A Novel Secure Two-Party Identity-Based Authenticated Key Agreement Protocol Without Bilinear Pairings

Seyed-Mohsen Ghoreishi, Ismail Fauzi Isnin, Shukor Abd Razak and Hassan Chizari

Abstract Many Identity-Based two-party Key Agreement protocols have been proposed in recent years. Some of them are built on pairing maps, whereas some others could eliminate the pairings in order to decrease the complexity of computation. In this paper, we proposed a secure pairing-free Identity-Based two-party Key Agreement protocol which besides supporting security requirements uses less computational cost in comparison with existing related works.

Keywords Identity-based · Pairing-free · Two-party · Key Agreement · Efficiency

1 Introduction

A Key Agreement protocol enables two or more entities to establish a shared secret through an unsecure channel. In an Identity-Based Key Agreement protocol, the public key of involving entities is driven from their public identity. Since providing a secure session key in an unsecure channel is one of the most significant challenging issues, Key Agreement protocols received widespread attention in cryptography research community. It is worth to note that the focus of this paper is on two-party Identity-Based Key Agreement protocols.

S.-M. Ghoreishi (✉) · I.F. Isnin · S.A. Razak · H. Chizari
Faculty of Computing, Univeristi Teknologi Malaysia (UTM), 81310 Johor, Malaysia
e-mail: mohsen.gh100@gmail.com

I.F. Isnin
e-mail: ismailfauzi@utm.my

S.A. Razak
e-mail: shukorar@utm.my

H. Chizari
e-mail: chizari@utm.my

A. Abraham et al. (eds.), *Pattern Analysis, Intelligent Security and the Internet of Things*, Advances in Intelligent Systems and Computing 355,
DOI 10.1007/978-3-319-17398-6_26

In order to avoid complex certificate management in traditional public key cryptosystems (PKC), Shamir in [1] introduced a novel idea named identity-based cryptography. In this category of PKC, users' public key is their identity (e.g., telephone number, image, and email address). Therefore, both communicating entities should have knowledge about each other's identifier before starting the communication.

However, making this theory functional remained an open problem until 2001 that Boneh and Franklin in [2] could propose a fully functional identity-based encryption scheme.

Following the work of Boneh and Franklin, various identity-based cryptosystems including Key Agreement protocols have been published based on bilinear pairings [3–6]. Bilinear pairing is a cryptographic function that maps a pair of elements of two elliptic curve-based algebraic groups to an element of a determined finite field [7]. However, pairing operations have been considered as an expensive cryptographic function by consuming about twenty times more expensive computational cost than scalar multiplication over an elliptic curve group [7]. Hence, to avoid high computational cost of pairings, several Identity-Based pairing-free Key Agreement protocols have been proposed recently (refer to Sect. 2).

To improve the efficiency, we proposed a pairing-free Identity-Based Key Agreement protocol, named PF_{ID} *KA*.

The rest of this paper is organized as follows. Some related works are reviewed in the Sect. 2. In Sect. 3, preliminaries including utilized notations and description of main phases of Identity-Based Key Agreement protocols are described. Section 4 assigns to our proposed pairing-free Key Agreement protocol in detail. In Sect. 5, analysis over security and efficiency of the proposed protocol is provided. At last, we draw the conclusion.

2 Related Works

There exist many pairing-free two-party Key Agreement protocols over elliptic curve-based algebraic groups. In 2010, Cao et al. in [8] proposed a pairing-free Identity-Based authenticated Key Agreement protocol with two message exchanges. They could reduce the required message exchange in comparison with previous related works presented in [9, 10]. However, as shown in [11], the proposed protocol by Cao et al. in [10] was not secure against known session-specific temporary information attack and key offset attack. Islam and Biswas in [11] could propose an improved version that does not suffer from mentioned security flaws. Their proposed scheme requires less computational cost by the use of three scalar multiplication and one point addition.

Besides the proposed protocols above, Farash and Attari in [12] have tried to modify the proposed protocol of Cao et al. [10] by considering different private key generators.

3 Preliminaries

In this section, we are going to present the required preliminaries for this article.

3.1 Notations

The suggested notations and assumptions, which are needed to realize following sections, are listed as follows:

q	A large prime number
$\mathbb{F}_q$	A finite field over q
$E/\mathbb{F}_q$	An elliptic curve over $\mathbb{F}_q$
G	A subgroup of $E/\mathbb{F}_q$
P	A generator of the group G
s	A randomly chosen element of $\mathbb{Z}_q^*$
P_{pub}	sP
H_1, H_2	Two collision-free one-way hash functions
ID_i	Identity of user i
k_s	Session key

Next section explains the main phases of Key Agreement protocols in the context of identity-based cryptosystems in detail.

3.2 Main Phases of Identity-Based Key Agreement Protocols

A possible way to define an Identity-Based two-party Key Agreement protocol is to partition four sub-protocols as main phases. Based on this categorization, these phases are named SETUP, EXTRACTION, EXCHANGE, and COMPUTATION.

SETUP
In this phase, the corresponding algorithm takes the security parameter to generate Params and master key. A trusted third party named private key generator (PKG) keeps master key confidential, whereas Params must be publicly known to all entities.

EXTRACTION
In this phase, each entity can obtain his private key by interacting with the PKG.

EXCHANGE
In this phase, communicating parties compute a trapdoor one-way function of a randomly chosen value and exchange it.

COMPUTATION
In this phase, communicating parties can compute the considered session key as a function of Params and other possessing public and secret parameters.

4 Our Proposed Identity-Based Key Agreement Protocol

In this section, we propose our efficient pairing-free Identity-Based Key Agreement protocol (named PF_{ID} *KA*) which can satisfy all security requirements. The outline of current section is to investigate this protocol in detail.

SETUP
This algorithm generates the master key $s \in_r \mathbb{Z}_q^*$ randomly and then outputs Params $\langle q, \mathbb{F}_q, E/\mathbb{F}_q, G, P, P_{\text{Pub}}, H_1, H_2 \rangle$ by the use of taken security parameter. In Params, $H_1: \{0,1\}^* \times G \rightarrow \mathbb{Z}_q^*$ and $H_2: \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \rightarrow \mathbb{Z}_q^*$. The rest elements are introduced in Sect. 3.

EXTRACTION
In this phase, an entity such as the one who possesses ID_i identifier refers to PKG to take corresponding private key. The PKG first randomly chooses $r_i \in_r \mathbb{Z}_q^*$, then computes $R_i = r_i P$ and $h_i = H_1(ID_i, R_i)$. Finally, the entity's private key would be $\langle R_i, s_i \rangle$ where $s_i = r_i + h_i s (\text{mod}\, q)$.

Now assume that two entities, A and B, are going to agree on a session key. The EXCHANGE and COMPUTATION phases are as follows:

EXCHANGE
To explain the EXCHANGE phase, mentioned entities do the following:

1. A chooses a random $a \in_r \mathbb{Z}_q^*$, computes the key token $T_A = a(s_A P) = a((r_A + h_A s (\text{mod}\, q))P)$ and sends T_A, R_A to the entity B.
2. B chooses a random $b \in_r \mathbb{Z}_q^*$, computes the key token $T_B = b(s_B P) = b((r_B + h_B s (\text{mod}\, q))P)$ and sends T_B, R_B to the entity A.

COMPUTATION
In this phase, mentioned entities are able to compute the shared secret as follows:

A computes $K_{AB} = [a(r_A + h_A s (\text{mod}\, q))]T_B$
B computes $K_{BA} = [b(r_B + h_B s (\text{mod}\, q))]T_A$

Following equation proves that the two computed values for this shared secrets would be the same.

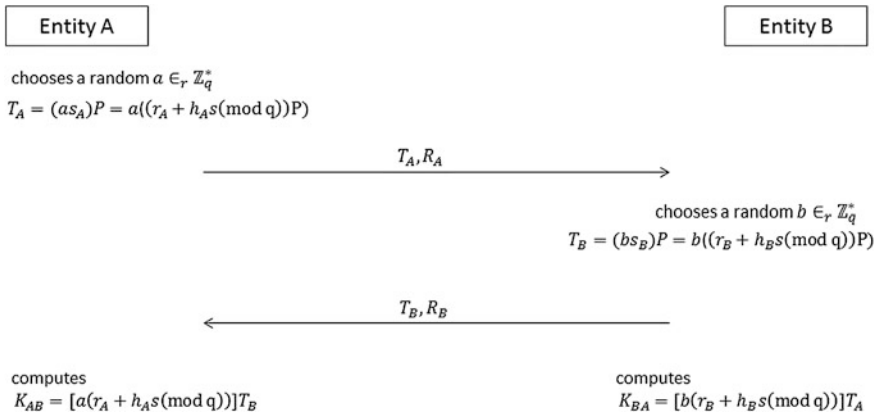

Fig. 1 Our proposed protocol

$$\begin{aligned} K_{AB} &= [a(r_A + h_A s(\text{mod } q))]T_B \\ &= (as_A)[b((r_B + h_B s(\text{mod } q))P)] \\ &= (as_A)(bs_B)P \\ &= [b(r_B + h_B s(\text{mod } q))]T_A \\ &= K_{BA} \end{aligned}$$

Finally, the agreed session key, k_s, is a key derivation function of K_{AB}:

$$\begin{aligned} k_s &= H_2(ID_A, ID_B, T_A, T_B, K_{AB}) \\ &= H_2(ID_A, ID_B, T_A, T_B, K_{BA}) \end{aligned}$$

Figure 1 illustrates PF_{ID} *KA* protocol in a general form.

5 Security and Efficiency Analysis

In this section, we will explain the required security considerations for a Key Agreement protocol. Moreover, we represent the computational cost of existing related works to compare them with our proposed protocol from computational efficiency viewpoint.

5.1 Security Considerations

In order to evaluate the security of Key Agreement protocols, one common approach is the use of following security features explained in [13, 14].

Known-Key Security (KKS)
The KKS indicates that any knowledge about past secret session keys do not lead to finding future ones. The main reason is that the secret session key is unique and independent from past established ones.

Forward Secrecy (FS)
A protocol can support this property if in the condition of leakage of entities' long-term private keys, the previously established session keys remain secret.

Perfect Forward Secrecy (PFS)
A protocol has this property if in the condition of leakage of entities' long-term private keys including PKG, the previously established session keys remain secret.

Key-Compromise Impersonation (KCI)
In the condition of compromising the long-term key of one of the entities, adversary can impersonate the victim to others but not vice versa.

Unknown Key-Share Resilience (UKSR)
Unknown key-share happens if an adversary could convince an entity to share a secret session key with him instead of a legitimate entity. A Key Agreement protocol should be resilient against this type of attack.

Key Control (KC)
This security property indicates that the secret session key would be generated by both communicating entities together. It means the session key should not be predetermined by one of them alone.

Known Session-Specific Temporary Information (KSSTI)
If the session key can be computable by the adversary in the condition of the leakage of a and b (refer to the EXCHANGE phase in Sect. 4), the protocol would be vulnerable to this attack.

It is worth to note that our proposed protocol supports all mentioned security attributes. In addition, it can provide key confirmation and prevent key offset attack if the entities A and B exchange message authentication code (MAC) of a significant message which is generated based on the session key (for more information refer to [11]).

5.2 Efficiency Considerations

As mentioned in the second section, related to our proposed protocol, several two-party Identity-Based Key Agreement protocols without bilinear pairings have been

Table 1 Efficiency comparisons of different protocols

Authors	Exchange and computation from A entity viewpoint	Computed exponentiation (scalar multiplication)	Computed point addition	Efficiency consideration
Cao et al. [8]	$T_A = aP, T_B = bP$ $K_{AB}^1 = s_A T_B + aS_B$ $K_{AB}^2 = aT_B$	$aP, s_A T_B, aS_B, aT_B,$	$(s_B T_A) + (bS_A)$	4 exponentiation (scalar multiplication) 1 point addition
Islam and Biswas [11]	$T_A = aS_A, T_B = bS_B$ $K_{AB} = s_A[T_B + aS_B]$	$aS_A, aS_B, s_A[T_B + aS_B]$	$T_B + (aS_B)$	3 exponentiation (scalar multiplication) 1 point addition
PF_{ID} *KA*	$T_A = a(s_A P)$ $K_{AB} = a(s_A[T_B])$	$a(s_A P), s_A T_B, a(s_A[T_B])$	–	3 exponentiation (scalar multiplication)

proposed. Cao et al. in [8] proposed a pairing-free Key Agreement protocol that has four scalar multiplications and one point addition. The proposed protocol by Islam and Biswas in [11] has only three scalar multiplications and one point addition. Moreover, in 2014, another pairing-free two-party Identity-Based Key Agreement scheme has been proposed by Farash et al. in [12] that has four scalar multiplications.

To clear our claim, Table 1 depicts details of proposed protocols in [8, 11] and the assigned computational costs.

As illustrated in Table 1, our proposed pairing-free Identity-Based Key Agreement protocol is quite efficient because it just requires three scalar multiplications without any point addition performed by each communicating participant.

6 Conclusion

In recent years, various pairing-free cryptosystems have been designed in order to reduce high cost of computation resulted by utilizing pairing maps. In this area, several pairing-free Key Agreement protocols in the context of Identity-Based cryptosystems have been proposed. In this paper, we could propose an authenticated Identity-Based two-party Key Agreement protocol without using pairing maps. The proposed protocol is efficient in comparison with existing related works.

Acknowledgments Authors would like to thank Universiti Teknologi Malaysia and Ministry of Higher Education, Malaysia, for sponsoring this research under vote number 01G98.

References

1. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Advances in Cryptology—Crypto 1984. Lecture Notes in Computer Science 196, Springer, Berlin (1984)
2. Boneh, D., Franklin, M.: Identity based encryption from the weil pairing. In: Advances in Cryptology—Crypto (2001)
3. Smart, N.P.: An identity based authenticated key agreement protocol based on the Weil pairing. Electron. Lett. **38**, 630–632 (2002)
4. Chen, L., Kudla, C.: Identity based authenticated key agreement from pairings. In: IEEE Computer Security Foundations Workshop, pp. 219–233 (2003)
5. Yuan, Q., Li, S.A.: A new efficient ID-based authenticated key agreement protocol. Cryptology ePrint Archive, Report 2005/309 (2005)
6. Wang, Y.: Efficient Identity-based and authenticated key agreement protocols. Transactions on Computational Science Xvii (2013)
7. Chen, L., Cheng, Z., Smart, N.P.: Identity-based key agreement protocols from pairings. Int. J. Inf. Secur. **6**, 213–241 (2007)
8. Cao, X., Kou, W., Du, X.: A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. Inf. Sci. **180**, 2895–2903 (2010)
9. Zhu, R.W., Yang, G., Wong, D.S.: An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices. Theor. Comput. Sci. **9**, 198–207 (2007)
10. Cao, X., Kou, W., Yu, Y., Sun, R.: Identity-based authentication key agreement protocols without bilinear pairings. IEICE Trans. Fundam. **91**(12), 3833–3836 (2008)
11. Islam, S.K.H., Biswas, G.P.: An improved pairing-free identity-based authenticated key agreement protocol based on ECC. Procedia Eng. **30**, 499–507. ISSN 1877-7058 (2012)
12. Farash, M.S., Attari, M.A.: A pairing-free ID-based key agreement protocol with different PKGs. Int. J. Netw. Secur. **16**(2), 143–148 (2014)
13. Cheng, Z., Nistazakis, M., Comley, R., Vasiu, L.: On the indistinguishability-based security model of key agreement protocols-simple cases. Cryptology ePrint Archieve, Report 2005/129 (2005)
14. Blake-Wilson, S., Johnson, D., Menezes, A.: Key agreement protocols and their security analysis. In: Proceedings of the 6th IMA International Conference on Cryptography and Coding, vol. 1335, pp. 30−45, LNCS, Springer, Berlin (1997)