Research Journal of Applied Sciences 12 (5-6): 352-357, 2017
ISSN: 1815-932X
© Medwell Journals, 2017

Cryptanalysis on Anonymous Two Factor Mutual Authentication with Key Agreement Scheme For Session Initiation Protocol

Younsung Choi
Department of Cyber Security, Howon University, Impi-Myeon, Gunsan-Si,
54058 Jeonrabuk-Do, Korea

Abstract: In order to solve the limitations of the password-based authentication scheme, various two-factor authentication schemes for session initiation protocol is studied and regards it as good solution. In 2015, Lu proposed secure two-factor authenticated key agreement which provide the anonymity and key agreement for session initiation protocol using elliptic curve cryptography. However, Reddy point out the vulnerability the Lu scheme and proposed an enhanced anonymous two-factor mutual authentication with key-agreement scheme for session initiation protocol in 2016 but there are various security problem yet. So, this study analyzes all phases of Reddy authentication scheme and then shows that their scheme is still vulnerable on off-line password (and identity) guessing attack a DoS attack, wrong password change phase and session key disclosure attack.

Key words: Cryptanalysis, session initiation, protocol, security analysis, authentication, scheme

INTRODUCTION

SIP (Session Initiation Protocol) is a useful communications protocol for signaling and controlling multimedia communication sessions. Recently, SIP is the most widely used for the current unified communications and voice through internet protocols. SIP can establish, alter and terminate the connection between various communication parties. SIP is made for application layer protocol and it is designed to be independent of the underlying transport layer. And SIP is integrating many elements of the hypertext transfer protocol and the simple mail transfer protocol. Moreover, SIP is text-based protocol and is used for requests from clients and responses from servers over public communication (Johnston, 2009; Yang *et al*., 2005; Franks *et al*., 1999).

Rosenberg *et al*. (2002) proposed a challenge response based authentication scheme for SIP. Various researchers studies more efficient and secure authentication schemes for SIP after (Rosenberg *et al*., 2002)'s scheme (Irshad *et al*., 2014; He *et al*., 2012; Wang and Zhang, 2008; Wu *et al*., 2009). Lu *et al*. (2015) introduces an anonymous two-factor elliptic curve cryptography based authenticated key agreement scheme for SIP. Lu *et al*. (2015) asserted that their scheme is secure various against attacks and provides anonymity. However, Reddy *et al*. (2016) show that Lu *et al*. (2015)'s scheme is vulnerable on imperfect mutual authentication and agreement, prone to extraction of sensitive information and prone to key-compromise user impersonation attacks. And Reddy *et al*. (2016) proposed security enhanced elliptic curve cryptography based scheme which provide anonymous two-factor mutual authentication with key agreement scheme for SIP. They claimed their scheme provide user anonymity, mutual authentication, perfect forward secrecy and is more secure on various attacks than diverse authentication schemes including Lu *et al*. (2015) scheme. However, this study find out the security vulnerabilities such as off-line password (and identity) guessing attack, a DoS attack, wrong password change phase and session key disclosure attack after analyzing all phases by Reddy *et al*. (2016) authentication scheme.

Table 1: Notations

Notations	Descriptions
U	A user
S	A server
ID_U	Identity of U
PW_U	Password of U
SC	Smartcard of U
r_U, α	Random numbers chosen by U
Pri_S	Private key of S
Pub_S	Public key of S
r_S, β	Random numbers chosen by S
P	A point on the elliptic curve
SK	Session key
||	The concatenation operation
h(·)	A secure one-way hash function
⊕	An exclusive-or operation

Review of Reddy *et al.* (2016)'s scheme: This study proposes, an improved anonymous two-factor authentication with key-agreement for session initiation protocol using elliptic curve cryptography (Reddy *et al*., 2016). The notations of the proposed protocol are listed in Table 1.

MATERIALS AND METHODS

System initialization phase: Before the protocol is ever executed, this scheme computes and shares the secret as follows.

Step 1: S generates a point P on an elliptic curve E(a, b) over F_p.

Step 2: S selects $h(\cdot)$ and $Pri_S \epsilon z^*_p$ calculates $Pub_S = Pri_S \cdot P$.

Step 3: S stores Pri_S and publishes $\{E(a, b), P, Pub_S, h(\cdot)\}$.

User registration phase: For a user U, this phase is performed only once when U registers itself with the server. Algorithm 1 illustrates how the phase works and its description follows.

Algorithm 1 (Reddy *et al.*, 2016)'s user registration phase):

User U   Server S
$\langle ID_U, PW_U\rangle$ $\langle Id_s, k, h(\cdot)\rangle$
Choose ID_U, PW_U, r_U, r
$PID_U = h(ID_U||r_U)$
$RPW = h(PW_U||r_U)\oplus r$

$\xrightarrow{\textbf{(Secure channel) (PID}_\textbf{u}\textbf{, RPW)}}$

$M = h\ (PIDu\backslash\backslash IDs\backslash\backslash k)$
$N = M \oplus RPW$

$\xleftarrow{\textbf{(Secure channel) smart card (N, P, Pub}_\textbf{s}\textbf{, h(.))}}$

$V_1 = r_U \oplus h(ID_U||PW_U)$
$N' = N\oplus r = M\oplus h(PW_U||r_U)$
$V_2 = h(PID_U||h(h(PW_U||r_U))$
$\langle N', V_1, V_2, P, Pub_s, h(\cdot)\rangle$ in smart card

Step 1: User U selects ID_U, PW_U and 2 random numbers r_U and r. Then, calculates:

$$PID_U = h(ID_U || r_U)$$
$$RPW = h(PW_U || r_U) \oplus r$$

and then sends registration request $\{ID_U, RPW\}$ to S using a secure communication.

Step 2: S calculates M, N as:

$$M = h(PID_U||ID_S||k), N = M \oplus RPW$$

and then, S inputs $\{N, P, Pub_S, h(\cdot)\}$ on user's smart card SC and send it to U.

Step 3: U computes V_1, N', V_2 as:

$$V_1 = r_U \oplus h(ID_U || PW_U)$$
$$N' = N \oplus r = M \oplus h(PW_U || r_U)$$
$$V_2 = h(PID_U || h(PW_U || r_U))$$

and then, U stores them on the received smart card SC. Therefore, SC stores $\{N', V_1, V_2, P, Pub_S, h(\cdot)\}$.

Mutual authentication with key-agreement phase: In mutual authentication with key-agreement phase, user U and server S can authenticate each other and compute a session-key. Algorithm 2 shows the process of mutual authentication with key-agreement phase as:

Algorithm 2 (Off-line password (and identity) guessing attack of Reddy *et al.* (2016)'s scheme):

An adversary steals U's smart card and obtains all of information
→So adversaty can gets N', V_1, V_2, P, pub_S, h (.) using physiacl monitoring
The adversary knows the formula of parameters
□ $V_2 = h\ (PID_U\|h\ (PW_U\|r_U))$
□ $PID_U = h(ID_U\|r_U)$
□ $r_U = V_1\oplus h\ (ID_U\|PW_U)$
▣$V_2 = h\ (PID_U\|h\ (PW_U)$
→[Using PID_U] $V_2 = h\ (h(ID_U\|r_U)\|h\ (PWU\|r_U)$
→[Using r_U] $V_2 = h\ (h(ID_U\|V_1\oplus h\ (ID_U\|PW_U))\|h(PW_U\|V_1\oplus h(ID_U\|PW_U))$
→The adversary has V_1, V_2, h (.) and does not know ID_U and PW_U
$|D_{id}|$ and $|D_{PW}|$ denote the number of identities in $|D_{id}|$ and passwords in $|D_{PW}|$
D_{id} and D_{PW} are very limited in practice such as $|D_{id}| \leq |D_{PW}| \leq 10^6$
▣→So, the adversary can obtain ID_U and PW_U from user's smart card

Step 1: U inserts smart card SC and inputs own ID_U and PW_U. SC computes r_U, PID_U:

$$r_U = V_1 \oplus h(ID_U || PW_U)$$
$$PID_U = h(ID_U || r_U)$$

and checks the accuracy $V_2 \approx h(PID_U||h(PW_U||r_U))$. If they are same, then the smart card SC generates a random number α and computes N_U, M, Y as:

$$N_U = a\times P, N'_U = a\times Pub_s$$
$$M = N' \oplus h(PW_U || r_U)$$
$$Y = h(PID_U || N_U || M)$$

and then, user U sends the Request (AID_U, N_U, Y) to server S.

Step 2: S computes N'_U, PID_U, M as:

$$N'_U = Pri_S \cdot N_U, PID_U = AID_U \oplus N'_U$$
$$M = h(PID_U || ID_S || k)$$

and then, verifies $Y \approx h\ (PID_U||N_U||M)$. If they are same, server S authenticates U, otherwise process aborts. S generates a random number β and computes X, N_S, SK_S, $auth_S$:

$$\begin{aligned} X &= M \oplus \beta \\ N_S &= \beta \times N_U^{'} \\ SK_S &= h\left(PID_U \mid\mid N_S \mid\mid \beta\right) \\ auth_S &= h\left(SK_S \mid\mid PID_U \mid\mid M\right) \end{aligned}$$

and then, server S sends challenge (realm, X, $auth_S$) to user U.

Step 3: Using receiving challenge messages, SC computes β, N'_S, SK_U as:

$$\begin{aligned} \beta &= M \oplus X, N_S^{'} = \beta \times N_U^{'} \\ SK_U &= h\left(PID_U \mid\mid N_S^{'} \mid\mid \beta\right) \end{aligned}$$

and then verifies $auth_S$ messages as:

$$auth_S \approx h\left(SK_U || PID_U M\right)$$

If $auth_S$ is same to h $(SK_U||PID_U||M)$, U authenticates S and further computes $auth_U$:

$$auth_U = h\left(SK_U \mid\mid PID_U \mid\mid \beta\right)$$

and then, U sends the RESPONSE(realm, $auth_U$) to server S.

Step 4: Server S checks $auth_U$ = h ($SK_S||PID_U||\beta$). If they are same, S accepts for next communication using computed session key $SK_U = SK_S$.

Password changing phase: Reddy *et al.* (2016)'s protocol allows users to freely update their passwords. The password change phase works as.

Step 1: U inserts SC and enters the existing user's ID_U and PW_U. SC computes r_U:

$$r_U = V_1 \oplus h\left(ID_U \mid\mid PW_U\right)$$

and then, SC verifies the computed value and V_2 as:

$$V_2 \approx h\left(PID_U || h\left(PW_U || \; r_U\right)\right)$$

If $V_2 \approx h\ (PID_U||h(PW_U||r_U))$ are same, then U derives M as:

$$M = N' \oplus h\left(PW_U || r_U\right)$$

Step 2: A user U selects a new password PW_U new and computes RPW^{new}, $V_1{}^{new}$, N'^{new}, $V_2{}^{new}$ as:

$$\begin{aligned} RPW^{new} &= h\left(PW_U^{new} || r_U\right) \oplus r \\ V_1^{new} &= r_U \oplus h\left(ID_U || PW_U^{new}\right) \\ N^{'new} &= M \oplus h\left(PW_U^{new} || r_U\right) \\ V_2^{new} &= h\left(PID_U || h\left(PW_U^{new} || r_U\right)\right) \end{aligned}$$

and then, user S replaces the existing values on the received smartcard. Thus, the smartcard contains $\{N^{'new}, V_1{}^{new}, V_2{}^{new}, P, Pub_S, h(\cdot)\}$.

RESULTS AND DISCUSSION

Cryptanalysis on Reddy *et al.* (2016)'s scheme: We analyze Reddy *et al.* (2016)'s anonymous two-factor mutual authentication with key-agreement scheme for session initiation protocol and determine various security vulnerabilities including off-line password (and identity) guessing attack, a DoS attack, wrong password change phase, session key disclosure attack.

Off-line password (and identity) guessing attack: Reddy *et al.* (2016)'s authentication scheme, an adversary can user's identity and password from user's smart card. It is reason that an attacker can extract the stored information from smart card using Simple Power Analysis (SPA), Differential Power Analysis (DPA). Algorithm 2 shows the process of off-line password (and identity) guessing attack by Reddy *et al.* (2016)'s scheme (Ma *et al*., 2014). An adversary gets or steals the user's smart card and then the adversary obtain the all of information (N', V_1, V_2, P, Pub_s, $h(\cdot)$) from the smart card using physical monitoring such as SPA and DPA which is proved by various studies Kocher and Messerges and the adversary can knows the equation of all parameters such as V_2, PID_U and r_U:

$$\begin{aligned} V_2 &= h\left(PID_U || h(PW_U || r_U\right) \\ PID_U &= h\left(ID_U || r_U\right), r_U = V_1 \oplus h\left(ID_U || PW_U\right) \end{aligned}$$

Using this equation and the parameter extracted from smart cards, the adversary can modify V_2 = h $(PID_U||$ h $(PW_U||r_U)$ as fallows:

$$\text{Using } PID_U \rightarrow V_2 = h\left(h(ID_U || r_U\right) || h\left(PW_U || r_U\right)$$

$$\text{Using } r_U \rightarrow V_2 = h\begin{pmatrix} h\left(ID_U || V_1 \oplus h\left(ID_U || PW_U\right)\right) \\ || h(PW_U || V_1 \oplus h\ \left(ID_U || PW_U\right) \end{pmatrix}$$

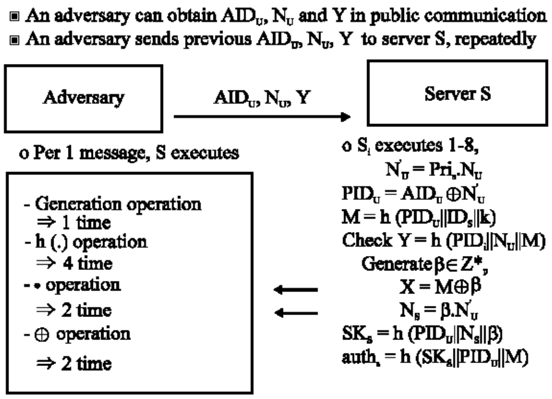
▣ An adversary can obtain AID_U, N_U and Y in public communication
▣ An adversary sends previous AID_U, N_U, Y to server S, repeatedly
Adversary
AID_U, N_U, Y
Server S
o Per 1 message, S executes
- Generation operation
⇒ 1 time
- h (.) operation
⇒ 4 time
- • operation
⇒ 2 time
- ⊕ operation
⇒ 2 time
o S_i executes 1-8,
$N'_U = Pri_s.N_U$
$PID_U = AID_U \oplus N'_U$
$M = h(PID_U||ID_s||k)$
Check $Y = h(PID_i||N_U||M)$
Generate $\beta \in Z^*_p$
$X = M \oplus \beta$
$N_s = \beta.N'_U$
$SK_s = h(PID_U||N_s||\beta)$
$auth_s = h(SK_s||PID_U||M)$

Fig. 1: A DoS attack by Reddy *et al.* (2016)'s scheme

The adversary has V_1, V_2, $h(\cdot)$ frome user's smart card and so does not know ID_U and PW_U on $V_2 = h(h(ID_U||V_1 \oplus h(ID_U||PW_U))||h(PW_U||V_1 \oplus h(ID_U||PW_U))$. But the adversary can guess the ID_U and PW_U because they are both small size. $|D_{id}|$ and $|D_{pw}|$ defined the number of identities in D_{id} and the number of passwords in D_{pw}. If T_H is the running time for Hash, the running time of the aforementioned attack procedure is $O|D_{id}| \times |D_{pw}| \times T_H)$ because both password and identity are human-memorable short strings but not high-entropy keys. So, $|D_{id}|$ and $|D_{pw}|$ are often chosen from two corresponding dictionaries of small size. As $|D_{id}|$ and $|D_{pw}|$ are very limited in practice, $|D_{id}| \leq |D_{pw}| \leq 10^6$, the aforementioned attack can be completed in polynomial time. Therefore, the adversary can ID_U and PW_U using off-line password (and identity) guessing attack on Reddy *et al.* (2016)'s authentication scheme.

DoS attack: Reddy *et al.* (2016)'s scheme does not use the timestamps so they use random number for preventing the replay attack. However, Reddy *et al.* (2016)'s scheme has problem on a DoS attack. Figure 1 shows the possibility of a DoS attack by Reddy *et al.* (2016)'s authentication scheme.

An adversary can obtain and intercept the previous authentication message $\{AID_U$, N_U and $Y\}$ in public communication. Then, the adversary resend $\{AID_U$, N_U and $Y\}$ after user's authentication phase ends. However, the server cannot figure out that the message is previous message and cannot checks the legitimacy of incoming message because the server cannot check and know the freshness of message before $auth_U$ is same to $h(SK_S||PID_U||\beta)$ $(auth_U \simeq h(SK_S||PID_U||\beta))$. So, the server executes various operation such as random number generation operation, hash operation, · operation and exclusive or operation before checking whether $auth_U$ sent by the adversary and computed $h(SK_S||PID_U||\beta)$ are same. Therefore, the adversary can execute the DoS attack without difficulty (Choi *et al.*, 2014, 2016; Moon *et al.*, 2016).

Wrong password change phase: When a user want to change own password, the user process the password change phase but password change phase of Reddy *et al.* (2016)'s scheme has procedural problem (Li *et al.*, 2014; Madhusudhan and Mittal, 2012). To change the password, first the user inputs present ID_U and PW_U. So, the user's smart card computes r_U, M and verifies V_2 as:

$$\begin{aligned} r_U &= V_1 \oplus h(ID_U||PW_U) \\ V_2 &\simeq h(PID_U||h(PW_U||r_U)) \\ M &= N' \oplus h(PW_U||r_U) \end{aligned}$$

Then, the user chooses a new password PW_U^{new} and then have to compute RPW^{new} as:

$$RPW^{new} = h(PW_U^{new}||r_U) \oplus r$$

But the user cannot compute RPW^{new} because the user does not know parameter r. This parameter r is used to protect the $h(PW_U||r_U)$ from the server in registration phase. However, parameter r does not store in the smart card and cannot compute r using other parameters. A parameter related r in smart card is only N′ as:

$$\begin{aligned} &N' = N \oplus r \\ &N = M \oplus RPW = h(PID_U||ID_S||k) \oplus h(PW_U||r_U) \oplus r \\ &\rightarrow N' = h(PID_U||ID_S||k) \oplus h(PW_U||r_U) \oplus r \oplus r \\ &\rightarrow N' = h(PID_U||ID_S||k) \oplus h(PW_U||r_U) \end{aligned}$$

As above formulas, N′ does not contain the information about r because the parameter r is removed by (exclusive or) operation. Therefore, the user by Reddy *et al.* (2016)'s scheme cannot change the user's password because user cannot compute parameter r.

Session key disclosure attack: Reddy *et al.* (2016)'s authentication is vulnerable on session key disclosure attack. An adversary can compute the session key including previous session key using smart card. Algorithm 3 shows session key disclosure attack on Reddy *et al.* (2016)'s scheme (Kumari *et al.*, 2013) as:

Algorithm 3 (Session key disclosure attack by Reddy *et al.* (2016)'s scheme):

An adversary obtains AID and X in public communication
An adversary steals user U' s smart card

An adversary can extracts all information form smart card using SPA, DPA
→So attacker can gets ID_U and PW_U using off-line guessing attack
An adversary has AID, X, ID_U, PW_U, N′ and V
→$r_U = V_1 \oplus h\ (ID_U \| PW_U)$
→$PID_U = h\ (ID_U \| r_U)$
→$N'_U = AID_U \oplus PID_U$
→$M = N' \oplus h\ (PW_U \| r_U)$
→$\beta = M \oplus X$
→$N_S = \beta \cdot N'_U$
→$SK_U = h\ (PID_U \| N'_U \| \beta)$
An adversary know all formula's parameter in $SK_U = h\ (PID_U \| N'_U \| \beta)$
→So An adversary can compute all of previous session key SK_U

Reddy *et al.* (2016)'s scheme, an adversary can obtains all of AID and X (including previous AID, X) in public communication between user and server. The adversary steals user's smart card, then he can extracts all information from smart card using power analysis such as SPA, DPA. And the adversary can compute user's ID_U and PW_U using the stored information. So, the adversary has AID, X, ID_U, PW_U, N′ and V_1, so he can compute the session key using them as following procedures.

$$\begin{aligned}
&r_U = V_1 \oplus h(ID_U \| PW_U) \\
&PID_U = h(ID_U \| r_U)\ (\text{using computed } r_U) \\
&N'_U = AID_U \oplus PID_U\ \ (\text{using computed } PID_U) \\
&M = N' \oplus h(PW_U \| r_U)\ (\text{using computed } r_U) \\
&\beta = M \oplus X(\text{using computed } M) \\
&N_S = \beta \times N'_U\ \ (\text{using computed } \beta) \\
&\rightarrow SK_U = h\left(PID_U \| N'_S \| \beta\right)
\end{aligned}$$

Therefore, the adversary knows and computes all equation's parameter of session key SK_U = h ($PID_U \| N'_S \| \beta$). Moreover, the adversary can calculate all of session key including previous session key.

CONCLUSION

Reddy *et al.* (2016) proposed an anonymous two-factor mutual authenticated key-agreement scheme for session initiation protocol using elliptic curve cryptography overcome the existing security problem but their scheme has security problem. So, this study analyze Reddy *et al.* (2016)'s scheme and point out that this scheme is vulnerable on off-line password (and identity) guessing attack, a DoS attack, wrong password change phase and session key disclosure attack.

ACKNOWLEDGEMENT

This research was supported by financial support of Howon University in 2017.

REFERENCES

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

Choi, Y., Y. Lee and D. Won, 2016. Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction. Intl. J. Distrib. Sens. Networks, 12: 1-16.

Franks, J., P. Hallam-Baker, J. Hostetler, S. Lawrence and P. Leach *et al.*, 1999. HTTP authentication: Basic and digest access authentication. Internet Engineering Task Force, ?Fremont, California, USA.

He, D., J. Chen and Y. Chen, 2012. A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography. Secur. Commun. Networks, 5: 1423-1429.

Irshad, A., M. Sher, M.S. Faisal, A. Ghani and M.U. Hassan *et al.*, 2014. A secure authentication scheme for session initiation protocol by using ECC on the basis of the Tang and Liu scheme. Secur. Commun. Networks, 7: 1210-1218.

Johnston, A.B., 2009. SIP: Understanding the Session Initiation Protocol. 3rd Edn., Artech House Publishers, ISBN: 1607839954, Norwood, MA., Pages: 395.

Kumari, S., M.K. Khan and R. Kumar, 2013. Cryptanalysis and improvement of a privacy enhanced scheme for telecare medical information systems. J. Med. Syst., 37: 1-11.

Li, X., J. Niu, Y. Liu, J. Liao and W. Liang, 2014. Robust dynamic ID-based remote user authentication scheme using smart cards. Intl. J. Ad. Hoc. Ubiquitous Comput., 17: 254-264.

Lu, Y., L. Li, H. Peng and Y. Yang, 2017. An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography. Multimedia Tools Appl., 76: 1801-1815.

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

Madhusudhan, R. and R.C. Mittal, 2012. An Efficient Fingerprint-Based Remote User Authentication Protocol using Mobile Devices. In: Soft Computing for Problem Solving, Kusum, D., N. Atulya, P. Millie and C.B. Jagdish (Eds.). Springer, Berlin, Germany, pp: 569-578.

Moon, J., Y. Choi, J. Kim and D. Won, 2016. An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. J. Med. Syst., 40: 1-11.

Reddy, A.G., E.J. Yoon, A.K. Das and K.Y. Yoo, 2016. An enhanced anonymous two-factor mutual authentication with key-agreement scheme for session initiation protocol. Proceedings of the 9th International Conference on Security of Information and Networks, July 20-22, 2016, ACM, New York, USA., ISBN:978-1-4503-4764-8, pp: 145-149.

Rosenberg, J., H. Schulzrinne, G. Camarillo, A. Johnston and J. Peterson *et al*., 2002. SIP: Session initiation protocol. Internet Engineering Task Force, ?Fremont, California, USA.

Wang, F. and Y. Zhang, 2008. A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography. Comput. Commun., 31: 2142-2149.

Wu, L., Y. Zhang and F. Wang, 2009. A new provably secure authentication and key agreement protocol for SIP using ECC. Comput. Standards Interfaces, 31: 286-291.

Yang, C.C., R.C. Wang and W.T. Liu, 2005. Secure authentication scheme for session initiation protocol. Comput. Secur., 24: 381-386.