Journal of King Saud University – Computer and Information Sciences (2017) 29, 63–73

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication

SK Hafizul Islam [a,*], G.P. Biswas [b]

[a] Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India
[b] Department of Computer Science and Engineering, Indian School of Mines, Dhanbad 826004, Jharkhand, India

Received 2 September 2014; revised 26 December 2014; accepted 13 January 2015
Available online 6 November 2015

KEYWORDS

Elliptic curve cryptography;
Identity-based cryptosystem;
Bilinear pairing;
Session key;
BAN logic

Abstract Recently, many identity-based two-party authenticated key agreement (ID-2PAKA) protocols using elliptic curve cryptography (ECC) have been proposed, however, these protocols do not provide adequate security and their computation costs are also relatively high due to bilinear pairing and map-to-point function. Moreover, they require many communication rounds for establishing the session key, and thus results in increased communication latency, which makes them unsuitable for real applications. This paper thus aims to propose a pairing-free ID-2PAKA protocol based on ECC that removes the security flaws of previous protocols. The proposed protocol helps two users to establish a common session key between them through an open network. The formal security analysis using BAN logic and the comparisons with other protocols are given, which demonstrated that our protocol is formally secure and thus, suitable for secure and efficient peer-to-peer communications.

1. Introduction

The flexibility and the mobility of mobile networks help the mobile users to access the network at anytime from anywhere with their personal devices (i.e., laptop, mobile phone). Further, the rapid advancement and deployment of mobile networks, and the portability of hand-held mobile devices attract mobile users to communicate with each other over mobile networks. However, the security and the privacy protection of communicating users in mobile networks are still two important issues, which must be achieved before using the mobile network for various purposes. Recently, the authenticated key agreement protocols are becoming popular with great attention paid for secure and reliable communication in many wireless mobile applications such as IP Multimedia Subsystem (Song et al., 2011), authentication protocol (Wang et al., 2010; Islam and Biswas, 2011; Lee et al., 2011), wireless mobile ad hoc networks (Liaw et al., 2005), mobile

* Corresponding author. Tel.: +91 8233348791, +91 8797369160.
E-mail addresses: hafi786@gmail.com, hafizul.ism@gmail.com, hafizul@pilani.bits-pilani.ac.in (S.H. Islam).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2015.01.004

IP registration (Sadhukhan et al., 2011), etc. In general, two types of authenticated key agreement protocols can be found: authenticated group key agreement protocol (Znaidi and Minier, 2011; Park and Jin, 2010; Kim and Kim, 2011; Islam and Biswas, 2012) and two-party authenticated key agreement (2PAKA) protocol (Smart, 2002; Chen and Kudla, 2002; Shim, 2003; Sun and Hsieh, 2003; Ryu et al., 2004; Boyd and Choo, 2005; Wang et al., 2009, 2008; McCullagh and Barreto, 2005; Xie, 2004; Li et al., 2005; Choie et al., 2005; Zhu et al., 2007; Cao et al., 2008, 2010; Islam and Biswas, 2012; Hölbl et al., 2012). The authenticated group key agreement protocols allow users (more than two) to come up with a common secret session key between them, whereas in the 2PAKA protocol, a common session is established between two communicating users. In both cases, the users can securely exchange the message encrypted by the session key over any hostile network. In the literature, the password-based authenticated key exchange protocol (Sui et al., 2005; Lu et al., 2007; Chang and Chang, 2008; Lo et al., 2010; Pu, 2010; Youn et al., 2011; Guo et al., 2008, 2012) can also be found, which allows two communicating users to generate a session key over any open network. However, the high computation cost and numerous communication rounds of these protocols, where a secret or a password is shared between a pair of users or with a trusted server prior to communication, makes them unsuitable for environments of low-power mobile devices. Therefore, this paper concentrates on the design of a secure and pairing-free ID-2PAKA protocol using elliptic curve cryptography (ECC) Miller et al., 1985; Koblitz, 1987 and identity-based cryptosystem (IBC) Shamir et al., 1981 suitable for low-power mobile devices.

1.1. Discussion about relevant works

In the literature, several ID-2PAKA protocols based on bilinear pairing along with a map-to-point hash function that is used to convert a random string to point on the elliptic curve group, and ECC have been proposed and some of them are discussed now. Based on the identity-based encryption scheme (Boneh and Franklin, 2001), Smart (2002) proposed an ID-2PAKA protocol, but it does not provide the perfect forward secrecy (PFS) of the session key (Chen and Kudla, 2002; Shim, 2003). Shim (2003)) proposed an efficient ID-2PAKA protocol using Weil pairing and claimed that it removes the security flaws of Smart (2002). Sun and Hsieh (2003)) demonstrated that Shim's protocol is not secure against the man-in-the-middle attack (MIMA). Based on the bilinear pairing, Ryu et al. (2004) proposed an ID-2PAKA protocol, which has vulnerability against the key-compromised impersonation (K-CI) attack (Boyd and Choo, 2005). In 2009, Wang et al. (2009) independently showed that Ryu's protocol is not secure against the reflection attack (RA) and then proposed an improved protocol and claimed that known attacks are protected. Xie (2004) showed that the ID-2PAKA protocol proposed by McCullagh and Barreto (2005) is not secure against the K-CI attack and then proposed an enhanced protocol. However, Li et al. (2005) analyzed that Xie's protocol is still insecure against the K-CI attack. In 2008, Wang et al. (2008) proposed an improved protocol over Chen and Kudla's protocol. In 2005, Choie et al. (2005) proposed some efficient pairing-based ID-2PAKA protocols, and claimed that the protocols are designed to provide required security attributes with minimal communication overheads.

In 2005, Sui et al. (2005) proposed an ECC-based password-based authenticated key agreement protocol, which offers PKG's (private key generator) perfect forward security and was included in 3GPP2 (third generation partnership project) specifications to improve the security of the authenticated key distribution protocol useful for wireless communications. However, Lu et al. (2007) shows that the protocol is vulnerable to the off-line password guessing attack, and then proposed an improvement of the protocol in Sui et al. (2005). Unfortunately, Chang and Chang (2008) proved that Lu et al.'s protocol is not secure against the password guessing attack and then proposed a modified protocol to remove the security flaws of Lu et al. (2007). However, Lo et al. (2010) demonstrated that Chang et al.'s protocol lacks to provide the mutual authentication property. Lo et al. also proposed an improved password-based authenticated key agreement protocol using ECC and claimed that the protocol could resist various attacks. In 2010, (Pu, 2010) independently demonstrated that Lu's protocol could not resist the off-line password guessing attack. Recently, Youn et al. (2011) have discovered some security weaknesses of Guo et al.'s protocol (Guo et al., 2008) and proposed an efficient protocol. In 2012, Guo et al. (2012) proposed another efficient and provably secure password-based authenticated key agreement protocol for wireless communications.

1.2. Motivations

Most of the 2PAKA protocols proposed so far can be implemented using two costly operations such as bilinear pairings and map-to-point (MTP) function. In addition, some of these protocols need a number of communication rounds for successful key establishment, which in turn leads to high communication latency. In order to reduce the computation cost, Zhu et al. (2007) and Cao et al. (2008) independently proposed two pairing-free ID-2PAKA protocols, but these protocols require three communication rounds. In 2010, Cao et al. (2010) proposed another two-round pairing-free ID-2PAKA protocol with minimum computation costs. Unfortunately, (Islam and Biswas, 2012) demonstrated that Cao et al.'s protocol (Cao et al., 2010) is vulnerable to known session-specific temporary attack (KSTIA) and key off-set attack (KOA)/key replicating attack (KRA). From these discussions, it can be concluded that the previous protocols are unsuitable for resource-constrained (battery-power, processing, memory or computation) environments for the following reasons: (1) most of the existing authenticated key agreement protocols have high computation costs and communication rounds, and none of them can provide adequate security, (2) in some password-based authenticated key agreement protocols, two users in a group can achieve mutual authentication and session key agreement if they share a password (secret) in advance, which is unsuitable for large scale peer-to-peer communication networks, since each user is required to keep a large number of secrets corresponding to all group members, and (3) in other password-based authenticated key agreement protocols, each user pre-shares a secret with a trusted server and communicates with other users via the server for which many communication rounds are to be performed. As we know, the

communication latency and the energy consumption increase with the number of communication rounds and thus, more delay is involved in the transmit-response phase of the participating users. Lack of security and computation of the earlier protocols also encourage us to investigate and develop a new secure 2PAKA protocol that can easily be used for low-power mobile devices.

1.3. Our contributions

In this paper, we proposed an improved pairing-free ID-2PAKA protocol using ECC and IBC for two-party communication through an insecure channel, which possesses minimum communication rounds. The proposed protocol is secure, user-friendly and suitable for mobile networks due to the following properties:

(1) *Elimination of public key certificate*: The proposed ID-2PAKA protocol is based on the identity-based cryptosystem, which has an inherent property that it does not require any certificate to authenticate the public key. Accordingly, our protocol does not require any public key certificate to authenticate users' public key.
(2) *Bilinear pairing- and MTP hash function- free realization*: In the literature, many pairing-free ID-2PAKA protocols (Cao et al., 2008, 2010; Debiao et al., 2011) have been designed. The relative computation cost of the bilinear pairing is approximately two to three times more than an elliptic curve scalar point multiplication (ECPM) and the computation cost of the MTP hash function is more than an ECPM (Cao et al., 2010; Islam and Biswas, 2012). In addition, the implementation of bilinear pairing needs a non-singular elliptic curve group with large order and the MTP hash functions usually implemented as a probabilistic algorithm (Zhu et al., 2007; Cao et al., 2008). Similar to the protocols given in Cao et al. (2008, 2010), the proposed protocol is easy to implement as it is free from bilinear pairing and MTP function.
(3) *Formal security*: In the literature, most of the 2PAKA protocols claimed their security informally, which may not be considered to be fully secured against all attacks. However, we analyzed our protocol formally based on the BAN logic model, which assures the security of the proposed protocol claimed in this paper. It also provides all other security attributes of an ID-2PAKA protocol (Blake-Wilson et al., 1997).

1.4. Outline of the paper

The rest of the paper is organized as follows. In Section 2, we have described some preliminaries, which are used throughout the paper. Section 3 described the proposed protocol and its security analysis using the BAN logic model is given in Section 4. A comparison of our protocol with the related protocols in terms of security, computation and communication costs is given in Section 5. Finally, the paper ended with some remarks in Section 6.

2. Preliminaries

In this section, we have discussed the preliminaries of the theory of elliptic curve cryptography, identity-based cryptosystem and some computational problems.

2.1. Elliptic curve cryptography

Miller et al. (1985) and Koblitz (1987) first proposed the elliptic curve cryptography (ECC) and it is believed that the computation of ECC-based discrete logarithm problem using any polynomial-time bounded algorithm is computationally infeasable. In addition, a 160 bit size ECC-based key offers the same level of security as that obtained using a 1024 bit RSA-based key. Further, the elementary operations like point multiplication, addition etc. in the elliptic curve group are much faster than the modular exponentiation executed in the multiplicative group. Therefore, the ECC-based protocols are efficient in terms of (1) security, (2) computation, (3) storage and (4) communication bandwidth.

Let $E_p(a,b)$ be a set of elliptic curve points over the prime field F_p, defined by the following non-singular elliptic curve equation:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \text{ with } x, y, a, b \in F_p \text{ and } (4a^3 + 27b^2) \bmod p \neq 0 \quad (1)$$

The additive cyclic elliptic curve group defined as $G_p = \{(x,y) : x, y \in F_p \text{ and } (x,y) \in E_p(a,b)\} \cup \{O\}$, where the point O is known as "*point at infinity*" or "*zero point*". A brief discussion about the elliptic curve group properties is given below:

- *Point addition*. Let P, Q be two points on the curve (1), then $P + Q = R$, where the line joining P and Q intersects the curve (1) at $-R$, and the reflection of it with respect to the *x-axis* is the point R.
- *Point subtraction*. If $Q = -P$, then $P + Q = P - P = O$ i.e., the line joining P and $-P$ intersects the curve (1) at the point O.
- *Point doubling*. Point doubling is the addition of a point P on the curve (1) to itself to obtain another point Q on the same curve. Let $2P = Q$, the tangent line at P intersects the curve (1) at $-Q$; reflection of it with respect to the *x-axis* is the point Q. The scalar point multiplication on the cyclic group G_p is defined as $kP = P + P + \cdots + P\,(k \text{ times})$.
- *Order of a point*. A point P has order n if $nP = O$ for smallest integer $n > 0$. More about the elliptic curve and its group properties can be found in Hankerson et al. (2004).

2.2. Identity-based cryptosystem

The traditional PKI-based cryptosystem needs a certificate to authenticate user's public key. However, the PKI-based system suffers from the problem of management of public keys and certificates for a large organization. These difficulties can be defeated by means of identity-based cryptography (IBC) proposed by Shamir et al. (1981). In IBC, a publicly known string such as email address, physical IP address, etc. is used as a

public key and a trusted third-party, called private key generator (PKG) creates user's private key by binding his/her master private key and the identity of the user. The user's private key, which is given by PKG to the corresponding user through a secure channel, is only known to the corresponding user and PKG. The main advantages of using IBC includes: (1) elimination of public key certificates, (2) public keys need not to be exchanged prior to the communication, (3) public keys can be revoked easily by binding an expiry date to the public key, etc. Compared with PKI-based cryptosystems, IBC provides more lightweight, flexible usage and easy management of public keys and thus, it is efficiently applicable to real environments. Note that, (Shamir et al., 1981) does not proposed a true identity-based encryption/decryption scheme, however, (Boneh and Franklin, 2001) first proposed a practical identity-based encryption scheme using bilinear pairing over the elliptic curve group.

2.3. Computational problem

Definition 1. Elliptic curve discrete logarithm problem (ECDLP): Given two random elements $P, Q \in G_p$, for any polynomial time algorithm it is computationally hard to find the integer $a \in_R Z_p^*$ such that $Q = aP$.

Definition 2. Computational Diffie–Hellman problem (CDHP): Given a random instance $(P, aP, bP) \in G_p$ for any $a, b \in_R Z_p^*$, computation of abP is infeasible by any polynomial time algorithm.

3. The proposed pairing-free ID-2PAKA protocol

This section proposed a pairing-free ID-2PAKA protocol, which eliminates the security flaws of protocols available in the literature without increasing the communication rounds. The list of notations used in the proposed protocol is explained in the Table 1. The proposed protocol consists of three entities, namely a trusted private key generator (PKG) and two users A and B, who act as the initiator and responder, respectively. The protocol comprises three algorithms like **Setup**, **Extract** and **Key agreement**, each of which is described below:

3.1. Setup phase

This algorithm takes a security parameter $k \in \mathbb{Z}^+$ as input, and returns system's parameter and a master key. Given k, PKG does the following:

(a) Chooses a k-bit prime p and determines the tuple $\{F_p, E/F_p, G_p, P\}$, where the point P is the generator of G_p.
(b) Chooses the master key $x \in_R Z_p^*$ and computes the system public key $P_{pub} = xP$.
(c) Chooses three one-way and secure hash functions $H_0 : \{0,1\}^* \times G_p \longrightarrow Z_p^*$, $H_1 : G_p^3 \longrightarrow Z_p^*$ and $H_2 : \{0,1\}^* \times \{0,1\}^* \times G_p^6 \longrightarrow \{0,1\}^k$.
(d) Publishes $\Omega = \{F_p, E/F_p, G_p, p, P, P_{pub}, H_0, H_1, H_2\}$ as the system's parameter and keeps the master key x secret.

3.2. Extract phase

This algorithm takes PKG's master private key, identity of a user, and the system's parameter as input, and then returns the identity-based long-term private key of a user as explained below. For a user A with identifier ID_A, the PKG executes the following:

(a) Chooses $r_A \in_R Z_p^*$, computes $R_A = r_A P$ and $h_A = H_0(ID_A, R_A)$.
(b) Computes $d_A = (r_A + h_A x) \bmod p$.

PKG sends (d_A, R_A) via a secure and confidential channel to the user A. The corresponding public key of A is computed as $P_A = R_A + H_0(ID_A, R_A)P_{pub}$ and the private/public key pair (d_A, P_A) can be verified by checking whether the equation $P_A = R_A + H_0(ID_A, R_A)P_{pub} = d_A P$ holds. Since

Table 1 List of notations and their meanings used in the proposed pairing-free ID-2PAKA protocol.

Notation	Description
PKG	Private Key Generator
ID_i	Identity of the user i, $i \in \{A, B\}$.
p	A large prime number
$E_p(a, b)$	A set of elliptic curve points over the prime field F_p
P	Base point of the elliptic curve group of order n
$H_i()$	One-way and secure hash function, $i = 0, 1, 2$
d_A	Private key of A, where $d_A = (r_A + h_A x) \bmod p$, $r_A \in Z_p^*$, $R_A = r_A P$, $h_A = H_0(ID_A, R_A)$
P_A	Public key of A, where $P_A = R_A + h_A P_{pub} = d_A P$
d_B	Private key of B, where $d_B = (r_B + h_B x) \bmod p$, $r_B \in Z_p^*$, $R_B = r_B P$, $h_B = H_0(ID_B, R_B)$
P_B	Public key of B, where $P_B = R_B + h_B P_{pub} = d_B P$
a	Random number chosen by the user A, where $T_A = (a + d_A)^2 P$
b	Random number chosen by the user B, where $T_B = (b + d_B)^2 P$
S_A	Signature of (T_A, R_A) computed by A as $S_A = (a + d_A)^2 (d_A + H_1(T_A, R_A))^{-1}$
S_B	Signature of (T_B, R_B) computed by B as $S_B = (b + d_B)^2 (d_B + H_1(T_B, R_B))^{-1}$
SK	Session key, where $SK = H_2(ID_A, ID_B, T_A, T_B, K_A) = H_2(ID_A, ID_B, T_A, T_B, K_B)$ and $K_A = (a + d_A)^2 T_B = (a + d_A)^2 (b + d_B)^2 P = (b + d_B)^2 T_A = K_B$

User A	User B
Select $a \in_R Z_p^*$	Select $b \in_R Z_p^*$
Compute $T_A = (a+d_A)^2 P$	Compute $T_B = (b+d_B)^2 P$
Compute $S_A = (a+d_A)^2 (d_A + H_1(T_A, R_A))^{-1}$	Compute $S_B = (b+d_B)^2 (d_B + H_1(T_B, R_B))^{-1}$
$(ID_A, T_{A1}, T_{A2}, R_A, S_A) \rightarrow$	
	$\leftarrow (ID_B, T_{B1}, T_{B2}, R_B, S_B)$
Compute $P_B = R_B + H_0(ID_B, R_B) P_{pub}$	Compute $P_A = R_A + H_0(ID_A, R_A) P_{pub}$
Verify $S_B(P_B + H_1(T_B, R_B)P) = T_B$	Verify $S_A(P_A + H_1(T_A, R_A)P) = T_A$
Compute $K_A = (a+d_A)^2 T_B$	Compute $K_B = (b+d_B)^2 T_A$
Compute he session key $SK = H_2(ID_A, ID_B, T_A, T_B, K_A)$	Compute the session key $SK = H_2(ID_A, ID_B, T_A, T_B, K_B)$

Figure 1 Key agreement phase of the proposed protocol.

$$\begin{aligned} P_A &= R_A + H_0(ID_A, R_A) P_{pub} \\ &= r_A P + H_0(ID_A, R_A) xP \\ &= (r_A + H_0(ID_A, R_A) x) P \\ &= (r_A + h_A x) P \\ &= d_A P \end{aligned}$$

3.3. Key agreement phase

Step 1. The user A selects $a \in_R Z_p^*$ and performs the following:

(1) Compute $T_A = (a+d_A)^2 P$ and $S_A = (a+d_A)^2 (d_A + H_1(T_A, R_A))^{-1}$.
(2) Send(ID_A, T_A, R_A, S_A) through an open channel to B.

Step 2. On receiving the message (ID_A, T_A, R_A, S_A), B chooses $b \in_R Z_p^*$ and does the following:

(1) Computes $T_B = (b+d_B)^2 P$ and $S_B = (b+d_B)^2 (d_B + H_1(T_B, R_B))^{-1}$.
(2) Sends (ID_B, T_B, R_B, S_B) over an open channel to A.

Step 3. Now, A and B execute the following operations:

(1) A computes $P_B = R_B + H_0(ID_B, R_B) P_{pub}$ and checks whether $S_B(P_B + H_1(T_B, R_B)P) = T_B$ holds. If it holds, A computes $K_A = (a+d_A)^2 T_B$ and the session key as $SK = H_2(ID_A, ID_B, T_A, T_B, K_A)$.
(2) Similarly, B computes $P_A = R_A + H_0(ID_A, R_A) P_{pub}$ and verifies the equation $S_A(P_A + H_1(T_A, R_A)P) = T_A$. If it holds, B computes $K_B = (b+d_B)^2 T_A$ and the session key as $SK = H_2(ID_A, ID_B, T_A, T_B, K_B)$.

- *Correctness of the protocol*: A and B compute the partial session key as $K_A = (a+d_A)^2 T_B = (a+d_A)^2 (b+d_B)^2 P = (b+d_B)^2 T_A = K_B$ and thus, A and B successfully established a common and secure session key SK between them. The key agreement phase of the proposed protocol is given in Fig. 1.

4. Formal analysis of the proposed protocol using BAN logic model

In 1990, Burrows et al. (1990) proposed the BAN logic model, which defines some simple, but sound and powerful tools based on which the cryptographic protocols can be analyzed more rigorously than any informal method. In this section, we analyzed and justified the correctness of our protocol using the BAN logic model. We first described the BAN logic model and then the security analysis of the proposed protocol using BAN logic is shown below.

4.1. Definition of BAN logic model

This section described the basic syntax, semantics and inference rules used in BAN logic model (Burrows et al., 1990; Yang and Li, 2006). In this model, P and Q denote the principals, where P_P and P_Q denote the public keys, and d_P, d_Q denote the corresponding secret keys.

4.1.1. Basic notations and descriptions

We briefly described some basic notations and semantics of the BAN logic model as follows.

(N1) $P| \equiv X$: P believes X, which means that P believes if X is true.
(N2) $P \triangleleft X$: P sees X. That is, someone sends a message containing X to P and P reads and repeats X.
(N3) $P| \sim X$: P once said X. That is, at some time P sent a message including X, which is not known whether the message was sent long ago or during the current run of the protocol, but it is known that P believes X then.
(N4) $P|| \sim X$: P has recently said X. This means that P uttered X in the current run of the protocol.
(N5) $P| \Rightarrow X$: P controls X. That is, P has an authorization over the statement X and should be trusted on it.

(N6) $\#(X)$: The formula X is fresh. That is, X has not been sent in a message at any time before the current run of the protocol.

(N7) $\xrightarrow{P_P} P$: It means that P_P is the public key of P and the corresponding secret key d_P will never be discovered by others except P or an entity trusted by him.

(N8) $\{X\}_K$: This represents the formula X is encrypted under the key K.

(N9) $P \overset{K}{\leftrightarrow} Q$: P and Q may use the symmetric key K for secure communication and it will never be discovered by others except P or Q, or an entity trusted by either of them.

(N10) $\frac{P}{Q}$: It means if P is true then Q is also true.

4.1.2. Inference rules

In the following, we described a set of inference rules of BAN logic model defined in Burrows et al. (1990), Yang and Li (2006).

(P1) *Message-meaning rule*: This rule is related with the interpretation of messages and helps to explain the origin of the messages. If P believes P_Q be the Q's public key and receives a message $\{X\}_{d_Q}$ encrypted under Q's private key d_Q, then P may conclude that Q once said the message X, i.e., $\dfrac{P| \equiv \xrightarrow{P_Q} Q, P \triangleleft \{X\}_{d_Q}}{P| \equiv Q| \sim X}$.

(P2) *Nonce verification rule*: If P believes that X is fresh and that Q has said X during the current state of the protocol, then P believes that Q believes X, that is, $\dfrac{P| \equiv \#(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$.

(P3) *Jurisdiction rule*: If P believes that Q has jurisdiction over the statement X and P believes that Q believes X, then P believes X, i.e., $\dfrac{P| \equiv Q| \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}$.

(P4) *Seeing rule*: If P sees a message (X, Y), then it also sees part of the message (i.e., X and Y), provided that the key is known to him, i.e., $\dfrac{P \triangleleft X, P \triangleleft Y}{P \triangleleft (X, Y)}$.

(P5) *Belief rule*: The principal P can believe a collection of statements if and only if P believes each of the statements individually, i.e., $\dfrac{P| \equiv X, P| \equiv Y}{P| \equiv (X, Y)}$ and $\dfrac{P| \equiv (X, Y)}{P| \equiv X}$.

(P6) *Freshness rule*: If P believes that one part X of a formula is fresh, then it believes that the entire formula (X, Y) must also be fresh, that is, $\dfrac{P| \equiv \#(X)}{P| \equiv \#(X, Y)}$. But (X, Y) being fresh tell us nothing about the freshness of either X or Y.

(P7) *Session key rule*: If P believes the session key SK is fresh and P believes Q believes X, then P believes $P \overset{SK}{\leftrightarrow} Q$, that is, $\dfrac{P| \equiv \#(SK), P| \equiv Q| \equiv X}{P| \equiv P \overset{SK}{\leftrightarrow} Q}$, where X is the main part from which SK is derived.

4.1.3. Synthetic rules

In the BAN logic model, the inference rules and basic postulates help to meet the desired goals of the cryptographic protocols. Buttyan et al. (1998) also derives a set of synthetic rules that can be used to build a cryptographic protocol in a systematic way and to prove the soundness of the protocol. We have listed some of such synthetic rules as given below. The notation $R \mapsto S$ means, the formula S is deduced from the formula R.

$(S1) P \triangleleft X \mapsto P \triangleleft (X, Y)$ $\quad (S3) P| \equiv Q| \sim X \mapsto Q \triangleleft X$

$(S2) P| \equiv Q| \sim X \mapsto P| \equiv Q| \sim (X, Y)$ $\quad (S4) P| \equiv Q|| \sim X \mapsto P| \equiv \#(X)$

4.2. Analysis of the proposed protocol

In this section, we formally proved the correctness and soundness of the proposed protocol based on BAN logic model, i.e., at the end of a session both the users ensure that they establish a fresh session key among them.

4.2.1. Initial assumptions

To analyze the proposed protocol, we first list the following assumptions about the initial state of the protocol:

$(A1) A| \equiv \xrightarrow{P_B} B$ $\quad (A4) B| \equiv \xrightarrow{P_B} B$

$(A2) B| \equiv \xrightarrow{P_A} A$ $\quad (A5) A| \equiv \#(T_A)$

$(A3) A| \equiv \xrightarrow{P_A} A$ $\quad (A6) B| \equiv \#(T_B)$

$(A7) A| \equiv \#(R_A)$ $\quad (A11) A| \equiv B| \Rightarrow (T_B)$

$(A8) B| \equiv \#(R_B)$ $\quad (A12) B| \equiv A| \Rightarrow (T_A)$

$(A9) A| \equiv B| \Rightarrow P_B$ $\quad (A13) A| \equiv B| \Rightarrow R_B$

$(A10) B| \equiv A| \Rightarrow P_A$ $\quad (A14) B| \equiv A| \Rightarrow R_A$

4.2.2. Idealized form

Now we transformed the proposed protocol to an idealized form according to the BAN logic model as given below:

$(I1) A \longrightarrow B : T_A, R_A, \{T_A, R_A\}_{d_A}$ $(I2) B \longrightarrow A : T_B, R_B, \{T_B, R_B\}_{d_B}$

4.2.3. Goals to be achieved

The main concern of our protocol is to build the trust between the users A and B such that they can share a common and fresh secret key in each session. Therefore, we have to reach the following goals in order to validate the security claim of the proposed protocol:

$(G1) A| \equiv A \overset{SK}{\leftrightarrow} A$ $\quad (G3) A| \equiv B| \equiv A \overset{SK}{\leftrightarrow} B$

$(G2) B| \equiv A \overset{SK}{\leftrightarrow} A$ $\quad (G4) B| \equiv A| \equiv A \overset{SK}{\leftrightarrow} B$

4.2.4. Verification of the protocol

In this section, we analyzed the ideal form of the protocol using the BAN logic model. The detailed steps are given as follows:

From (I1) we get the following:

(V1) $A| \equiv (T_A, R_A)$
(V2) $B \triangleleft (T_A, R_A)$
(V3) $B \triangleleft \{T_A, R_A\}_{d_A}$

From (I2) we obtain the following:

(V4) $B| \equiv (T_B, R_B)$
(V5) $A \triangleleft (T_B, R_B)$
(V6) $A \triangleleft \{T_B, R_B\}_{d_B}$

From (V3) and (A2), on applying message-meaning rule (P1), we get

(V7) $B| \equiv A|\Box(T_A, R_A)$

From the initial assumptions (A5), (A7) and through freshness rule (P6), we obtain

(V8) $A| \equiv \#(T_A, R_A)$

From (V7) and (V8), we can say,

(V9) $B| \equiv A||\Box(T_A, R_A)$

From (V9) and using the synthetic rule (S4) we get

(V10) $B| \equiv \#(T_A, R_A)$

From (V7), (V10) and through the nonce verification rule (P2), we get

(V11) $B| \equiv A| \equiv (T_A, R_A)$

On applying the belief rule (P5), we get from (V11)

(V12) $B| \equiv A| \equiv (T_A)$

(V13) $B| \equiv A| \equiv R_A$

On applying the jurisdiction rule (P3), from (V12) and the initial assumption (A12), we get

(V14) $B| \equiv (T_A)$

On applying jurisdiction rule (P3), from (A14) and (V13), we get

(V15) $B| \equiv R_A$

Now, B computes $P_A$and K_B, and finally the session key SK. From $K_B$and (V10), on applying the freshness rule (P6), we get

(V16) $B| \equiv \#(K_B)$

Also from (V16), we get

(V17) $B| \equiv \#(SK)$

From (V11) and (V17), on applying the session key rule (P7), we obtain

(V18) $B| \equiv A \overset{SK}{\leftrightarrow} B$

Due to the symmetry of the protocol, A believes that B is bound to derive the same belief as

(V19) $B| \equiv A| \equiv A \overset{SK}{\leftrightarrow} B$

From (V6) and the initial assumption (A1), on applying the message-meaning rule (P1), we get

(V20) $A| \equiv B|\Box(T_B, R_B)$

From the initial assumptions (A4), (A8) and through freshness rule (P6), we obtain

(V21) $B| \equiv \#(T_B, R_B)$

From (V20) and (V21), we have,

(V22) $A| \equiv B||\Box(T_B, R_B)$

From (V22) and the synthetic rule (S4), we get

(V23) $A| \equiv \#(T_B, R_B)$

From (V20), (V23) and through the nonce verification rule (P2), we get

(V24) $A| \equiv B| \equiv (T_B, R_B)$

From (V24), on applying the belief rule (P5), we get

(V25) $A| \equiv B| \equiv (T_B)$

(V26) $A| \equiv B| \equiv R_B$

From (A11), (V25) and through the jurisdiction rule (P3), we get

(V27) $A| \equiv (T_B)$

From (A13), (V26) and through the jurisdiction rule (P3), we get

(V28) $A| \equiv R_B$

The user A computes P_B and K_A, and the final session key SK. From K_A and (V23) and using the freshness rule (P6), we get

(V29) $A| \equiv \#(K_A)$

From (V29), we get

(V30) $A| \equiv \#(SK)$

From (V24), (V30) and using the session key rule (P7), we obtain

(V31) $A| \equiv A \overset{SK}{\leftrightarrow} B$

Due to the symmetry of the protocol, A believes that B is bound to derive the same belief as

(V32) $A| \equiv B| \equiv A \overset{SK}{\leftrightarrow} B$

Thus, we have reached the desired goals (G1), (G2), (G3) and (G4) of the proposed protocol corresponding to the equations (V17), (V18), (V31) and (V32) as shown above, and it can be concluded that A and B successfully generate a fresh, common and secure session key between them using the protocol presented in this paper.

4.3. Security analysis of the proposed protocol against different attacks

In addition to the formal security analysis through BAN logic model, the proposed protocol also provides other security attributes and resilience against all possible attacks such as known session-specific temporary information attack, key replicating/key off-set attack, known-key attack, key-compromise impersonation attack, perfect forward security, PKG forward security, etc. as discussed in Boyd and Choo (2005), Blake-Wilson et al. (1997), Menezes et al. (1997). Note that the security of the proposed protocol against these attacks depends on the infeasibility of solving the ECDLP and CDHP in the elliptic curve group.

4.3.1. Known session-specific temporary information attack (KSTIA)

The known session-specific temporary information attack states that the secrecy of the generated session key should not be exposed to an outsider even if the ephemeral secrets of a session are known to him/her. As stated, A and B compute the session key SK, whose security entirely depends on the partial session key $K_A (= K_B)$. Now even if the ephemeral session secrets (a, b) are exposed, then an outsider only can generate the session key SK if d_A and d_B are known to him/her. However, the computation of d_A and d_B are not possible from the public keys (P_A, P_B) due to the difficulties of ECDLP. Therefore, the known-session specific temporary information attack is infeasible in our protocol.

4.3.2. Key off-set attack (KOA)/Key replicating attack (KRA)

The proposed protocol can withstand the key off-set attack. In our protocol, the user A initiates the session key agreement phase by sending a message (ID_A, T_A, R_A, S_A) to the user B. Suppose that an adversary E captures the message (ID_A, T_A, R_A, S_A) and modifies it to (ID_A, T_A^*, R_A, S_A), and then forwards the same to B. Let us consider $T_A^* = \sigma T_A$ for an arbitrary constant σ. Note that E can never forge the signature S_A without knowing the private key d_A of A to compensate the change and forge the message. On the other hand, user B, on receiving (ID_A, T_A^*, R_A, S_A), checks the validity of the message with the equation $S_A(P_A + H_1(T_A^*, R_A)P) = T_A^*$ as

$$\begin{aligned} S_A(P_A + H_1(T_A^*, R_A)P) &= (a + d_A)^2 (d_A + H_1(T_A, R_A))^{-1} \\ &\quad (P_A + H_1(T_A^*, R_A)P) \\ &= (a + d_A)^2 (d_A + H_1(T_A, R_A))^{-1} \\ &\quad (d_A + H_1(T_A^*, R_A))P \\ &\quad [\because H_1(T_A, R_A) \neq H_1(T_A^*, R_A)] \end{aligned}$$

Since the verification fails, thus the key agreement session is terminated by B. Therefore, the key off-set attack/key replicating attack is not possible in our proposed protocol.

4.3.3. Key freshness/No key control (NKC)

The property of session key freshness is defined in Menezes et al. (1997), which states that neither communicating entity can predetermine the session key being established subsequently. In 2005, (Phan, 2005) analyzed that Harn et al.'s Diffie-Hellman-DSA key exchange protocol (Harn et al., 2004) does not provide session key freshness. In order to achieve this property, Phan suggested that the generated partial session key K_A should be computed from the ephemeral secrets (a, b) chosen independently by both participants A and B. In our protocol, A and B contributed to generate the session key in the same manner as suggested by Phan (2005) and neither participant can force the other for the session key to be a preselected value or the session key lies within a set containing a small number of elements. Since the session key SK depends on (T_A, T_B), the contributions of A and B, respectively, the partial session key K_A can only be computed by the participants cooperatively and any single entity cannot control the outcome of the session keys or enforce the other. Thus, the property of the session key freshness/no key control is preserved in our protocol.

4.3.4. Known-key attack (K-KA)

Assume that the session key SK of any previous session is compromised to an adversary E, however, in the proposed protocol, any future session key cannot be obtained from an exposed session key. In our proposed protocol, a unique and fresh session key is computed in each session using the private keys d_A and d_B, and the ephemeral secrets (a, b), which differ in every session. Since E, due to the difficulties of ECDLP, cannot derive the ephemeral secrets (a, b) from (T_A, T_B) (also the private keys d_A and d_B from P_A and P_B), and thus, the disclosure of one session key does not allow E to gain any secret knowledge from which any other future session keys can be

generated. Therefore, the proposed protocol is known-key attack protected.

4.3.5. Perfect forward security (PFS) and PKG forward security (PKG-FS)

The protection of this attack means that the disclosure of users' private keys must not allow the compromise of any past session keys i.e., if the private keys of A and B are compromised, the adversary E cannot recover any past session keys. It is known that E can compute the session key SK if and only if $K_A(=K_B)$ is known. Now if the private keys d_A and d_B of A and B are disclosed, however, E cannot obtain K_A because (a,b) are unknown to him/her. The partial session key K_A cannot be calculated by E since (a,b) are unknown due to the infeasibility of deriving them from (T_A,T_B) by solving ECDLP. Also from this discussion, any one can see if the secret key of PKG is disclosed so the secret keys of all participants are compromised, however, the current or past session keys are still secured and valid. Thus, the perfect forward security and PKG forward security are preserved in our protocol.

4.3.6. Key-compromise impersonation attack (K-CI)

Suppose A's secret key d_A is exposed to an adversary E, who then tries to impersonate B to A in order to obtain the current session key. However, E cannot impersonate B, since the signature S_B without B's private key cannot be generated. Therefore, the K-CI attack is protected in the proposed protocol.

4.3.7. Reflection attack (RA) and Unknown key-share attack (UKA)

In the proposed protocol, note that the session key SK is generated not only using $K_A(=K_B)$, but also using the identities of the participants and the messages (T_A,T_B) exchanged in a session. Thus, according to Wang et al. (2009), our protocol provides the resilience against the unknown key-share attack and reflection attack.

5. Comparison of the proposed protocol with contemporary protocols

In this section, we compared the proposed protocol with other existing protocols (Smart, 2002; Shim, 2003; Ryu et al., 2004; Wang et al., 2009; McCullagh and Barreto, 2005; Xie, 2004; Zhu et al., 2007; Cao et al., 2008, 2010; Sui et al., 2005; Lu et al., 2007; Chang and Chang, 2008) in terms of security, computation and communication efficiency.

5.1. Security comparison

In Section 1.1, we provided a literature survey, which shows that out of the most recently published protocols, two of them (Cao et al., 2008, 2010) are the most efficient both in communication and computation costs. However, the paper (Islam and Biswas, 2012) shows that these two protocols are vulnerable to KSTIA and KOA attacks. The KSTIA as described in Blake-Wilson et al. (1997), Zhao and Gu (2012) states that the session key should not be compromised even if the session's ephemeral secrets are exposed (loss of secret information/leakage of ephemeral keys). Blake-Wilson et al. (1997) investigated the KOA attack and pointed out that any authenticated key agreement protocol, which does not contain asymmetry in the session key formation, is vulnerable to this attack. In such an attack, an active adversary can intercept, modify and delete the messages exchanged between the entities (users), and can force them to accept the same session key, which is not actually the one the entities want to agree on. According to the above discussion, it is supposed that protocols in Smart (2002), Chen and Kudla (2002), Ryu et al. (2004), Wang et al. (2009), McCullagh and Barreto (2005), Xie (2004), Cao et al. (2008, 2010) and McCullagh and Barreto, 2005; Zhu et al., 2007; Cao et al., 2008, 2010 are not secure against KOA and KSTIA attacks. A summarization of the security analysis of the different key agreement protocols including ours is given in Table 2, which shows that the proposed protocol is more efficient than others.

Table 2 Security comparison of the proposed protocol with others.

Protocol	Weaknesses against attack(s)
Smart (2002)	PFS
Shim (2003)	MIMA
Ryu et al. (2004)	K-CI, RA
Wang et al. (2009)	KOA,K-CI,
McCullagh and Barreto (2005)	KOA, KSTIA,K-CI
Xie (2004)	K-CI
Zhu et al. (2007)	KSTIA
Cao et al. (2008)	KOA, KSTIA
Cao et al. (2010)	KOA, KSTIA
Sui et al. (2005)	OPGA
Lu et al. (2007)	PGA, OPGA
Chang and Chang (2008)	MA
Proposed	Not found

OPGA: off-line password guessing attack; PGA: Parallel guessing attack; MA: Mutual authentication.

Table 3 Running time (ms) of different operations.

Notation	Descriptions and running time
T_{BP}	Time to execute bilinear pairing, $T_{BP} \approx 20.01$ ms
T_{PX}	Time to execute pairing-based exponentiation, $T_{PX} \approx 6.38$ ms
T_{EM}	Time to execute elliptic curve scalar point multiplication, $T_{EM} \approx 0.83$ ms

5.2. Efficiency comparison

In this section, we provide a comparison between our and other existing protocols in terms of communication round, bandwidth requirement and computation cost. According to the experimental results of Cao et al. (2010), the running times (miliseconds) are given in Table 3, where the hardware platform is a PIV 3 GHZ processor with 512 M bytes memory and the Windows XP operating system. To evaluate the efficiency of our protocol with others against the communication cost, we have followed the concept as discussed in Cao et al. (2010), which states that for achieving the comparable security

Table 4 Comparison of computation and communication efficiency.

Protocol	Communication Cost		Computation cost
	Communication round	Bandwidth required (bits)	
Wang et al. (2009)	2	$512 \times 1 = 512$	$2T_{BP} + 4T_{EM} \approx 43.34$ ms
McCullagh and Barreto (2005)	2	$512 \times 1 = 512$	$2T_{BP} + 2T_{EM} + 2T_{PX} \approx 54.44$ ms
Wang et al. (2008)	2	$512 \times 2 = 1024$	$2T_{BP} + 6T_{EM} \approx 45.00$ ms
Choie et al. (2005)	2	$512 \times 2 = 1024$	$4T_{BP} + 6T_{EM} \approx 85.02$ ms
Choie et al. (2005)	2	$512 \times 1 = 512$	$4T_{BP} + 8T_{EM} \approx 86.68$ ms
Zhu et al. (2007)	3	$160 \times 4 = 640$	$12T_{EM} \approx 10.06$ ms
Cao et al. (2008)	3	$160 \times 2 = 320$	$12T_{EM} \approx 9.96$ ms
Cao et al. (2010)	2	$160 \times 2 = 320$	$10T_{EM} \approx 8.30$ ms
Hölbl et al. (2012)	2	$512 \times 3 + 160 = 1696$	$6T_{BP} + 10T_{EM} + 2T_{PX} \approx 141.12$ ms
Proposed	2	$160 \times 3 = 480$	$8T_{EM} \approx 6.64$ ms

with the 1024-bit RSA key, the bilinear pairing-based protocols execute the Tate pairing operation on a super singular elliptic curve $E(F_p)$: $y^2 = x^3 + x$ (Miller et al., 1985; Koblitz, 1987) with embedding degree 2 and the large prime order p, which is a 160-bit Solinas prime of the form $p = 2^{159} + 2^{17} + 1$ and q is at least 512-bit prime number that satisfies the condition $q + 1 = 12pr$ (Solinas et al., 2011). In order to meet the same level of security, pairing-free elliptic curve-based protocols execute different operations on the Koblitz curve defined as $y^2 = x^3 + ax^2 + b$ on F_l, $l = 2^{163}$ with $a = 1$ and b is a 163-bit random prime number (Koblitz, 1987). Thus, the security provided by a 512-bit random number in a pairing-based protocol is equivalent to a 160-bit random number in a pairing-free protocol. Here, we assume that the output of the hash function $H()$ is 160 bits. In Table 4, we given the comparative results of our protocol and other existing protocols in terms of communication round, bandwidth requirement and computation cost.

It is found that although the proposed protocol and Cao et al.'s protocol (Cao et al., 2010) have the same communication round (minimum number of rounds), however, our protocol requires slightly more communication bandwidth. Note that the proposed protocol requires lesser computation costs than others, and the protection of all kinds of attacks is possible in our protocol with the sacrifice of slightly increased bandwidth requirement. Therefore, it can be claimed that our protocol is more secure than others and thus, suitable for different real life applications including wireless communications.

6. Conclusion

In this paper, we proposed an improved pairing-free ID-2PAKA protocol using elliptic curve cryptography and identity-based cryptosystem. The proposed protocol is secure than the protocols proposed earlier. The formal analysis for the validity of the proposed protocol based on the BAN logic model is given. The security of the proposed protocol is based on the difficulties of solving the ECDLP and the CDHP, and thus, the resilience against all possible attacks and their detailed analysis is given. The efficiency analysis in terms of computation cost and communication cost is done, which shows that our protocol increases the computation and communication costs with respect to others.

Acknowledgments

SK Hafizul Islam is supported by the Outstanding Potential for Excellence in Research and Academics (OPERA) award, Birla Institute of Technology and Science (BITS), Pilani Campus, Rajasthan, India. The authors are grateful to the Editor-In-Chief and anonymous reviewers for their insightful comments and valuable suggestions, which helped to improve the paper.

References

Blake-Wilson, S., Johnson, D., Menezes, A., 1997. Key agreement protocols and their security analysis. In: Proceedings of the 6th IMA International Conference on Cryptography and Coding, LNCS 1335, Springer-Verlag, pp. 30–45.

Boneh, D., Franklin, M.K., 2001. Identity-based encryption from the Weil pairing. In: Proceedings of the Cryptology (Crypto'01), LNCS 2139, Springer-Verlag, pp. 213–229.

Boyd, C., Choo, K.K.R., 2005. Security of two-party identity-based key agreement. In: Proceedings of the Process in Cryptology, LNCS 3715, pp. 229–243.

Burrows, M., Abadi, M., Needham, R., 1990. A logic of authentication. ACM Trans. Comput. Syst. 8 (1), 18–36.

Buttyan, L., Staamann, S., Wilhelm, U., 1998. A simple logic for authentication protocol design, In: Proceedings of the 11th IEEE workshop on Computer Security Foundations (CSFW '98), pp. 153–162.

Cao, X., Kou, W., Yu, Y., Sun, R., 2008. Identity-based authentication key agreement protocols without bilinear pairings. IEICE Trans. Fund. E91–A (12), 3833–3836.

Cao, X., Kou, W., Du, X., 2010. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. Inf. Sci. 180, 2895–2903.

Chang, C.-C., Chang, S.-C., 2008. An improved authentication key agreement protocol based on elliptic curve for wireless mobile networks. In: Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1375–1378.

Chen, L., Kudla, C., 2002. Identity based key agreement protocols from pairings. In: Proceedings of the 16th IEEE Computer Security Foundations Workshop, pp. 219–233.

Choie, Y.J., Jeong, E., Lee, E., 2005. Efficient identity-based authenticated key agreement protocol from pairings. Appl. Math. Comput. 162, 179–188.

Debiao, H., Jianhua, C., Jin, H., 2011. Identity-based digital signature scheme without Bilinear Pairings. *Cryptology ePrint Archive, Report 2011/079, 2011*. http://eprint.iacr.org/2011/079/.

Guo, H., Li, Z., Mu, Y., Zhang, X., 2008. Cryptanalysis of simple three-party key exchange protocol. Comput. Sec. 27, 16–21.

Guo, H., Xu, C., Mu, Y., Li, Z., 2012. A provably secure authenticated key agreement protocol for wireless communications. Comput. Electr. Eng. http://dx.doi.org/10.1016/j.compeleceng.2011.10.015.

Hankerson, S., Menezes, A., Vanstone, S., 2004. Guide to Elliptic Curve Cryptography. Springer-Verlag, New York, USA.

Harn, L., Mehta, M., Hsin, W.-J., 2004. Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA). IEEE Commun. Lett. 8 (3), 198–200.

Hölbl, M., Welzer, T., Brumen, B., 2012. An improved two-party identity-based authenticated key agreement protocol using pairings. J. Comput. Syst. Sci. 78, 142–150.

Islam, S.H., Biswas, G.P., 2011. A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. J. Syst. Softw. 84 (11), 1892–1898.

Islam, S.H., Biswas, G.P., 2012. A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile network. Ann. Telecommun. http://dx.doi.org/10.1007/s12243-012-0296-9.

Islam, S.H., Biswas, G.P., 2012. An improved pairing-free identity-based authenticated key agreement protocol based on ECC. In: Proceedings of the International Conference on Communication Technology and System Design (ICCTSD'11), Procedia Engineering 30, pp. 499–507.

Kim, J., Kim, K., 2011. A scalable and robust hierarchical key establishment for mission-critical applications over sensor networks. Telecommun. Syst. http://dx.doi.org/10.1007/s11235-011-9650-x.

Koblitz, N., 1987. Elliptic curve cryptosystem. J. Math. Comput. 48 (177), 203–209.

Lee, C.-C., Liao, I.-E., Hwang, M.-S., 2011. An efficient authentication protocol for mobile communications. Telecommun. Syst. 46, 31–41.

Li, S., Yuan, Q., Li, J., 2005. Towards security two-part authenticated key agreement protocols. *Cryptology ePrint Archive, Report, 2005/300, 2005*. http://eprint.iacr.org/2005/300.

Liaw, S.-H., Su, P.-C., Chang, H. K.-C., Lu, E.-H., & Pon, S.-F., 2005. Secured key exchange protocol in wireless mobile ad hoc networks. In: Proceedings of the International Carnahan Conference on Security Technology (CCST'05), pp. 171–173.

Lo, J.-W., Lee, C.-C., Hwang, M.-S., 2010. A secure and efficient ECC-based AKA protocol for wireless mobile communications. Int. J. Innov. Comput. Inform. Control 6 (11), 5249–5258.

Lu, R., Cao, Z., Zhu, H., 2007. An enhanced authenticated key agreement protocol for wireless mobile communication. Comput. Stand. Interf. 29, 647–652.

McCullagh, N., Barreto, P.S.L.M., 2005. A new two-party identity-based authenticated key agreement. In: Proceedings of the Topics in Cryptology-CT-RSA, pp. 262–274.

Menezes, A., Oorschot, P.V., Vanstone, S., 1997. Handbook of Applied Cryptography. CRC Press, Boca Raton, FL.

Miller, V.S., 1985. Use of elliptic curves in cryptography. In: Proceeding of the Advances in Cryptology (Crypto'85), LNCS 218, Springer-Verlag, pp. 417–426.

Park, J., Jin, Q., 2010. Effective session key distribution for secure fast handover in mobile networks. Telecommun. Syst. 44, 97–107.

Phan, R.C.W., 2005. Fixing the integrated Diffie-Hellman-DSA key exchange protocol. IEEE Commun. Lett. 9 (6), 570–572.

Pu, Q. (2010). Cryptanalysis of Lu et al'.s password-based authenticated key agreement protocol. In: Proceedings of the 2nd International Conference on Multimedia and Information Technology, pp. 215–218.

Ryu, E., Yoon, E., Yoo, K., 2004. An efficient ID-based authenticated key agreement protocol from pairings. In: Proceedings of the Networking'04, LNCS 3042, pp. 1458–1463.

Sadhukhan, P., Das, P.K., Saha, S., 2011. Hybrid mobility management schemes integrating mobile IP and SIP for seamless invocation of services in All-IP network. Telecommun. Syst. http://dx.doi.org/10.1007/s11235-011-9483-7.

Shamir, A., 1981. Identity-based cryptosystems and signature protocols. In: Proceedings of the Advances in Cryptology (Crypto'84), LNCS, Springer-Verlag, pp. 47–53.

Shim, K., 2003. Efficient ID-based authenticated key agreement protocol based on Weil pairing. Electron. Lett. 39 (8), 653–654.

Smart, N.P., 2002. An identity based authenticated key agreement protocol based on the Weil pairing. Electron. Lett. 38, 630–632.

Solinas, J.A. Generalized Mersenne Prime: Encyclopedia of Cryptography and Security, second ed., Springer, US, 509–510, 2011.

Song, S., Abid, M., Moustafa, H., Afifi, H., 2011. Performance evaluation of an authentication solution for IMS services access. Telecommun. Syst. http://dx.doi.org/10.1007/s11235-011 9543-z.

Sui, A., Hui, L., Yiu, S., Chow, K., Tsang, W., Chong, C., Pun, K., Chan, H., 2005. An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication. In: Proceedings of the IEEE Wireless and Communications and Networking Conference (WCNC'05), pp. 2088–2093.

Sun, H., Hsieh, B., 2003. Security analysis of Shim's authenticated key agreement protocols from pairings. *Cryptology ePrint Archive2003/113*. http://eprint.iacr.org/2003/113/.

Wang, S., Cao, Z., Cao, F., 2008. Efficient identity-based authenticated key agreement protocol with PKG forward secrecy. Int. J. Netw. Sec. 7 (2), 181–186.

Wang, S., Cao, Z., Choo, K.K.R., Wang, L., 2009. A proposed identity-based key agreement protocol and its security proof. Inf. Sci. 179, 307–318.

Wang, N.-W., Chao, H.-C., Chen, I.-Y., Huang, Y.-M., 2010. A novel user's authentication scheme for pervasive on-line media services. Telecommun. Syst. 44, 181–190.

Xie, G., 2004. Cryptanalysis of Noel McCullagh and Paulo S.L.M. Barreto's two-party identity-based key agreement. *Cryptology ePrint Archive, Report 2004 308, 2004*. http://eprint.iacr.org/2004/308/.

Yang, S., Li, X., 2006. A limitation of BAN logic analysis on a man-in-the-middle attack. J. Inform. Comput. Sci. 1 (3), 131–138.

Youn, T.-Y., Kang, E.S., Lee, C., 2011. Efficient three-party key exchange protocols with round efficiency. Telecommun. Syst. http://dx.doi.org/10.1007/s11235-011-9649-3.

Zhao, J., Gu, D., 2012. Provably secure three-party password-based authenticated key exchange protocol. Inf. Sci. 184, 310–323.

Zhu, R.W., Yang, G., Wong, D.S., 2007. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices. Theoret. Comput. Sci. 378, 198–207.

Znaidi, W., Minier, M., 2011. Key establishment and management for WSNs. Telecommun. Syst. http://dx.doi.org/10.1007/s11235-010-9391-2.