New Secure Identity-Based and Certificateless Authenticated Key Agreement Protocols Without Pairings

Seyed-Mohsen Ghoreishi, Shukor Abd Razak, Ismail Fauzi Isnin and Hassan Chizari
Faculty of Computing,
Universiti Teknologi Malaysia
Skudai 81310, Johor, Malaysia
mohsen.gh100@gmail.com, {shukorar, ismailfauzi, chizari}@utm.my

***Abstract*—Recently, various pairing-based and pairing-free two party Key Agreement protocols in the context of Identity-Based and Certificateless cryptosystems have been published. The pairing-free Key Agreement protocols could improve the efficiency by eliminating the high expense of pairing maps. In this paper, we proposed several secure and efficient Identity-Based and Certificateless pairing-free two party Key Agreement protocols. In compare with related works, our protocols require less computational cost.**

Keywords—Identity-Based, Certificateless, Pairing-Free, Key Agreement, Efficiency

I. INTRODUCTION

A cryptographic protocol that enables two or more entities to generate a shared session secret by exchanging key tokens over an open channel, named Key Agreement protocol. In this category of cryptographic protocols, the final session key would be driven from mentioned shared secret. Due to the importance of the security of the used cryptographic session key in an open channel, Key Agreement protocols became one of critical issues in cryptographic research area.

The outline of this paper is to focus on two-party Key Agreement protocols in the context of Public Key Cryptography (PKC). Hence, existing entities possess a pair of keys; Public Key and Private Key. Based on the structure of the Public Key, it is possible to categorize existing public key cryptosystems in three classes named Traditional, Identity-Based and Certificateless. A Traditional public key cryptosystem relies on digital certificates provided by a trusted party named Certificate Authority (CA). In this group of cryptosystems, the need to CA leads to complex management of Public Key Infrastructure (for more details refer to [1]). To avoid mentioned drawback and to eliminate the need to certificates, Adi Shamir in [2] introduced a powerful theory named Identity-Based cryptography; replacing the users' Public Key with their identity (e.g. telephone number, image, email address, etc.). Hence, all involving entities need to learn some basic information (As an identifier) before they communicate with each other. This idea was an open problem for seventeen years, until Boneh and Franklin could propose a fully functional Identity-Based scheme in the context of Encryption primitives [3]. It is worth to note that in an Identity-Based cryptosystem, each entity takes its Private Key by interacting with a trusted third party named Private Key Generator (PKG). As a result, PKG might be able to eavesdrop the messages or impersonate entities. This inherent problem of Identity-Based cryptosystems is named "Key Escrow." To avoid this problem, the concept of Certificateless Public Key Cryptography (CL-PKC) was introduced by Al-Riyami and Paterson [4]. In this category of cryptosystems, a trusted third party named Key Generation Center (KGC) is responsible for generating partial private keys for existing users. This key is driven by Master Key (which is only known to KGC), and the users' identity. Once an entity receives this key material, chooses a secret value and then generates considered final Private Key. Hence, there is no problem regarding to the Key Escrow [4].

In continue to what pointed above, a subset of Identity-Based and Certificateless Key Agreement Protocols have been proposed based on Bilinear Pairings, which maps two elements of elliptic curve based algebraic groups to an element of a determined finite field [5]. However, high expense of computing pairing operations persuaded researchers to propose ECC-based Key Agreement protocols. To improve the efficiency and supporting more security options, we proposed several Key Agreement protocols without bilinear pairings in the context of Identity-based and Certificateless cryptosystems.

The rest of this paper is organized as follows. The second section describes some preliminaries including utilized notations and description of main phases of Identity-Based and Certificateless Key Agreement protocols. In the next section, we present our pairing-free Key Agreement protocols in detail. In the forth section, analysis over security and efficiency of the

978-1-4799-6444-4/14/$31.00 ©2014 IEEE

proposed protocols is provided. The last section assigns to the conclusion.

II. PRELIMINARIES

This section introduces the required preliminaries for the rest of this paper. The TABLE I introduces suggested notations and assumptions, which are needed to realize following subsections.

TABLE I. SUGGESTED NOTATIONS AND ASSUMPTIONS

Notation	Description
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	Generator of the group G
P_{Pub}	sP

Next subsection represents detail explanations of the main phases of Key Agreement protocols, in the context of Identity-Based cryptosystems.

A. Main phases of Identity-Based Key Agreement protocols

Based on our categorization, it is possible to define an Identity-Based Key Agreement protocol in four phases. The first and second phases are SETUP and EXTRACTION, respectively. The utilized algorithm of the SETUP phase is responsible to generate Params and Master-Key, after taking the required security parameter. The first parameter, Params, is publicly known to all entities whereas the Master-Key is a confidential secret for PKG. In the next phase, EXTRACTION, each entity can take his Private-Key after an interaction with the PKG. We named the third and fourth phases of Identity-Based Key Agreement protocols EXCHANGE and COMPUTATION, respectively. In the EXCHANGE phase, communicating parties compute a trapdoor one-way function of a randomly chosen value and exchange it. Then, in the COMPUTATION phase, parties can compute the considered session key based on the Params and other possessing public and secret parameters.

B. Main phases of Certificateless Key Agreement protocols

Based on our categorization, it is possible to define a Certificateless key agreement protocol in five phases, which are SETUP, PARTIAL-PRIVATE EXTRACT, SET-PRIVATE-PUBLIC KEYS, EXCHANGE, and COMPUTATION. Similar to the Identity-Based Key Agreement protocols, the considered algorithm of the SETUP phase is responsible to generate Params and Master-Key, after taking the security parameter. In the PARTIAL-PRIVATE EXTRACT phase, the KGC returns a partial-private to the entity who made a request. Afterward, each entity chooses a random value to compute his public and private keys in SET PRIVATE-PUBLIC KEYS phase. Finally, the entities can interact with each other to share the final session key in the fourth and fifth phases.

III. OUR PROPOSED KEY AGREEMENT PROTOCOLS

In this research, we propose two groups of efficient Key Agreement schemes. The first group is consisted of two Identity-Based cryptographic schemes, while the other one is consisted of a Certificateless scheme. The outline of current subsections is to investigate these protocols in detail. In all proposed Key Agreement protocols, it is assumed that involving entities, A and B, exchange one-way functions T_A and T_B of randomly chosen values to compute the shared secret K_{AB}. Finally, the agreed session key is a key derivation function of K_{AB}.

A. Proposed Identity-Based Key Agreement Protocols

In this section, we describe the proposed computationally efficient Identity-Based Key Agreement protocols which are the same in SETUP and EXTRACTION phases as follows:

SETUP: The SETUP algorithm of the proposed Identity-Based Key Agreement protocols takes the security parameter, k, and returns a master key $s \in \mathbb{Z}_q^*$ and Params $< q, \mathbb{F}_q, E/\mathbb{F}_q, G, P, P_{Pub}, H_1 >$ that $H_1: \{0,1\}^* \times G \to \mathbb{Z}_q^*$ is one-way collision-free hash function and other items are introduced in the TABLE I.

EXTRACTION: To explain the EXTRACTION phase, assume that an entity who possesses ID_i identifier refers to PKG to take corresponding Private Key. Here, the PKG first randomly chooses $r_i \in_r \mathbb{Z}_q^*$, then computes $R_i = r_i P$ and $h_i = H_1(ID_i, R_i)$. The final Private Key of this entity would be $< R_i, s_i >$ that $s_i = r_i + h_i s (\text{mod q})$.
Beside of two mentioned phases above, other phases of proposed Identity-Based Key Agreement schemes are explained separately for each protocol as follows:

- **Protocol-1:** Assume that two entities, A and B, are going to agree on a session key. It is necessary to point out that all entities such as an entity who possesses ID_i identifier, randomly chooses $x_i \in_r \mathbb{Z}_q^*$, then computes $X_i = x_i P$, $z_i = x_i + h_i' s_i (\text{mod q})$, and $Z_i = z_i P$. Here, $h_i' = H_1(ID_i, X_i)$. Before starting the first session, the entity A sends R_A, X_A to the B entity, while B entity returns back the values R_B, X_B to the A entity. Then, EXCHANGE and COMPUTATION phases are based on following processes:

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 $T_A = a(s_A z_A Z_B)$and sends T_A to the B entity.
(2) B chooses a random $b \in_r \mathbb{Z}_q^*$, computes the key token $T_B = b(s_B z_B Z_A)$ and sends T_B to the A entity.

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

A computes $K_{AB} = [a(s_A)]T_B$
B computes $K_{BA} = [b(s_B)]T_A$

Following equation proves that the two computed values for this shared secrets would be the same.
$K_{AB} = \left[a\left(r_A + h_A s(\text{mod q})\right)\right]T_B$
$= (as_A)[b(s_B z_B z_A)\text{P}]$
$= (bs_B)[a(s_A z_A z_B)\text{P}]$
$= [b(r_B + h_B s(\text{mod q}))]T_A$
$= K_{BA}$
Before explaining the next proposed Identity-Based Key Agreement protocol, it is necessary to point out that it is possible to assume that $z_i = x_i$, and $Z_i = z_i P$. In addition, it is possible to assume $z_i = x_i + s_i$, and $Z_i = z_i P$. Applying these two assumptions for the EXCHANGE and COMPUTATION phases above, leads to achievement of two other versions for the Protocol-1.

- **Protocol-2:** Assume that two entities, A and B, are going to agree on a session key. It is necessary to point out that all entities such as an entity who possesses ID_i identifier, randomly chooses $x_i \in_r \mathbb{Z}_q^*$, then computes $X_i = x_i P$, $z_i = x_i + h_i' s_i(\text{mod q})$, and $Z_i = z_i P$. Here, $h_i' = H_1(ID_i, X_i)$. Before starting the first session, the entity A sends R_A, X_A to the B entity, while B entity returns back the values R_B, X_B to the A entity. Then, EXCHANGE and COMPUTATION phases are based on following processes:

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 $T_A = a(z_A s_A S_B)$ that $S_B = s_B P$. Then, sends T_A to the B entity.
(2) B chooses a random $b \in_r \mathbb{Z}_q^*$, computes the key token $T_B = b(z_B s_B S_A)$ that $S_A = s_A P$. Then, sends T_B to the A entity.

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

A computes $K_{AB} = [a\left(x_A + h_A' s_A(\text{mod q})\right)]T_B$
B computes $K_{BA} = [b\left(x_B + h_B' s_B(\text{mod q})\right)]T_A$

Following equation proves that the two computed values for this shared secrets would be the same.
$K_{AB} = \left[a\left(x_A + h_A' s_A(\text{mod q})\right)\right]T_B$
$= (az_A)[b(z_B s_B s_A)\text{P}]$
$= (bz_B)[a(z_A s_A s_B)\text{P}]$
$= [b(x_B + h_B' s_B(\text{mod q}))]T_A$
$= K_{BA}$
Before explaining our proposed Certificateless Key Agreement protocol, it is necessary to point out that it is possible to assume that $z_i = x_i$, and $Z_i = z_i P$. In addition, it is possible to assume $z_i = x_i + s_i$, and $Z_i = z_i P$. Applying these two assumptions for the EXCHANGE and COMPUTATION phases above, leads to achievement of two other versions for the Protocol-2.

B. Proposed Certificateless Key Agreement Protocol

In this section, we describe the proposed computationally efficient Certificateless Key Agreement protocol.

- **Protocol-3:** The SETUP, PARTIAL-PRIVATE-EXTRACT and SET-PUBLIC-PRIVATE KEYS phases are as follows:

SETUP: This algorithm takes the security parameter and returns a master key $s \in \mathbb{Z}_q^*$and Params $< q, \mathbb{F}_q, E/\mathbb{F}_q, G, P, P_{Pub}, H_1 >$ that $H_1: \{0,1\}^* \times G \rightarrow \mathbb{Z}_q^*$.

PARTIAL-PRIVATE-EXTRACT: This algorithm takes $r_i \in_r \mathbb{Z}_q^*$ and computes $R_i = r_i P$ and $h_i = H_1(ID_i, R_i)$.Then, the partial-private-key of the user i will be $s_i = r_i + h_i s(\text{mod q})$.

SET-PUBLIC-PRIVATE KEYS: This algorithm takes $x_i \in_r \mathbb{Z}_q^*$ and computes $X_i = x_i P$, $z_i = x_i + h_i' s_i(\text{mod q})$, and $Z_i = z_i P$. Here, $h_i' = H_1(ID_i, X_i)$. The private and public key of the user i will be $SK_i = (s_i, x_i)$ and $PK_i = (R_i, S_i, X_i)$, respectively. Here, the value of $S_i = \left(R_i + h_i P_{pub}\right) = s_i P$ will be publicly computable by all entities. Beside of three mentioned phases above, other phases of the proposed Certificateless Key Agreement scheme 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 $T_A = a(z_A s_A S_B)$. Then, sends T_A to the B entity.
(2) B chooses a random $b \in_r \mathbb{Z}_q^*$, computes the key token $T_B = b(z_B s_B S_A)$. Then, sends $T_B$to the A entity.

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

A computes $K_{AB} = [a\left(x_A + h_A^{'}s_A(\text{mod q})\right)]T_B$

B computes $K_{BA} = [b\left(x_B + h_B^{'}s_B(\text{mod q})\right)]T_A$

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

$K_{AB} = \left[a\left(x_A + h_A^{'}s_A(\text{mod q})\right)\right]T_B$
$= (az_A)[b(z_B s_B s_A)\text{P}]$
$= (bz_B)[a(z_A s_A s_B)\text{P}]$
$= [b(x_B + h_B' s_B(\text{mod q}))]T_A$
$= K_{BA}$

It is worth to note that it is possible to consider other condition for this protocol in a way that an entity who possesses ID_i identifier, randomly chooses $x_i \in_r \mathbb{Z}_q^*$, then computes $X_i = x_i P$. It is possible to assume $z_i = x_i + s_i$, and $Z_i = z_i P$. Applying these two assumptions for the EXCHANGE and COMPUTATION phases above, leads to achievement of two other versions for the Protocol-3.

IV. Security And Efficiency Analysis

In this section, we are going to discuss about the security and efficiency of the proposed protocols. Our proposed Key Agreement protocols could achieve all security attributes and it is efficient in compare with other existing related works.

A. Security Considerations

One possible method for evaluating the security of key agreement protocols is the use of following security properties as defined in [6, 7].

- ***Known-Key Security (KKS):*** To satisfy this security property, peer entities should generate a unique secret session key which is independent from generated secret session keys in past sessions. Therefore, any knowledge about past secret session keys do not allow deducting future secret session keys.

- ***Forward Secrecy (FS)*:** The Forward Secrecy property is that if long-term private keys of the entity(ies) be compromised, the previously established session keys must be still secret.

- ***Perfect Forward Secrecy (PFS):*** A system has Perfect Forward Secrecy if previously established session keys by entities are not corrupted even after compromising the long-term keys of all the involving entities (including the Key Generation Center).

- ***Key-Compromise Impersonation*:** A protocol is secure against Key Compromise Impersonation attack if compromising the long-term key of one entity help the adversary to impersonate the victim to others but does not lead to impersonating others to the victim.

- ***Unknown Key-Share Resilience:*** A protocol is resilient against the Unknown Key-Share attack, if the entity does not share the secret session key with the adversary. Unknown Key-Share happens when the adversary convinces the entity to share a secret session key with him while victim mistakenly believes that he shared a secret with a legitimate entity.

- ***Key Control:*** To satisfy this security property, the generated key should be determined jointly by both peer entities; not predetermined by one of them alone.

- ***Known Session-Specific Temporary Information:*** a protocol is vulnerable against this attack if an adversary can compute k_s by assuming the leakage of a and b.

Since the agreed keys in our proposed protocols satisfy all above mentioned security attributes, our protocols are secure against mentioned issues. In addition, by assuming that the entities A and B compute a Message Authentication Code (MAC) of a significant message by the use of the agreed key k_s, and exchange the result with each other, our proposed protocols support key conformation property and prevent Key Off-Set attack (for more detail refer to [8]).

B. Efficiency Considerations

Related to our protocols, a subset of Identity-Based and Certificateless Key Agreement Protocols have been proposed. A two-party Identity-Based Key Agreement without bilinear pairings has been proposed by Cao et al. in [9] that has four scalar multiplications and one addition. The proposed protocol by Hafizul Islam et al. in [8] 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 [10] that has four scalar multiplications. In addition, in the context of Certificateless Key Agreement protocols without pairings, Hou et al. proposed a protocol with four scalar multiplications [11]. The proposed protocol by Geng et al. in [12] computes five scalar multiplications. In 2011, He et al. in [13] proposed another protocol that computes four scalar multiplications and one point addition for key computation. Moreover, another scheme is proposed in [14] based on computing four scalar multiplications and two point additions.

The TABLE II depicts details of some proposed protocols and the assigned computational costs.

As we can see in TABLE II, from efficiency viewpoint, our proposed Key Agreement protocols only compute three scalar multiplications without computing any point addition for each communicating entities, which are quite efficient.

TABLE II. EFFICIENCY COMPARISIONS OF DIFFERENT PROTOCOLS

Authors	**Exchange and computation from A entity viewpoint**	**Computed Exponentiation (Scalar Multiplication)**	**Computed point addition**	**Efficiency Consideration**
Cao et al. [9]	$T_A = aP, T_B = bP$ $K_{AB}^1 = s_A T_B + aS_B$ $K_{AB}^2 = aT_B$	$aP, s_A T_B, aS_B, aT_B$	$(s_B T_A) + (bS_A)$	4 Exponentiation (Scalar Multiplication) 1 point addition
Islam et al. [8]	$T_A = aS_A, T_B = bS_B$ $K_{AB} = s_A[T_B + aS_B]$	$aS_A, aS_B, s_A[T_B + aS_B]$	$T_B + (aS_B)$	3 Exponentiation (Scalar Multiplication) 1 point addition
He et al. [13]	$T_A = aP, T_B = bP$ $K_{AB}^1 = (x_A + s_A)T_B + a(X_B + S_B)$ $K_{AB}^2 = aT_B$	$aP, (x_A + s_A)T_B,$ $a(X_B + S_B), aT_B$	$[(x_A + s_A)T_B] + [a(X_B + S_B)]$	4 Exponentiation (Scalar Multiplication) 1 point addition
He et al. [14]	$T_A = aP, T_B = bP$ $K_{AB}^1 = (a + s_A)[T_B + S_B]$ $K_{AB}^2 = (a + x_A)[T_B + X_B]$ $K_{AB}^3 = aT_B$	$aP, (a + s_A)[T_B + S_B],$ $(a + x_A)[T_B + X_B], aT_B$	$(T_B + S_B), (T_B + X_B)$	4 Exponentiation (Scalar Multiplication) 2 point addition
Our proposed Protocol-1	$T_A = a(s_A z_A Z_B), T_B = b(s_B z_B Z_A)$ $K_{AB} = [as_A]T_B$	$a(s_A z_A Z_B), [as_A]T_B$	-	3 Exponentiation (Scalar Multiplication)
Our proposed Protocol-2	$T_A = a(z_A s_A S_B), T_B = b(z_B s_B S_A)$ $K_{AB} = [az_A]T_B$	$a(z_A s_A S_B), [az_A]T_B$	-	3 Exponentiation (Scalar Multiplication)
Our proposed Protocol-3	$T_A = a(z_A s_A S_B), T_B = b(z_B s_B S_A)$ $K_{AB} = [az_A]T_B$	$a(z_A s_A S_B), [az_A]T_B$	-	3 Exponentiation (Scalar Multiplication)

V. CONCLUSION

Due to the high computational cost of Bilinear Pairings, the pairing-free cryptosystems attracted researchers in recent years. In this area, a subset of pairing-free Key Agreement protocols in the context of Identity-Based and Certificateless cryptosystems have been proposed. In this paper, we could propose several secure and authenticated Identity-Based and Certificateless two-party Key Agreement protocols without pairings. The proposed protocols are efficient in compare with related works.

REFERENCES

[1] C. Adams and S. Lloyd. (2003) ."Understanding Public-Key Infrastructure" . Concepts, Standards, and Deployment Considerations..2nd ed, Pearson education, Boston, USA.

[2] A. Shamir, (1984). "Identity-Based Cryptosystems And Signature Schemes", In Advances In Cryptology—Crypto 1984, Lecture Notes In Comput.Sci. 196, Springer-Verlag, Berlin, 1984.

[3] D. Boneh, M. Franklin. (2001). "Identity Based Encryption From The Weil Pairing". Advances In Cryptology—Crypto.

[4] S.S.Al-Riyami K.G.Paterson. (2003). "Certificateless public key cryptography". page 452C473. C.S. Laih (ed.) Advances in Cryptology C Asiacrypt 2003, Lecture Notes in Computer Science.

[5] L Chen, Z Cheng, NP Smart – (2007). "Identity-Based Key Agreement Protocols From Pairings" .International Journal Of Information Security– Springer.

[6] Z. Cheng, M. Nistazakis, R. Comley, L. Vasiu. (2005). "On the in distinguishability-based security model of key agreement protocols-simple cases", Cryptology ePrint Archieve, Report 2005/129.

[7] S. Blake-Wilson, D. Johnson, A. Menezes. (1997). "Key agreement protocols and their security analysis", Proc. of the 6th IMA International Conference on Cryptography and Coding, LNCS, Springer-Verlag, 1335:30−45.

[8] SK Hafizul Islam, G.P. Biswas. (2012). "An improved pairing-free identity-based authenticated key agreement protocol based on ECC". Procedia Engineering, Volume 30, Pages 499-507, ISSN 1877-7058.

[9] X. Cao, W. Kou, X. Du. (2010). "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges", Information Sciences. 180:2895−2903.

[10] M.S. Farash, M.A. Attari. (2014). "A pairing-free ID-based key agreement protocol with different PKGs". Int. J. Network Security 16(2), 143–148.

[11] M. Hou, Q. Xu. (2009). "A two-party certificateless authenticated key agreement protocol without pairing", in: 2nd IEEE International Conference on Computer Science and Information Technology, pp. 412–416.

[12] M. Geng, F. Zhang. (2009). "Provably secure certificateless two-party authenticated key agreement protocol without pairing", in: International Conference on Computational Intelligence and Security, pp. 208–212.

[13] Debiao He, Yitao Chen, Jianhua Chen, Rui Zhang, Weiwei Han. (2011). "A new two-round certificateless authenticated key agreement protocol without bilinear pairings", Mathematical and Computer Modelling, Volume 54, Issues 11–12, Pages 3143-3152, ISSN 0895-7177.

[14] Debiao He, Sahadeo Padhye, Jianhua Chen, (2012), "An efficient certificateless two-party authenticated key agreement protocol", Computers & Mathematics with Applications, Volume 64, Issue 6, , Pages 1914-1926, ISSN 0898-1221.