is unable to guess the password in the transmitting SIP message.

Mutual authentication. The user (Alice) and the SIP server can verify the identity of each other via $Auth_A$ and $Auth_s$. Therefore, the proposed scheme achieves mutual authentication between the user and the server.

Man in the middle attack. An adversary Bob cannot launch the man in the middle attack to fraud the server or user client. Because he needs to pass the verification

Table 3
Computational comparison with others protocols

	11]	[2]	[4]	[5]	[14]	[3]	[9]	Proposed scheme
Exponentiation	0	4	0	0	0	0	0	0
ECC computation	0	0	4	4	6	12	8	12
Hash function	1	8	6	5	7	13	11	8

Table 4
Comparison of the security properties of different schemes

Security attacks	[11]	[2]	[4]	[5]	[14]	[3]	[9]	Proposed scheme
Mutual authentication	NP	P	P	P	P	P	P	P
Perfect forward secrecy	NP	NP	NP	P	P	NP	P	P
No password or verifier table	NP	NP	P	P	P	NP	P	P
Password guessing attack	IS	IS	IS	S	S	S	S	S
Stolen verifier attack	IS	IS	IS	S	S	S	S	S
Data integrity	NP	NP	NP	NP	NP	NP	NP	P
Efficient password change	NP	NP	NP	NP	NP	NP	P	P
Signaling attacks	IS	IS	IS	IS	IS	IS	IS	S
Suitable for different SIP domains	No	No	No	No	No	No	No	Yes

P – provided, NP – not provided, S – secure, IS– insecure

process of the server SIP and to construct a valid session key SK. to generate a session key Bob needs to extract a or b, he faced the elliptic curve discrete logarithm problem.

Stolen verifier attack. An adversary cannot impersonate the user to cheat the SIP server by using stolen information because in this approach there is no password or verification table stored in the SIP server. Consequently, it can resist the stolen verifier attack.

Insider attacks. The proposed scheme process can resist insider attacks, as the SIP server side does not need to store the user password or verifier table, on another side, the private key is chosen by the client, thus cannot be computed or leaked by an insider.

Forward secrecy. Assume that an adversary Bob attempts to find the session key Alice's $SK_A = a.PK_s + sk_A.T_A$. He cannot extract the integer "a" because it is protected by elliptic curve logarithm discrete problem. Thus Bob cannot construct the session key. The forward secrecy is provided.

Data integrity. The shared secret key is obtained during the mutual authentication process. The server can check if the data received from the Alice is correct or not and the same thing for Alice. Therefore, proposed scheme supporting data integrity.

5.2. Performance Comparison

The computation costs of the proposed scheme and previously reported schemes are shown in the Table 3. In general, an 160 bit ECC could offer approximately the same level of security as RSA with 1024 bit key. We divide the computation cost of our scheme into three parts including registration phase, mutual authentication phase, and session key agreement phase. In registration phase, our approach requires two scalar multiplications of elliptic curve. In mutual authentication phase, it needs six scalar multiplications of elliptic curve, two additions of elliptic curve and eight hashing operations. In session key agreement phase, our scheme requires two scalar multiplications of elliptic curve. The total computation cost is $10T_m + 2T_a + 8T_h$.
As shown in Table 3, the approaches no. 2, 3 and 4 reduce the computation cost significantly, but their protocols have some security weakness. The functionality comparison between our scheme and others related scheme is reported in Table 4. Screamingly obvious, proposed scheme can not only solve the security weakness of SIP server, also it is more suitable for different SIP domains.

6. Conclusion

This paper proposes a new authentication and key agreement mechanism using Digital Signature Algorithm Based on ECC, which achieves mutual authentication and key negotiation. Furthermore, the proposed scheme could resist several attacks, such as insider attacks, off-line password guessing attacks, stolen verifier attacks and replay attack. Proposed scheme shows that the corrupted TA cannot obtain the long-term private keys of user clients and the registered servers to launch the forgery attack. Moreover, the proposed authentication protocol is more suitable to authenticate users with different SIP domains.

References

[1] C.-H. Wang and Y.-S. Liu, "A dependable protection for end-to-end VoIP via Elliptic-Curve Diffie-Hellman and dynamic changes", *J. of Netw. and Computer Appl.*, vol. 34, no. 5, pp. 1545–1556, 2011 (doi: 10.1016/j.jnca.2010.10.011).

[2] C.-C. Yang, R.-C. Wang, and W.-T. Liu, "Secure authentication scheme for session initiation protocol", *Comp. & Secur.*, vol. 24, no. 5, pp. 381–386, 2005 (doi: 10.1016/j.cose.2004.10.007).

[3] H.-L. Yeh, T.-H. Chen, and W.-K. Shih, "Robust smart card secured authentication sheme on SIP using Elliptic Curve Cryptography, *Comp. Standards & Interfaces*, vol. 9, no. 2, pp. 397–402, 2014 (doi:10.1016/j.csi.2013.08.010).

[4] L. Wu, Y. Zhang, and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC", *Com. Standards & Interfaces*, vol. 31, no. 2, pp. 286–291, 2009 (doi: 10.1016/j.csi.2008.01.002).

[5] E.-J. Yoon *et al.*, "A secure and efficient SIP authentication scheme for converged VoIP networks", *Comp. Commun.*, vol. 33, no. 14, pp. 1674–1681, 2010 (doi: 10.1016/j.comcom.2010.03.026).

[6] F. Wang and Y. Zhang, "A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography", *Comp. Commun.*, vol. 31, no. 10, pp. 2142–2149, 2008 (doi: 10.1016/j.comcom.2008.01.054).

[7] Y.-P. Liao and S.-S. Wang, "A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves", *Comp. Commun.*, vol. 33, no. 3, pp. 372–380, 2010 (doi: 10.1016/j.comcom.2009.10.005).

[8] R. Arshad and N. Ikram, "Elliptic curve cryptography based mutual authentication scheme for session initiation protocol", *Multimed. Tools & Appl.*, vol. 66, no. 2, pp. 165–178, 2013 (doi: 10.1007/s11042-011-0787-0).

[9] L. Zhang, S. Tang, and S. Zhu, "An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks", *J. of Netw. & Comp. Appl.*, vol. 59, pp. 126–133, 2016 (doi: 10.1016/j.jnca.2015.06.022).

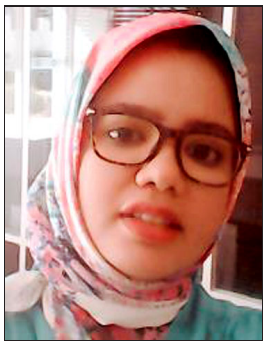
[10] J. Rosenberg *et al.*, "SIP: Session Initiation Protocol", IETF RFC 3261, 2002 [Online]. Available: https://www.ietf.org/rfc/rfc3261.txt

[11] J. Franks *et al.*, "HTTP Authentication: Basic and Digest Access Authentication", IETF RFC 2617, 1999 [Online]. Available: https://www.ietf.org/rfc/rfc2617.txt

[12] N. Koblitz, "Elliptic curve cryptosystems", *Mathem. of Comput.*, vol. 48, no. 177, pp. 203–209, 1987 (doi: 10.1090/S0025-5718-1987-0866109-5).

[13] S. V. D. Johnson, A. Menezes, "The elliptic curve digital signature algorithm (ECDSA)", *Int. J. of Inform. Secur.*, vol. 1, no. 1, pp. 36–63, 2001 (doi: 10.1007/s102070100002).

[14] S. Sadat, M. Nik, and M. Shahrabi, "Mutual SIP authentication scheme based on ECC", *Int. J. of Comp. & Elec. Engin.*, vol. 6, no. 2, pp. 196–200, 2014 (doi: 10.7763/IJCEE.2014.V6.821).



Asma Jebrane received his B.Tech. in 2011 from the Faculty of Sciences Semlalia, University Cadi Ayyad, Morocco. She received her M.Sc. in Instrumentations and telecommunication from the University Ibn Zohr, Morocco, in 2013. She is currently a Ph.D. student at Faculty of Sciences, Ibn Zohr University. Her research interests include information/security, especially VoIP protocol, and cryptography.
E-mail: jebrane.asma@gmail.com
Laboratory of Electronic, the Treatment of Signal and Physical Modeling (LETSMP)
Faculty of Sciences
Ibn Zohr University
B.P 8106, Agadir 80000 Morocco

Ahmed Toumanari received his Ph.D. in Computational Physics in 1999 and Habilitation degree in 2007, from Ibn Zohr University, Morocco. After his experience as a software engineer in GFI company, he is a Professor with the Department of Computer Science, Ibn Zohr University, Agadir, Morocco. Currently, his research interests include security of ad hoc and sensor networks, cloud computing and biomedical image. He is a member of the signals systems and computer science group (ESSI) at National School of Applied Sciences.
E-mail: atoumanari@yahoo.fr
Laboratory of the Systems Engineering and Information Technology
National School of Applied Science
Ibn Zohr University
80000 Agadir Morocco

Naîma Meddah received her M.Sc. in Computer Science in 2008 from the Hassan II University of Science and Technology Casablanca, Morocco. Then, she has been working at Higher Institute of Applied Technologies ISTA OFPPT as a trainer of computer networking techniques. Currently she is a Ph.D. student at National School of Applied Science, Ibn Zohr University, Morocco. Her research interests include: cloud computing, visualization, cloud security and attribute-based cryptography.
E-mail: n.meddah@gmail.com
Laboratory of the Systems Engineering and Information Technology
National School of Applied Science
Ibn Zohr University
80000 Agadir Morocco

Mohamed Bousseta is a Professor with the Department of Physics Faculty of Science Ibn Zohr and a member of Laboratory of Electronic, the Treatment of Signal and Physical Modeling (LETSMP) at Faculty of Sciences Ibn Zohr Agadir, Morocco.

E-mail: m_bosseta60@hotmail.fr
Laboratory of Electronic, the Treatment of Signal and Physical Modeling (LETSMP)
Faculty of Sciences
Ibn Zohr University
B.P 8106, Agadir 80000 Morocco