A Secure Authenticated Key Agreement Protocol for Application at Digital Certificat

Javad Saadatmandan and Amirhossein Rahimi
(Corresponding author: Javad Saadatmandan)

Department of Mathematics, Qom Branch, Islamic Azad University
Qom, Iran
jsaadatmandan2014@gmail.com

(Received Mar. 25, 2018; Revised and Accepted Sept. 2, 2019; First Online Feb. 9, 2020)

Abstract

To establish secure channel for network communication in open and distributed environments, authenticated key agreement protocol is an important primitive for establishing session key. So far, a great deals of identity-based protocols have been proposed to provide secure mutual authentication and common session key establishment in two-party setting for secure communications in the open environment. Majority of the existing authenticated key agreement protocols only provide partial forward secrecy. Therefore, such protocols are unsuitable for real-world applications that require a stronger sense of perfect forward secrecy. In this paper, we present a secure two-party identity-based authenticated key agreement protocol with achieves most of the required security attributes. We also show that the scheme achieves the security attributes include known-key secrecy, perfect forward secrecy, PKG forward secrecy, key-compromise impersonation resilience, unknown key-share resilience, no key revelation and known session-specific temporary key information secrecy and also proposed algorithm achieves the shorter run time, lower computation cost, lower communication cost, and a more effective storage method. In addition, the adversary can not compromise the agreed session key.

Keywords: Identity-Based Cryptography; Key Agreement; Perfect Forward Secrecy; PKG Forward Secrecy

1 Introduction

Key agreement protocol is used to provide secure communications in open and distributed environments [4]. Key establishment is a process whereby two (or more) entities can establish a shared secret key (session key) after message interactions. There are two different approaches to key establishment between two entities. In one scenario, one entity generates a session key and securely transmits it to the other entity, this is known as enveloping or key transport [11, 15].

In order to provide authentication for the key agreement protocol, public key certificate is often used in the traditional PKI setting. This require the parties to obtain and verify certificates whenever they want to use a specific public key and the management of public key certificates remains a technically challenging problem. Adi Shamir introduced the identity-based cryptography in 1984 [16]. His idea was to allow parties to use their identities as public keys. With the help of Private Key Generator (PKG), the users attain their private keys and perform cryptographic tasks subsequently. Authentication without the help of public key certificate is the major advantage of identity-based cryptography. Therefore,identity-based key agreement protocols without pairing may be more appealing in practice.

Two-party authenticated key agreement (AK) protocol not only allows parties to compute a session key known only to them but also ensures the authenticity of the parties [12,15]. This secret session key can be used to provide privacy and data integrity during subsequent sessions. A key agreement protocol is said to provide implicit key authentication (of Bob to Alice) if Alice is assured that no other entity besides Bob can possibly ascertain the value of the secret key. A key agreement protocol that provides mutual implicit key authentication is called an authenticated key agreement protocol (or AK protocol) [9]. A key agreement protocol provides key confirmation (of Bob to Alice) if Alice is assured that Bob possesses the secret key. A protocol that provides mutual key authentication as well as mutual key confirmation is called an authenticated key agreement with key confirmation protocol (or an AKC protocol).

In this study, an effective and secure authenticated key agreement (AK) protocol is proposed based on a secure one-way hash function, discrete logarithm problem. By comparing the proposed algorithm with other similar algorithms, we found out that the proposed algorithm had a shorter run time, a lower computation and communication cost, and a more effective storage method. We also investigated the fundamental characteristics of hash functions by arguing that, as these functions cannot be executed computationally via inverse operators, their application in the proposed algorithm would provide further protection against known cyber attacks.

It is desirable for any authenticated key agreement protocol to possess the following security attributes:

Known-key secrecy. The overture of one secret session key should not compromise other session keys. Therefore key agreement can prevent to compromise session keys and the insider, replay, parallel session, reflection, and man in the middle attacks.

Forward secrecy. If long-term private keys of one or more of the entities are compromised, the secrecy of previously established session keys should not be affected. We say that a system has partial forward secrecy if the compromise of one (or more but not all) of the entities' long-term keys can be corrupted without compromising previously established session keys, and perfect forward secrecy means if the long-term keys of all the entities involved may be corrupted without compromising any session key previously established by these entities. In order to resistance against comprehensive research attack for recovery of secret random number the better way is that the length of the random number should be greater than secret session key. Therefore, random numbers are required for safekeeping confidential information(secret session key). Remember that Leaking the server's secret key can lead to the risk of the session keys being discovered.

PKG Forward Secrecy. The PKG's master key may be corrupted without compromising the security of session keys previously established by any users. It certainly implies the perfect forward secrecy.

Key-compromise impersonation resilience. For an entity called Alice, the compromise of an entity Alice's long-term private key will allow an adversary to impersonate Alice, but it should not enable the adversary to impersonate other entities to Alice.

Unknown key-share resilience. An entity Alice should not be able to be coerced into sharing a key with any entity Eve when in fact entity Alice thinks that he is sharing the key with another entity Bob.

Known session-specific temporary information secrecy [13]. Some random private information is used as an input of the session key generation function. The revelation of this private temporary information should not compromise the secrecy of (other) generated session key. Known session-specific temporary information secrecy was first explored and discussed by Canetti-Krawczyk in [1]. Generally, this important security attribute requires that if the ephemeral secrets of a session are accidentally leaked to the adversary, the secrecy of the specific session key should not be affected. This revelation is reasonably not partial as it may happen in some practical scenarios. In 2009 and 2010, Cao etc. [2, 3] proposed two pairing-free identity-based authenticated key agreement schemes with two or three passes (one round). They all achieved the basic security attributes without pairing operation. However, we find that their protocols do not offer an important security feature, namely known session specific temporary information secrecy, which considers the impact of ephemeral secrets exposure in affecting the secrecy of the session key.

No key control. Neither entity should be able to force the session key to be a preselected value. Key escrow [14] is desirable under certain circumstances especially in certain closed groups applications. For example,escrow is essential in situations where confidentiality as well as survey trail are legal requirements, such as secure communications in the health care profession. So far, some identity-based authenticated key agreement protocols in the escrow mode (e.g. [5, 14, 18, 20, 21]) were proposed. But most of them did not provide perfect forward secrecy attribute. Although Shim [17] proposed a protocol To be claimed to provide such a property, it was later found to be vulnerable to the manin-the-middle attack [19]. In 2006, Gentry proposed an identity-based encryption system [7] that is fully secure in the standard model and has several advantages over previous such systems, Its complexity assumption is called the truncated **q-ABDHE**. Based on the work of Gentry, we present a new two-party identity-based authentication key agreement protocol that can be used in the escrow mode, whilst it achieves the perfect forward secrecy attribute.

The remainder of this paper is organized as follows. Section 2 gives the necessary technical backgrounds and reviews of the identity-based encryption scheme of Gentry and the scheme of Cao *et al.*. In Section 3, we put forward our new proposed scheme. In Section 4, we give the security analysis and efficiency of the proposed protocols, as well as comparisons over comparably protocols. In this paper, we discuss this problem in detail and give an improved one round scheme with efficient computational performance. Finally, we draw some conclusions.

2 Technical Backgrounds

2.1 Bilinear Maps

Let G_1 and G_2 are two (multiplicative) cyclic groups of prime order p, g is a generator of G_1, assume that the discrete logarithm problem (DLP) is hard in both G_1 and G_2. An admissible pairing e is a bilinear map $e : G_1 \times G_1 \longrightarrow G_2$, which satisfies the following three properties [11]:

Table 1: Notations

Symbol	Definition	Symbol	Definition
ID	User ID (User Identiiy)	Not +	Operator XOR
G	Cyclic Additive Group	F_p	Prime Finite Field
G_1 , G_2	Multiplicative Cyclic Group	$H(0)$	Secure Scrambling Function
PKG	Private Key Generator	Z_p^*	Multiplication Group p
AK	Authenticated Key	$\|$	Concatenation Operation
SK	Session key	X (modp)	Remainder of X:p
P_{pub}	Public Key	r_{ID}	Random
e	Bilinear Map	ECC	Elliptic Curve Cryptography
DLP	Discrete Logarithm Problem	CDH	Computional Dffe-Hellman Assumption

- Bilinear: for all $u, v \in G_1$ and $a, b \in Z_p^*$, we have

$$e\left(u^a, v^a\right) = e\left(u, v\right)^{ab};$$

- Non-degenerate: $e\left(g, g\right) \neq 1$;
- Computable: If u, $v \in G_1$, one can compute $e\left(u, v\right) \in G_2$ in polynomial time efficiently.

2.2 Elliptic Curve Groups

$y^2 = \big(x^3 + ax + b\big) \bmod P$ with, $a, b \in Z_P$ and $8a^3 + 81b^2 \bmod p \neq 0$. The points on E/F_p together with an extra point 0 form a group

$$G = \{(x, y) : x, y \in F_p, E(x, y) = 0\} \,\mathrm{U, o}.$$

G is a cyclic additive group under the point addition "+" defined as follows: Let $p, q \in G, l$ to be the line containing p and q (tangent line to E/F_p if $p = q$), and R, the third point intersection of l with E/F_p at R, o and $p + q$ Scalar multiplication over E/F_p by an integer is defined by repeating addition, i.e. $kp = p + p + \cdots + p(k)$.

3 The New Proposed Scheme

In this section, we propose an efficient perfect forward secure one-round identity based authenticated key agreement protocol without pairing, which achieves almost all the known security attributes, especially the known session-specific temporary information secrecy. At the same time, it is more computational efficient than the other comparable schemes.The security of the protocol can be reduced to the CDH assumption in the random oracle model. The protocol consists of three phases, *i.e.* **Setup, Key Generation** and **Key Agreement**. These three phases are almost as same as that of Cao's schemes [2] with slight modification, and the generation of the session key is different. we would like an escrowable identity-based key agreement protocol in which the user's session key could be recovered by the PKG whilst the others couldn't recover the user's past session keys even the long term key of user was compromised. The protocol involves three entities: two users called Alice and Bob who wish to establish a shared secret session key, and a PKG that is responsible for the creation and distribution of users' private keys using its master key. The protocol consists of four phases, *i.e.* **Setup, Key Generation** and **Key Agreement** and **Correctness Verification**. In order to keep the integrity of description of the protocol, We give the brief description as below:

Setup: To provide a private key generation service, the private key generator (PKG) first generates the system parameters and its public/private key pairs as follows. Given a security system parameter k, the private key generator (PKG) chooses the tuple $\{E/F_p, G, p\}$ as defined in Section 2, choose the master private key $x \in Z_p^*$, calculates the public key of PKG as $P_{pub} = kp^x$. And then choose two groups of prime order p, three secure cryptographic hash functions and one the bilinear map, *i.e.* G, G_t: groups of prime order p; $e : G \times G \longrightarrow G_t$: The bilinear map:

$$H_1 : \{0,1\}^* \times G \longrightarrow Z_p^*$$
$$H_2 : \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \longrightarrow \{0,1\}^k$$
$$H_3 : \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \times G \longrightarrow \{0,1\}^k$$

Let $g, p, t \in G$, $t = g^x \bmod p$, $g_T = e(g, t) \in G_t$. The public key of the PKG Then the PKG publishes the system public parameters as $< E/F_p, G, P_{pub}, t, g_T, H_1, H_2, H_3 >$ and the master private key of the PKG is x.

Key Generation: To generate a private key for the identity Z_p^*, the PKG generates a long-term private key for user identity as bellow. For a user whose identity $r_{ID} \in Z_P^*, r_{ID} \neq x$, the PKG generates a random $r_{ID} \in Z_P^*$, it always assigns identical r_{ID} for a given identity ID and computes $R_{ID} = (kp^{-r_{ID}})^{\frac{1}{(x - ID)}}, h_{ID} = H_1(ID\|R_{ID})$ and outputs the private key as $d_{ID} =< R_{ID}, s_{ID} >$, where $s_{ID} = r_{ID} + h_{ID}x$. The long-term private key of user with identity ID is transmitted to him via a secure out-of-bound channel. The user with identity ID can verify his long-term private key by checking the equation $s_{ID}P = R_{ID} + H_1(ID \parallel R_{ID})P_{pub}$. The long-term private key is valid if the equation holds and vice versa. Suppose there are two entities called Alice (act as the initiator) and Bob (act as the responder) who want to establish the session key.

Key Agreement:

Alice and Bob are two entities who want to establish a shared session key with implicit key authentication by running the following protocol. We use ID_A and ID_B to demonstrate the identification strings of Alice and Bob (It could be E-mail address or any other strings). The protocol is a 2-pass procedure, the details are as follows.

Scheme 1.

1) $A \longrightarrow B : \{ID_A, R_A\}$. B chooses $b \in Z_p^*$ and computes the message

$$T_B = g_B^{b(R_A + H_1(ID_A \| R_A)P_{pub})} \bmod p.$$

2) $B \longrightarrow A : \{ID_B, R_B, T_B\}$. A chooses $a \in Z_p^*$ and computes the message

$$T_A = g_A^{b(R_B + H_1(ID_B \| R_B)P_{pub})} \bmod p.$$

3) $A \longrightarrow B : \{T_B\}$. B computes

$$K_{BA} = (b+1)\, s_B^{-1} T_A + H_1\left((ID_A \| R_A)\, p_{pub}\right) + bp$$

and

$$SK_{BA} = H_2\left(ID_A \| ID_B \| T_A \| T_B \| K_{BA}\right).$$

Finally A computes

$$K_{AB} = (a+1)\, s_A^{-1} T_B + H_1\left((ID_B \| R_B)\, p_{pub}\right) + ap$$

and

$$SK_{BA} = H_2\left(ID_A \| ID_B \| T_A \| T_B \| K_{BA}\right).$$

Correctness Verification:

At the end of the protocol execution, Alice and Bob will agree on the same session key. We can easily verify that $sk = SK_{BA} = SK_{AB}$ From the form of and SK_{BA} and SK_{AB}, we can know that if the adversary acquired the session-specific ephemeral secrets a and b, he can not learns the session key SK_{BA} or SK_{AB}, because he can not compute $H_1((ID_A \| R_A)p_{pub})$, T_A, T_B and too s_A^{-1}, s_B^{-1}. Because hash function inverse is computationally infeasible without knowing server 's secret key. So this scheme does to gain the additional security attribute - Known session-specific temporary information secrecy. It is easy to validate that

$$\begin{aligned}
K_{AB} &= (a+1)\, s_A^{-1} T_B + H_1\left((ID_A \| R_A)\, p_{pub}\right) + ap \\
&= as_A^{-1} T_B + s_A^{-1} T_B + H_1\left((ID_A \| R_A)\, p_{pub}\right) + ap \\
&= abp + ap + bp + s_B p \\
&= bap + bp + ap + s_A p \\
&= bs_B^{-1} T_A + s_B^{-1} T_A + H_1\left((ID_A \| R_A)\, p_{pub}\right) + bp \\
&= (b+1)\, s_B^{-1} T_A + H_1\left((ID_A \| R_A)\, p_{pub}\right) + bp \\
&= K_{AB}.
\end{aligned}$$

So we get the same agreed session key with $sk = SK_{BA} = SK_{AB}$.

Scheme 2.

1) $A \longrightarrow B : \{ID_A, R_A, T_A\}$.
The initiator A chooses a random ephemeral key $a \in Z_p^*$ and compute the message $T_A = ap$;

2) $B \longrightarrow A : \{ID_B, R_B, T_B\}$
On receiving the message from A, The responder B chooses a random ephemeral key and compute the message $T_B = bp$; Finally, A computes

$$\begin{aligned}
K_{AB} &= (T_B + R_B + H_1((ID_B \| R_B)P_{pub}) \cdot \\
&\quad (a + s_A); \\
SK_{AB} &= H_3(ID_A, ID_B, T_A, T_B, K_{AB}).
\end{aligned}$$

B computes

$$\begin{aligned}
K_{AB} &= (T_A + R_A + H_1((ID_A \| R_A)P_{pub}) \cdot \\
&\quad (b + s_B); \\
SK_{BA} &= H_2(ID_A, ID_B, T_A, T_B, K_{BA});
\end{aligned}$$

It is easy to validate that

$$\begin{aligned}
K_{AB} &= (T_B + R_B + H_1((ID_B \| R_B)P_{pub}) \cdot \\
&\quad (a + s_A); \\
&= (bP + s_B P)(a + s_A) \\
&= (aP + s_A P)(b + s_B) \\
&= (T_B + R_B + H_1((ID_B \| R_B)P_{pub}) \cdot \\
&\quad (b + s_B) \\
&= K_{BA} \\
&= (a + s_A)(b + s_B)P \\
&= abP + as_B P + bs_A P + s_A s_B P.
\end{aligned}$$

We can verify that $sk = SK_{BA} = SK_{AB}$.

4 Analysis of Security and Efficiency

In this section, we give the general analysis of security and efficiency, as well as comparisons over comparable protocols.

A. Security Analysis.

We informally declare that our new proposed scheme has several desirable security attributes, such as known-key secrecy, PKG forward secrecy, key-compromise impersonation resilience, unknown key-share resilience, and no key control. Especially, this scheme achieves the perfect forward secrecy attribute.

1) Known-key secrecy.
   If one session key is compromised, this does not mean that any other session keys are compromised. The fact is that each run of the protocol computes a different session key which depends on the ephemeral private keys x and y. While x and y were selected randomly by Alice and Bob independently.

2) Key-compromise impersonation resilience.
   Suppose an adversary called Eve who knows Alice's long term private key wishes to masquerade as Bob to Alice. Although Eve could declare with Bob's identity and send T_B to Alice, but without knowing the private key of Bob, he couldn't use K_{AB} to compute the identical session key as same as that of Alice.

3) Unknown key-share resilience.
   In order to attack this protocol, the adversary is required to learn the private key of some entity. In fact, Chen and Kudla [5] has pointed out that the unknown key-share resilience attribute is implied by the implicit key authentication.

4) No key control.
   In this protocol, x and y are selected by Alice and Bob randomly, neither entity is able to force the session key to be a preselected value. If the adversary Eve modified the exchanged message with such purpose, Alice and Bob can hardly compute the same session key.

5) Key agreement secrecy.
   The overture of one secret session key should not compromise other session keys. Therefore key agreement can prevent to compromise session keys and the insider, replay, parallel session, reflection, server spoofing, and man in the middle attacks. In order to resistance against comprehensive research attack for recovery secret random number is better the length of the random number to be greater than secret session key.Therefore, random numbers and session keys are required for safekeeping confidential information(secret session key).Remember that Leaking the server's secret key can lead to the risk of the session keys being discovered.

6) Perfect forward secrecy.
   If the long term keys of two parties involved were compromised, one (except the PKG) could compute K_{AB_1}, K_{BA_1} and $<as_BP$, bs_AP, $s_As_BP, T_A, T_B, s_A^{-1}, s_B^{-1}, H_1\left(\left(ID_B \| R_B\right) P_{pub}\right) >$ but he couldn't compute K_{AB_2} and K_{BA_2} without knowing same agreed session key with $SK_{BA} = SK_{AB}$.

   In order to compute K_{AB_1}, K_{BA_1}, K_{AB_2} and K_{BA_2} at two proposed schemes , one should solve the Computational Diffie-Hellman hard problem and inverse one-way hash function.

7) PKG forward secrecy.
   If the adversary acquired the system master key of PKG, it means that the adversary can also acquire the private key of both Alice and Bob. It still couldn't compute . In order to compute , one should solve the Computational Diffie-Hellman problem and other inverse one-way hash function.

8) Known session-specific temporary information secrecy.
   If the adversary knew the ephemeral session secrets a and b but not the long-term key of both, then he could only compute $< abP$, as_BP, $bs_AP, R_{ID} >$ but not s_As_BP, s_{ID}.

   In order to compute s_As_BP, one need to acquire at least one of the long term private key of Alice and Bob. It is still a Computational Diffie- Hellman hard problem. In this scheme, the computation of K_{AB} or K_{BA} needs only two scalar addition and two scalar multiplication operations. If we consider the preprocessing of computation of $R_{ID} + H_1\left(\left(ID_{ID} \| R_{ID}\right) P_{pub}\right)$, then the computation cost is only one scalar addition and one scalar multiplication. It is more efficient than that of Cao' s scheme.

9) Resistance to the Modification Attack.
   In the proposed protocol, each authentication message is supported via a new secret randomized number and accompanied by a one-way hash function. Without this randomized number, the attacker is unable to calculate the correct hash function value for authenticating the ID message. For this reason, it is very difficult to generate a manipulated message from n valid message.

10) Resistance to Disclosure Server's Secret Key Attack.

    Proof. Even if the server's secret key x is disclosed, the attacker would not be able to retrieve ID_{ID} and h_{ID} from $R_{ID} + H_1\left(\left(ID_{ID} \| R_{ID}\right) P_{pub}\right)$. Since, due to using only one H(0) function method, the server can easily change/modify the secret key x and return it to the smart card. Remember that Leaking the server's secret key can lead to the risk of the session keys being discovered. □

11) Resistance to the Server spoofing Attack.

Proof. In this type of attack, a attacker cannot masquerade as a legal server since he cannot calculate $s_A s_B P, s_{ID}$ and R_{ID} without first identifying ID_{ID}, r_{ID} and x.

Therefore, the server would not be able to compute $sk = SK_{BA} = SK_{AB}$ without identifying ID_{ID}. In addition, the session key is different for the same user at different sign-in sessions. As a result, the proposed scheme is secured against the server deception attack. □

12) Resistance to the Parallel Session Attack.

Proof. Assuming that the attackers can, through replaying the sign-in request message $\{ID_A, R_A\}$, $\{ID_B, R_B, T_B\}$ turn themselves into an authorized user (U_i) within the valid time frame. However, in such a case, they would not be able to calculate $sk = SK_{BA} = SK_{AB}$ in the next step since the confirmation message does not contain all the data required for establishing the next steps. Because, the security of the proposed scheme authentication message against the parallel attack would depend on the complexity of the logarithmic calculations over $GF(p)$, one-way hash function, Elliptic Curve Groups and the Diffie–Hellman key agreement protocol. □

13) Resistance to the Insider Attack.

Proof. If an immune insider server obtains the confidential information $< abP, as_B P, bs_A P, R_{ID} >$, he would not be able to extract similar sensitive information $s_A s_B P, s_{ID}$ and $R_{ID} + H_1((ID_{ID} \| R_{ID}) P_{pub})$. Because it is computationally infeasible to invert the one-way hash function $h(0)$. In addition, solving a discrete logarithm problem has been a difficult task. The session key agreement also acts against the insider attack procedures. □

14) Resistance to the Replay Attack (Re-execution Attack).

Proof. We can assume the attackers have managed to impersonate the sign-in request message to replay the same sign-in message $\{ID_A, R_A\}$, $\{ID_B, R_B, T_B\}$ to the server. However, it would not be easy for the server to discover the replay attack through examining the protocol combines with the random numbers and timestamp. In this case, if the attacker re-executes an old message on the part of the server, then the server can easily discover the re-execution attack by comparing sign-in message with the current random number and timestamp. Therefore the proposed scheme is protected from the replay attack. □

B. Comparison with Existing Protocols.

One example of an identity-based authenticated key agreement protocol in the escrow mode is the protocol proposed by Chen and Kudla [5]. A drawback with this protocol (and also of Smart's identity-based authenticated key agreement protocol [18]) is that it does not provide perfect forward secrecy attribute. Although Shim [17] proposed a protocol that is claimed to provide such an attribute, it was later found to be vulnerable to the man-in-the-middle attack [19]. In 2005, Wang [21] proposed an identity-based authenticated key agreement protocol which achieves perfect forward secrecy in the escrow mode, it needs to do 3 exponentiation in G, one multiplication in G, and one pairing. Our protocol needs to do one exponentiation in G, 4 exponentiation in G_T, and one pairing. The computational efficiency of two schemes is almost the same. It is more efficient than that of Cao's scheme, because it can prevent to compromise session keys and the insider, replay, parallel session, reflection, server spoofing, and man in the middle attacks.

5 Conclusions

Perfect session-specific temporary information secrecy is an important security attribute for authenticated key agreement protocols (in both escrow and escrowless modes). We presented an identity-based authenticated key agreement protocol that is secure in the escrow mode. We demonstrated that our proposed protocol provides almost all of the known security attributes, especially the perfect session specific temporary information secrecy attribute with nice computational efficiency than reported other schemes.

References

[1] R. Canetti, H. Krawczyk, "Analysis of key exchange protocols and their use for building secure channels," in *Proceedings of the Advances in Cryptology (EUROCRYPT'01)*, LNCS 2045, Springer-Verlag, pp. 453-474, 2001.

[2] X. F. Cao, W. D. Kou, K. Fan, J. Zhang, "An identity-based authenticated key agreement protocol without bilinear pairing," *Chinese Journal of Electronics & Information Technology*, vol. 31. no. 5, pp. 1241-1244, 2009.

[3] X. F. Cao, W. D. Kou, X. N. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *Information Sciences*, vol. 180, no. 15, pp. 2895-2903, 2010.

[4] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password

change protocol", *Computers & Mathematics with Applications*, vol. 49, pp. 703–714, 2005.

[5] L. Chen, and C. Kudla, "Identity based key agreement protocols from pairings," in *Proceedings of the 16th IEEE Computer Security Foundations Workshop*, pp. 219-213, 2002.

[6] A. Cilardo, L. Coppolino, N. Mazzocca, L. Romano, "Elliptic curve cryptography engineering," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 395-406, 2006.

[7] C. Gentry, "Practical identity-based encryption without random oracles," in *Proceedings of the EUROCRYPTO'06*, LNCS 4004, Springer-Verlag, pp. 445-464, 2006.

[8] L. C. Huang, M. S. Hwang, "Two-party authenticated multiple-key agreement based on elliptic curve discrete logarithm problem", *International Journal of Smart Home*, vol. 7, no. 1, pp. 9-18, Jan. 2013.

[9] M. S. Hwang, S. Y. Hsiao, W. P. Yang, "Security on improvement of modified authenticated key agreement protocol," *Information - An International Interdisciplinary Journal*, vol. 17, no. 4, pp.1173–1178, Apr. 2014.

[10] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[11] C. C. Lee, M. S. Hwang, L. H. Li, "A new key authentication scheme based on discrete logarithms", *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343-349, July 2003.

[12] I. C. Lin, C. C. Chang, M. S. Hwang, "Security enhancement for the simple authentication key agreement algorithm", in *Proceedings 24th Annual International Computer Software and Applications Conference (COMPSAC'00)*, 2000.

[13] T. K. Mandt, C. H. Tan, "Certificateless authenticated two-party key agreement protocols," in *Proceedings of the 11th Annual Asian Computing Science Conference (ASIAN'06)*, Secure Software and Related Issues, LNCS 4435, Springer-Verlag, pp. 37-44, 2008.

[14] N. McCullagh, and P. S. L. M. Barreto, "A new two-party identity-based authenticated key agreement," in *Proceedings of CT-RSA'05*, LNCS 3376, Springer-Verlag, pp. 262-274, 2005.

[15] H. H. Ou, M. S. Hwang, "Double delegation-based authentication and key agreement protocol for PCSs," *Wireless Personal Communications*, vol. 72, no. 1, pp. 437–446, Sep. 2013.

[16] A. Shamir, "Identity-based cryptosystems and signature schemes," in *CRYPTO'84*, LNCS 196, Springer, pp. 47–53, 1984.

[17] K. Shim, "Efficient ID-based authenticated key agreement protocol based on the Weil pairing," *Electronics Letters*, vol. 9, no. 8, pp. 653-654, 2003.

[18] N. P. Smart, "An identity based authenticated key agreement protocol based on the Weil pairing," *Electronics Letters*, vol. 38, no. 13, pp. 630-632, 2002.

[19] H. Sun and B. Hsieh, "Security analysis of Shim's authenticated key agreement protocols from pairings," *Cryptology ePrint Archive*, Report 2003/113, 2003. (http://eprint.iacr.org/2003/113)

[20] S. B. Wang, Z. F. Cao, and X. L. Dong, "Provably secure identity-based authenticated key agreement protocols in the standard model," *Chinese Journal of Computers*, vol. 30, no. 10, pp. 1842-1854, 2007.

[21] Y. Wang, "Efficient identity-based and authenticated key agreement protocol," *Cryptology ePrint Archive*, Report 2005/108, 2005.

Biography

Javad Saadatmandan received his Ph.D from the Department of Mathematics and Computer Sciences at Qom University in Qom, Iran. He is presently an assistant professor of mathematics at IAU, Qom, Iran. His research interest include cryptographic protocols and wavelet transforms.

Amir Hossein Rahimi received the B.Sc. degree in 2009 in applied mathematics from the University of Arak, Iran, and the M.Sc. degrees in 2014 in cryptography engineering from Malek-Ashtar University of Technology Isfehan. His current research interests include areas of communication theory, information security, cryptography, smart grid, steganography, digital signature and authentication protocols. He has published more than 10 papers in the fields mentioned. Also, he have been teaching mathematical sciences in universities of Qom province, Iran form 2015 until now. Email:Amir.Rahimi361@Gmail.Com