A Lightweight Certificateless User Authentication Scheme for Mobile Environment

Alzubair Hassan[1(✉)], Rafik Hamza[1], Vittor Gift Mawutor[2], Akash Suresh Patil[1], and Fagen Li[2]

[1] School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 51006, People's Republic of China
alzubairuofk@gmail.com

[2] Center for Cyber Security, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Abstract. Nowadays, smartphone applications are the most widespread in our daily lives. These applications raised several security concerns such as authentication, key agreement, and mutual authentication. Accordingly, the researchers have been presented several user authentication schemes based on the identity-based cryptography (IBC) and certificateless cryptography (CLC). Smartphones considered as limited resources devices, thus, it needs lightweight protocols. However, the existing schemes are suffering from high computational costs especially the one that depends on CLC. In this paper, a lightweight certificateless user authentication scheme based on the elliptic curve cryptography (ECC) is introduced. The proposed scheme has the lowest computation costs comparing with the existing certificateless user's authentication protocols. Furthermore, The proposed scheme is secure under the computational Diffie-Hellman (CDH) Problem and the elliptic curve discrete logarithm problem (ECDLP). Indeed, the proposed scheme is suitable to use in the mobile client-server environment and the Internet of things (IoT) applications.

Keywords: User authentication · Key agreement · Certificateless cryptography · Elliptic curve cryptography

1 Introduction

It is an undeniable fact that many applications have been introduced to make life more comfortable. Many of these applications are network applications and therefore run in the client-server environment. In the client-server environment, powerful computers called servers provide services and resources to the client devices such as personal computers, laptops and mobile devices. Service providers are able to offer services and resources through these network applications via network [14].

X. Chen et al. (Eds.): ML4CS 2019, LNCS 11806, pp. 112–122, 2019.
https://doi.org/10.1007/978-3-030-30619-9_9

Recent upsurge of mobile environment has in turn increased the demand for network resources and services. These requests have and still being satisfied through the development of mobile applications. Mobile client-server environment contains several applications such as online payment, banking, shopping, and social network applications. These mobile devices have the problem of low computational power and battery limitation. This lead to a major drawback concerning the mobile devices capabilities. Also, the development of these mobile applications has not only help to solve much problem of the demand for network resources and services, but has also introduced other security issues. Therefore, the user authentication and key agreement are important in these applications [10].

By using the user authentication protocol, it easy to ensure that the system dealing with the authorized user. Otherwise, the system will give the service to an unauthorized user which is a danger. There is a need also for key agreement protocol to let the communicating parties (client and server) agree on a key that could be used to secure the communication in the future and the integrity. Many user authentication and key agreement schemes have been proposed and designed followed by the effect of Lamport scheme [13]. However, many of these authentication and key agreement schemes are insecure against many malicious attacks such as a forgery attack and replay attack. Also, many of these schemes are not suitable for mobile clients with low computational capabilities since many of them have high computational costs. From the above-mentioned issues, the mobile client-server environment requires secure user authentication and key agreement protocols. This paper proposes a lightweight certificateless user authentication scheme using elliptic curve cryptography (ECC). The proposed scheme has the lowest computation costs comparing with the existing certificateless user's authentication protocols. According to the security analysis, the proposed scheme is secure under the computational Diffie-Hellman (CDH) Problem and the elliptic curve discrete logarithm problem (ECDLP).

This paper presented as follows. The related works are discussed in Sect. 2. The preliminaries are given in Sect. 3. The proposed scheme is explained in Sect. 4. The result and discussion are introduced in Sect. 5. Finally, the conclusions are shown in Sect. 6.

2 Related Work

Over the years, many user authentication and key agreement protocols have been introduced for mobile client-server environment. These protocols have different authentication credentials. Before we move on to the different works done in this direction of security, we first want to mention the first basic key agreement protocol known as the Diffie-Hellman key agreement protocol [4]. This protocol has been modified in many ways to be able to provide implicit key authentication, which means, only the licit parties can be able to calculate the session key.

Previously, in order to develop an authentication and key agreement protocol, the Public Key Infrastructure (PKI) was employed, but this was very expensive

with regards to the storage and distribution. In order to curb this problem of the PKI, Shamir [16] introduced the identity-based cryptography (IBC). This scheme was not practical due to integer factorization. Boneh and Franklin [2] introduced an identity-based encryption protocol which sparked the idea of client-server protocols.

In 2006, Das et al. [3] proposed an identity-based remote client authentication scheme which was pairing based with smart cards. Goriparthi et al. [7] was able to prove that the scheme of Das *et al.* [3] was not secured against a forgery attack. This means that, the authentication process of the scheme can easily be passed by an adversary. Based on the forgery attack weakness of the above scheme, two different improved schemes were proposed. The first scheme was proposed by Fang and Huang [5] to overcome the forgery attack in [3]. After that, Giri and Srivastava [6] discovered that Fang and Huang' scheme could also not overcome a type of forgery attack and also offline attack. Giri and Srivastava [6] went further to propose another scheme. Their scheme was an improved scheme which could withstand the forgery attack. The scheme made use of public key encryption on smart cards. This made the bilinear pairing operation on the identity-based encryption to utilize more time.

Tseng *et al.* [20] proved that Giri and Srivastava' scheme has a very high computational cost for smart cards possessing low computing capabilities. Tseng et al. [21] presented a more secured pairing-based authentication scheme for wireless clients with smart cards. The proposed scheme provided better performance and could also withstand the forgery attack. Apart from the proposal and the proof, Tseng *et al* [20] showed that the schemes in [3] and [6] were not able to provide mutual authentication. In 2010, Yoon and Yoo [23] proposed a user authentication and key exchange protocol for mobile client-server environment based on Wu *et al.*'s scheme [22] to improve the performance of their scheme. He [11] proposed an efficient user authentication key agreement protocol based on bilinear pairing suitable for mobile client-server environment. He claimed his protocol gives better performance than that of [22] and [11]. In 2013, Sun et al. [18] mentioned that most of the identity-based remote user authentication protocols have an inherent weakness since the server knows all the private keys of clients, therefore very vulnerable to inside attack and also, most of them could not provide user anonymity and perfect forward secrecy. They further went ahead to proposed a novel user authentication protocol for a mobile client-server environment. Recently, Tsai et al. [19] proved that the protocol of Sun et al. could not overcome the inside attack proposed by them. The server in the authentication protocol of Sun et al. could not verify the validity of a user's partial public key.

It is a clear notion that all the identity-based protocols have the inherent key escrow problem. To overcome this issue, Certificateless user authentication protocol can be proposed. Accordingly, all the schemes employed certificateless cryptography (CLC) should be resisted to the adversaries TYPE I and TYPE II as mentioned in [1]. Adversary TYPE I can replace the users' public key, but he/she cannot access the master key of the key generator center (KGC). The adversary TYPE II owns the KGC's master key, but he/she nevertheless can't

substitute the public key of the users. In order to solve the key escrow problem, In 2017, Hassan et al. [8] proposed a certificateless user authentication protocol which was able to solve the key escrow problem. They claimed their scheme is secure against both adversary TYPE I and TYPE II. However, their protocol is not secured against the adversary TYPE II. In order to solve this security issue, Hassan *et al.* [9] proposed another certificateless user authentication protocol for the mobile client-server environment. This scheme proved to be secured and resistant to the adversaries TYPE I and TYPE II, but it has high computational cost due to the use of bilinear pairing. This paper proposes a lightweight protocol which is built on the CLC using ECC to reduce the computational costs in the previous works.

3 Preliminaries

Here, the elliptic curve cryptography and the hardness assumptions are introduced to use later in our proposed scheme.

1. **Elliptic curve cryptography:**
   It is known the elliptic curve clarified on prime field $\mathbb{F}_p$. Allow $\mathbb{E}(\mathbb{F}_p)$ indicates an elliptic curve $\mathbb{E}$ over a prime finite field $\mathbb{F}_p$, which is explained by the following an equation
   $$y^2 = x^3 + ax + b \tag{1}$$
   While $a, b \in \mathbb{F}_p$ and with $\Delta = 4a^3 + 27b^2 \neq 0$. The curve compose of all the points in $\mathbb{E}(\mathbb{F}_p)$ with the point at infinity $\mathcal{O}$. The reader can refer to [12].
2. **The elliptic curve discrete logarithm problem ECDLP:**
   An elliptic curve $\mathbb{E}$ defined over a finite field $\mathbb{F}_q$ is given. Where $P \in \mathbb{E}(\mathbb{F}_q)$ is a point in $\mathbb{E}$ with order n as well as there is a point $Q = lP$ where $0 \leqslant l \leqslant n-1$. It is hard to determine l.
3. **The computational Diffie-Hellman (CDH) Problem:**
   If we have $\mathbb{G}$ is a base point of $\mathbb{E}(\mathbb{F}_p)$ and $P, xP, yP \in \mathbb{G}$.Then, the $xyP \in \mathbb{G}$ could not be computed due to its difficulty.

4 The Proposed Protocol

We have used the work that presented in [12] to design our scheme. Certificateless cryptography with bilinear paring has been used to design the user authentication protocols. However, these protocols have high computational costs. To overcome this problem, we employed CLC with ECC to design a lightweight user authentication and key agreement protocol. In the proposed protocol, the server plays the role of the KGC. The server generates the partial private key for the client, then the client select secret value to prepare the full private key. Accordingly, we have the concept of the CLC used in this protocol. Our proposed protocol compose of the following:

4.1 Setup

– *Setup* (1^{λ}): The server plays the KGC. The server uses λ as security parameter while the public parameters generate as follows:
  1. A set of elliptic curve $(\mathbb{E})$ domain parameters $D = \{q, \mathbb{F}_q, n, a, b, h\}$ are used in our protocol.
  2. The server picks his master secret key $s \in_R \mathbb{Z}_q^*$ and compute the corresponding master public key $P_{pub} = sP$.
  3. Select Two cryptographic secure hash functions $H_1 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_q^*$, $H_2 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G} \times \mathbb{G} \times \mathbb{Z}_q^* \rightarrow \mathbb{Z}_q^*$.
  4. Publish the public parameters $\{D, \mathbb{G}, P, P_{pub}, H_1, H_2\}$ as general.

4.2 Key Extract

In this phase, the public and partial private keys are generated by the server as follows:

1. The client sends his identity ID_c to the server ID_s, then the server uses his secret value s and the set of $\mathbb{E}$ domain parameters to compute the user's partial private key $R_{ID_c} = sP$.
2. After receiving R_{ID_c}, the client selects his secret value $x_{ID_c} \in \mathbb{Z}_q^*$ to compute his full private key (R_{ID_c}, x_{ID_c}) and the public key $PK_{ID_c} = x_{ID_c}P$.

4.3 User Authenticated Key Exchange

1. After the client received the keys from the server, starts communicating with the server as follows:
   (a) Select $1 \leq k \leq n-1$.
   (b) Compute $kP = (x_1, y_1)$.
   (c) Compute $\varsigma = x_1 \bmod n$. if $\varsigma = 0$ then go step (a).
   (d) Choose $\varphi \in_R \mathbb{Z}_q^*$ and Compute $M = \varphi P$. Then, the client sends ID_c and M to the server.
2. The sever reacts as follows after received ID_c and M correctly:
   (a) Select $\beta \in \mathbb{Z}_q^*$. Then, $T = \beta P$ and $R_1 = \beta M$ are computed.
   (b) Compute $h_{ID_c} = H_1(ID_c, ID_s, R_{ID_c}, R_1)$.
   (c) Return T as well as h_{ID_c} to the client.
3. Since T and h_{ID_c} are received correctly, the client calculates the following equations:
   (a) Compute $R_2 = \varphi T$.
   (b) Check whether the received h_{ID_c} its equal to $H_1(ID_c, ID_s, R_{ID_c}, R_2)$.
   (c) Compute $S = k^{-1}(h_{ID_c} + x_{ID_c}\varsigma) \bmod n$. If $S = 0$ then go to step 1.
   (d) Here, the session key is computed as follow $sk = H_2(ID_c, ID_s, R_{ID_c}, R_2, h_{ID_c})$. Then, ς and S are sent to the server.
4. Finally, the server verifies from the validity of ς and S which are received from the client as follows:
   (a) Verify that ς and S are Integer in the internal $[1, n-1]$.
   (b) Compute $w = S^{-1} \bmod n$.

(c) Compute $u_1 = h_{ID_c} w \bmod n$.
(d) Compute $u_2 = \varsigma w \bmod n$.
(e) Compute $X = u_1 P + u_2 P K_{ID_c}$. If $X = \mathcal{O}$ then reject the client. Otherwise, Compute $v = x_1 \bmod n$ where $X = (x_1, y_1)$. Accept the client if and only if $v = \varsigma$.
(f) Here, the session key is computed as follow $sk = H_2(ID_c, ID_s, R_{ID_c}, R_1, h_{ID_c})$ (Fig. 1).

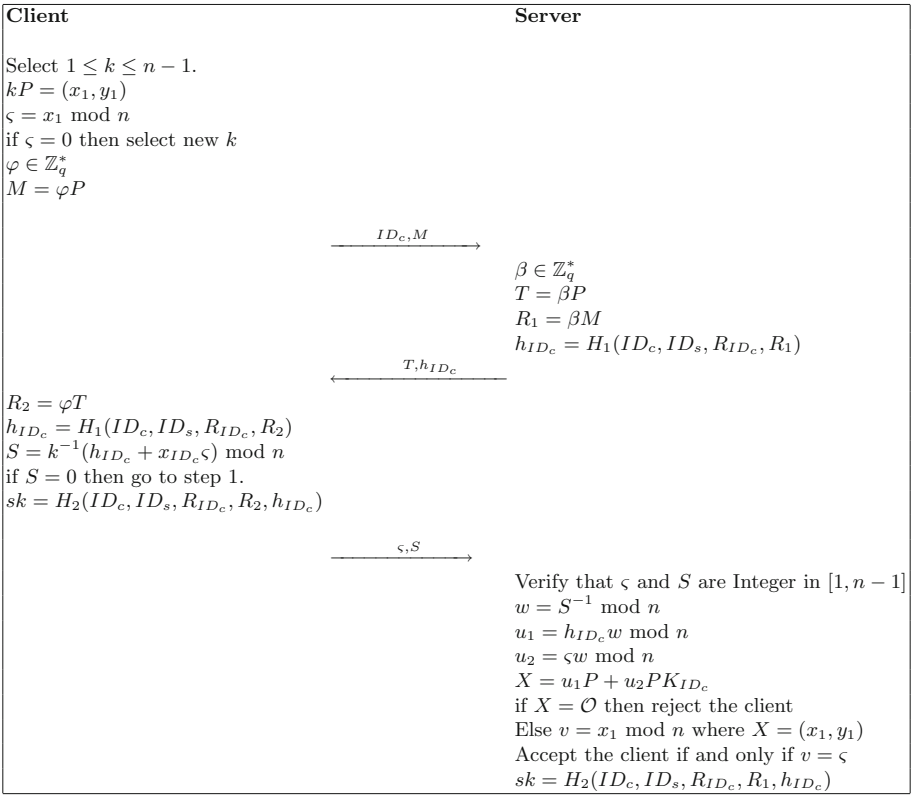

Fig. 1. User authenticated key exchange

4.4 The Correctness of Our Protocol

This subsection describes how the proposed scheme is free of error. Given $T = \beta P$ and $M = \varphi P$, the proposed scheme is correct due to

$$R_2 = \varphi T = \varphi \beta P = \beta \varphi P = \beta M = R_1 \tag{2}$$

In addition, given ς and S to the server. Then $S = k^{-1}(h_{ID_c} + x_{ID_c}\varsigma) \bmod n$. It can be written

$$\begin{aligned} k &\equiv S^{-1}(h_{ID_c} + x_{ID_c}\varsigma) \\ &\equiv S^{-1}h_{ID_c} + S^{-1}x_{ID_c}\varsigma \\ &\equiv wh_{ID_c} + wx_{ID_c}\varsigma \\ &\equiv u_1 + u_2 x_{ID_c}(modn) \end{aligned}$$

Therefore,

$$u_1 P + u_2 P K_{ID_c} = (u_1 + u_2 x_{ID_c})P = kP \tag{3}$$

Then $v = \varsigma$.
Finally, the session key in both sides (client and server) are equal.

$$\begin{aligned} sk =& H_2(ID_c, ID_s, R_{ID_c}, R_2, h_{ID_c}) \\ =& H2(ID_c, ID_s, R_{ID_c}, R_1, h_{ID_c}) \end{aligned}$$

5 Discussion

In this section, we demonstrate the efficiency of the performances and security properties compared with exciting authentication stat-of-art schemes.

5.1 Security Analysis

Our scheme offers user authentication, key agreement and mutual authentication for the mobile client-server environment. In the following discussion, we give a brief description of how our scheme satisfied the abovementioned security aspects as follows:

1. **User authentication:**
   Our scheme provides user authentication since it is depend on the elliptic curve digital signature algorithm (EDSA) in [12] which is secure under ECDLP. The client sends ς and S as a signature to the server. Then, the server needs to verify from the client by ensuring that ς and S are an integer in $[1, n-1]$. Adversary can not forge the signature due to the ECDLP.
2. **Key agreement:**
   The proposed scheme provide the key agreement which can be used for the future communication between both client and server. To get the session key, the adversary needs to solve the CDH problem in sk. The key agreement is $sk = H_2(ID_c, ID_s, R_{ID_c}, R_2, h_{ID_c}) = H_2(ID_c, ID_s, R_{ID_c}, R_1, h_{ID_c})$. The adversary cannot get access to the key agreement due to the CDH problem in R_2 and R_1.

3. **Mutual authentication:**
Our scheme enjoys mutual authentication and it is secure under CDH. The server can be sure that he is communicated with the right client by computing T and $h_{ID_c} = H_1(ID_c, ID_s, R_{ID_c}, R_1)$ in the server side. Then, the server sends T and the value of h_{ID_c} to the client to compute R_2 and $H_1(ID_c, ID_s, R_{ID_c}, R_2)$ as a value of h_{ID_c}. If a client gets the right value of the h_{ID_c}, then the server authenticates from the client. Otherwise, the server is communicated by the wrong client. The adversary cannot compromise the h_{ID_c} and T due to the CDH.

5.2 Performance Analysis

We conduct the performances evaluation regarding the security properties, the computational cost and the communication overhead of the proposed scheme compared with the existing protocols. The comparisons are done with He's scheme [11] (symbolize it by HDE), Hassan *et al.*'s scheme [9] (symbolize it by AHC). We represent a bilinear pairing operation time by T_{pr}, multiplication in $\mathbb{G}_1$ time by T_{mu}, inversion operation time by T_{inv}, addition in $\mathbb{G}_1$ time by T_d and hash function time by T_h.

The basis of our quantitative analysis is based on Scott*et al.*'s experimental results [15] as introduced in Table 1. From their experiment, Pentium IV with speeds 3 GHz, was employed to simulate the server. The Philips HiPersmart card provided a 32-bit RISC MIPS, 256 KB flash memory, 16 KB RAM and a maximum clock speed of 36 MHz was used to simulate the client. Their experiment considered the security level of the Ate pairing system, and employed an elliptic curve $\mathbb{E}$ over a finite field $\mathbb{F}_p$, with $p = 512$ bits and a large prime order $q = 160$ bits.

Table 1. Computation cost at client side and server side

	T_{pr}	T_{mu}	T_d	T_{inv}	T_H
Server	3.16 ms	1.17 ms	< 0.1 ms	< 1 ms	0.01 ms
Client	0.38 s	0.13 s	< 0.1 s	< 0.01 s	< 0.001 s

Table 2. Computational costs

	HDE [11]	AHC [9]	Ours
Client-time	$3T_m + 3T_h + T_{inv}$	$5T_{mu} + T_{ad} + 4T_h$	$5T_{mu} + 3T_d + 2T_h + T_{inv}$
Processing-time	0.266 s	0.754 s	0.962 s
Server-time	$T_{pr} + 2T_m + 2T_d + 3T_h$	$2T_{pr} + 4T_{mu} + 2T_d + 6T_h$	$T_{mu} + T_d + 2T_h + T_{inv}$
Processing-time	9.26 ms	11.26 ms	2.29 ms

The theoretical analysis is introduced to calculate the computational cost in Table 2. As a result, we find that the proposed scheme has the lowest computational cost in server side and the reasonable cost in the client side compared with

the existing protocols [9,11]. Hence, the proposed scheme has the advantage of working with mobile-based applications and IoT environment due to the use of the ECC scheme. In Table 3, we use ✓ to express that a scheme enjoys specified security properties, as well as ✗ to express that a scheme does not enjoy the specified security properties. Table 3 gives a comparison based on the security properties.

Table 3. Security properties

	HDE [11]	AHC [9]	Our protocol
Mutual authentication	✓	✓	✓
Key agreement	✓	✓	✓
Resistance to forgery attack	✓	✓	✓
Perfect forward-secrecy	✗	✓	✓
No key escrow problem	✗	✓	✓
Based ECC	✗	✗	✓

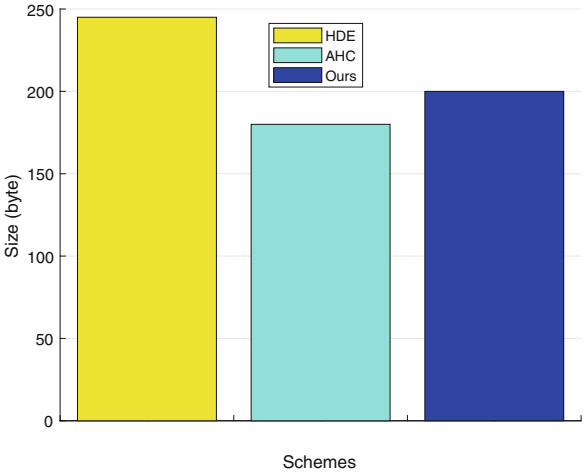

Fig. 2. Communication cost

To get the communication overhead, we compute the transformed elements between the client and server in all the schemes by using the following notation. Let $|ID| = \frac{80}{8} = 10$ bytes and employing the curve with $q = \frac{160}{8} = 20$ bytes, where the size of $\mathbb{G}_1$ is 1024 bits. Here, the size of $\mathbb{G}_1$ reduced to 65 bytes by using the compression method in [17].

The communication cost for He [11], Hassan *et al.* [9], and our scheme are shown as $|ID| + 2|\mathbb{Z}_q^*| + 2|\mathbb{G}_1| = 10 + 2 \times 20 + 3 \times 65 = 245$ bytes, $|ID| + 2|\mathbb{Z}_q^*| + 2|\mathbb{G}_1| = 10 + 2 \times 20 + 2 \times 65 = 180$ bytes and $|ID| + 3|\mathbb{Z}_q^*| + 2|\mathbb{G}_1| = 10 + 3 \times 20 + 2 \times 65 = 200$ bytes, respectively (see Fig. 2).

6 Conclusion

This paper presented a lightweight user authentication protocol with a key agreement and mutual authentication. The proposed scheme employed certificateless cryptography to solve the key escrow problem of identity-based cryptography, as well as the elliptic curve cryptography to reduce the computational and communication costs. Our protocol is secure under the hard assumptions CDH and ECDL problems. Indeed, Our protocol is fitting for both the mobile and IoT applications in client-server environments.

References

1. Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-40061-5_29
2. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. SIAM J. Comput. **32**(3), 586–615 (2003)
3. Das, M.L., Saxena, A., Gulati, V.P., Phatak, D.B.: A novel remote user authentication scheme using bilinear pairings. Comput. Secur. **25**(3), 184–189 (2006)
4. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
5. Fang, G., Huang, G.: Improvement of recently proposed remote client authentication protocols (2006)
6. Giri, D., Srivastava, P.: An improved remote user authentication scheme with smart cards using bilinear pairings. IACR Cryptology ePrint Arch. **2006**, 274 (2006)
7. Goriparthi, T., Das, M.L., Negi, A., Saxena, A.: Cryptanalysis of recently proposed remote user authentication schemes. IACR Cryptology ePrint Arch. **2006**, 28 (2006)
8. Hassan, A., Eltayieb, N., Elhabob, R., Li, F.: A provably secure certificateless user authentication protocol for mobile client-server environment. In: Barolli, L., Zhang, M., Wang, X. (eds.) EIDWT 2017. LNDECT, vol. 6, pp. 592–602. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59463-7_59
9. Hassan, A., Eltayieb, N., Elhabob, R., Li, F.: An efficient certificateless user authentication and key exchange protocol for client-server environment. J. Ambient Intell. Humaniz. Comput. **9**(6), 1713–1727 (2018)
10. Hassan, A., Omala, A.A., Ali, M., Jin, C., Li, F.: Identity-based user authenticated key agreement protocol for multi-server environment with anonymity. Mobile Netw. Appl. **24**(3), 890–902 (2019)
11. He, D.: An efficient remote user authentication and key agreement protocol for mobile client-server environment from pairings. Ad Hoc Netw. **10**(6), 1009–1016 (2012)
12. Johnson, D., Menezes, A., Vanstone, S.: The elliptic curve digital signature algorithm (ECDSA). Int. J. Inf. Secur. **1**(1), 36–63 (2001)
13. Lamport, L.: Password authentication with insecure communication. Commun. ACM **24**(11), 770–772 (1981)
14. Odelu, V., Das, A.K., Kumari, S., Huang, X., Wazid, M.: Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. Future Gener. Comput. Syst. **68**, 74–88 (2017)

15. Scott, M., Costigan, N., Abdulwahab, W.: Implementing cryptographic pairings on smartcards. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 134–147. Springer, Heidelberg (2006). https://doi.org/10.1007/11894063_11
16. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5
17. Shim, K.A., Lee, Y.R., Park, C.M.: EIBAS: an efficient identity-based broadcast authentication scheme in wireless sensor networks. Ad Hoc Netw. **11**(1), 182–189 (2013)
18. Sun, H., Wen, Q., Zhang, H., Jin, Z.: A novel remote user authentication and key agreement scheme for mobile client-server environment. Appl. Math. Inf. Sci. **7**(4), 1365 (2013)
19. Tsai, J.L.: Comments on a novel user authentication and key agreement scheme. IACR Cryptology ePrint Arch. **2014**, 115 (2014)
20. Tseng, Y.M., Wu, T.Y., Wu, J.D.: A mutual authentication and key exchange scheme from bilinear pairings for low power computing devices. In: 31st Annual International Computer Software and Applications Conference (COMPSAC 2007), vol. 2, pp. 700–710. IEEE (2007)
21. Tseng, Y.M., Wu, T.Y., Wu, J.D.: A pairing-based user authentication scheme for wireless clients with smart cards. Informatica **19**(2), 285–302 (2008)
22. Wu, T.Y., Tseng, Y.M.: An efficient user authentication and key exchange protocol for mobile client-server environment. Comput. Netw. **54**(9), 1520–1530 (2010)
23. Yoon, E., Yoo, K.: A new efficient id-based user authentication and key exchange protocol for mobile client-server environment. In: 2010 IEEE International Conference on Wireless Information Technology and Systems, pp. 1–4. IEEE (2010)