Secure and Authenticated Key Agreement Protocol with Minimal Complexity of Operations in the Context of Identity-Based Cryptosystems

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

Abstract— **Recently, a large variety of Identity-Based Key Agreement protocols have tried to eliminate the use of Bilinear Pairings in order to decrease complexity of computations through performing group operations over Elliptic Curves. In this paper we propose a novel pairing-free Key Agreement protocol over elliptic curve based algebraic groups. The results show that our proposed protocol is significantly less complex than related works from complexity of computation perspective.**

Keywords- Key Agreement; Identity-Based; Elliptic Curve; efficiency

I. INTRODUCTION

A fundamental cryptographic primitive that makes a pair or group of entities able to generate a shared session key is named Key Agreement protocol. The importance of Key Agreement protocols in the context of Public Key Cryptography (PKC) is due to the fact that the shared session key is driven from exchanged key materials in unsecure channel. Hence, providing security in such condition is a critical challenging issue.

In certificate-based PKC, to provide authentic public key, a Certification Authority (CA) is responsible to issue digital certificates. However, this type of PKC suffers from complex management of certificates (for more details refer to [1]). To solve mentioned problem Identity-Based Cryptography have been suggested by Adi Shamir in [2]. In Identity-Based PKC, the public key of users is their identity such as telephone number, image, email address and etc. Although the idea of Identity-Based Cryptography seems interesting, it remained impractical until 2001 that Boneh and Franklin could propose a fully functional Identity-Based scheme [3].

Followed by the mentioned work, many Identity-Based Key Agreement protocols have been proposed by the use of Bilinear Pairings [4-10]. Bilinear Pairings is a cryptographic function which maps two points of elliptic curve based algebraic groups to an element of a determined finite field [11]. High computational cost of performing Pairing operation led researchers proposing Pairing-Free Identity-Based Key Agreement protocols in recent years [12-15]. This new generation of Identity-Based Key Agreement protocols utilize cryptographic operations over elliptic curve based algebraic groups. In this paper we propose a Pairing-Free Identity-Based Key Agreement protocol which has better performance in compare with existing related works from computational cost perspective.

The organization of the rest of this paper is as followed. In the second section, required technical backgrounds including Bilinear Pairings are described. Some of existing Identity- Based Key Agreement protocols are reviewed in Section III. We introduce our proposed Pairing-free Key Agreement protocol in the fourth section. In Section V, we compared our proposed protocol with some related works from efficiency viewpoint. Finally in the last section, the conclusion of this paper is provided.

II. TECHNICAL BACKGROUND

The basis of this section is representing the required technical background for the rest of this paper. The following subsection briefly introduces Bilinear Pairings in detail.

A. Bilinear Pairings

A Bilinear Pairing is a cryptographic function such as $\hat{e}: G_1 \times G_2 \rightarrow G_T$ in which G_1, G_2 and G_T are three algebraic groups with same prime order and $\hat{e}$ is a bilinear map that has three main features "bilinearity", "non-degeneracy" and "computability". The first feature means that $\forall P \in G_1$, $\forall Q \in G_2$, $\forall a, b \in \mathbb{Z}_q$: $\hat{e}(P^a, Q^b) = \hat{e}(P, Q)^{ab}$. The second feature refers to this fact that if 1_1 , 1_2 and 1_T are identity elements of G_1, $G_2$and G_T, respectively, then *"$\hat{e}$"* do not

map any pair of $(G_1 \times G_2)$ to I_T unless (I_1, I_2). Finally, there must be an efficient algorithm for computation of $\hat{e}(P, Q)$ where P and Q are the elements of G_1 and G_2, respectively.

Due to the variety of pairing-based applications, many researches have been done in order to design efficient pairing maps such as well-known works Weil pairing and Tate pairing [16,17]. Design and implementation of pairing maps is a complex mathematical issue and this research excludes the details of this category of works. It is worth to note that in this research the considered Identity-Based Key Agreement protocols utilized Bilinear Pairings as a building block operation.

III. RELATED WORKS

The focus of this section is on the review of existing Identity- Based Key Agreement protocols. We categorized existing related works into two groups; Pairing-Based protocols and Pairing-Free ones. The following, sub-section reviews a Pairing-Based Identity-Based Key Agreement protocol. Then, a separated sub-section reviews a subset of existing Pairing-Free Identity-Based Key Agreement protocols.

A. Pairing-Based Identity-Based Key Agreement protocol

In this sub-section a Pairing-Based Key Agreement protocol in the context of Identity-Based PKC [10] is investigated. The utilized notations and assumptions are as followed:

- q: A large prime number
- G: An additive algebraic groups over Elliptic Curves
- G_T: A multiplicative algebraic groups over a Finite Field
- $|G| = |G_T| = \mathrm{I}\mathbb{Z}^*q\,\mathrm{I}$: The order of groups
- $\hat{e}: G \times G \rightarrow G_T$: A Bilinear Pairing
- g: A generator of G
- $H_1: \{0,1\}^* \rightarrow G$: A one-way collision-free hash function
- $H_2: G \times G \rightarrow G_T$: A one-way collision-free hash function
- $s \in_r \mathbb{Z}^*q$: Master-Key

By considering that two users such as A and B wants to agree on a session key, the proposed protocol by Wang et al. [10] consists following phases.

SETUP. In this phase, Master-Key and system parameters (Params) will be generated after taking the considered security parameter. Master-Key $s \in_r \mathbb{Z}^*q$ is a secret for a Trusted Third Party named PKG [1] while Params $< q, G, G_T, g, \hat{e}, H_1, H_2 >$ are publicly known to all involving users.

EXTRACTION. In this phase, each user such as i who possesses ID_i identifier can refer to PKG to collect corresponding Private-Key. To generate the user's Private Key, PKG first computes $Q_i = H_1(ID_i)$, then generates $d_i = sQ_i$ as the user's Private Key and sends to the user.

EXCHANGE. In this phase, mentioned users do the following:

(1) User A chooses a random $t_A \in_r \mathbb{Z}^*q$, and computes the key token $T_A = t_A Q_A$ then transfers T_A to the user B.

(2) User B chooses a random $t_B \in_r \mathbb{Z}^*q$, and computes the key token $T_B = t_B Q_B$ then transfers T_B to the user A.

COMPUTATION. In this phase, user A and user B can compute the shared secret by performing following computations:

A computes $s_A = H_2(T_A, T_B)$, $s_B = H_2(T_B, T_A)$ and $\hat{e}((t_A + s_A)d_A, s_B Q_B + T_B))$

B computes…..$s_B = H_2(T_B, T_A)$, $s_A = H_2(T_A, T_B)$ and $\hat{e}(s_A Q_A + T_A, (t_B + s_B)d_B))$

The final session key will be $\hat{e}(Q_A, Q_B)^{s(t_A+s_A)(t_B+s_B)}$

B Pairing-Free Identity-Based Key Agreement protocols

A subset of existing Identity-Based Key Agreement protocols that do not rely on the use of Bilinear Pairings are reviewed in this sub-section. Since the mentioned protocols do not require any Pairing computation, the overall computational cost of session key generation process is significantly lower than the Pairing-Based ones. In order to have a clear review we utilized same notations and assumptions in the considered protocols as followed:

- 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 $E/\mathbb{F}_q$
- $s \in_R \mathbb{Z}^*_q$: A randomly chosen value from $\mathbb{Z}^*_q$
- P: A generator of the group G
- ID_i: Identifier of the entity i
- H_1: one-way collision-free hash function, where $H_1: \{0,1\}^* \times G \rightarrow \mathbb{Z}^*_q$
- H_2: $\{0,1\}^* \times \{0,1\}^* \times G \times G \times G \times G \times G \times G \times G \rightarrow \{0,1\}^k$ where k is the number of bits for the prime q

Followed by what mentioned above, we are going to review the considered Pairing-Free Identity-Based Key Agreement protocols in details. In general, mentioned protocols can be seen in four main phases named "setup", "extraction", "exchange", and "computation". It is worth to note that, since the two initial phases of the considered Pairing-Free Identity- Based Key Agreement protocols are the same, we introduced them first. Then, the consequent phases are reviewed separately for each protocol.

SETUP. In this phase, the corresponding algorithm generates system parameters (Params) and Master-Key after taking the considered security parameter. Master-Key $s \in_R \mathbb{Z}^*_q$ is a secret for PKG while Params $<q, \mathbb{F}_q, E/\mathbb{F}_q, G, P, P_{Pub} = sP, H_1, H_2>$ are publicly known to all involving users.

EXTRACTION. In this phase, each user such as i who possesses ID_i identifier can refer to PKG to collect corresponding Private-Key. To generate the user's Private Key, PKG randomly chooses $r_i \in_R \mathbb{Z}^*_q$, then computes $R_i = r_i P$, $h_i = H_1 (ID_i, R_i)$ and $s_i = r_i + h_i s (mod\ q)$ then returns $< R_i, s_i >$ as a Private Key to the user.

After these phases users are able to agree on a session key through EXCHANGE and COMPUTATION phases of each protocol.

EXCHANGE and COMPUTATION phases of proposed protocol by Cao et al. [14]

By considering that two users such as A and B wants to agree on a session key, the proposed protocol by Cao et al. [14] consists of EXCHANGE and COMPUTATION phases as followed.

EXCHANGE. In this phase, mentioned users do the following:

(1) User A chooses a random $t_A \in_R \mathbb{Z}^*_q$, and computes the key token $T_A = t_A P$ then transfer T_A, R_A to the user B.

(2) User B chooses a random $t_B \in_R \mathbb{Z}^*_q$, and computes the key token $T_B = t_B P$ then transfer T_B, R_B to the user A.

COMPUTATION. In this phase, user A and user B can compute the shared secret as follows:

A computes $K^1_{AB} = s_A T_B + t_A (R_B + h_B P_{pub})$ and $K^2_{AB} = t_A T_B$

B computes $K^1_{BA} = s_B T_A + t_B (R_A + h_A P_{pub})$ and $K^2_{BA} = t_B T_A$

The final session key will be the output of driven function of this shared secrets and some public/private values.

EXCHANGE and COMPUTATION phases of proposed protocol by Islam et al. [15]

By considering that two users such as A and B wants to agree on a session key, the proposed protocol by Islam et al. [15] consists of EXCHANGE and COMPUTATION phases as followed.

EXCHANGE. In this phase, mentioned users do the following:

(1) User A chooses a random $t_A \in_R \mathbb{Z}^*_q$, and computes the key token $T_A = t_A (R_A + h_A P_{pub})$ then transfer T_A, R_A to the user B.

(2) User B chooses a random $t_A \in_R \mathbb{Z}^*_q$, and computes the key token $T_B = t_B (R_B + h_B P_{pub})$ then transfer T_B, R_B to the user A.

COMPUTATION. In this phase, user A and user B can compute the shared secret as follows:

A computes $K_{AB} = s_A [T_B + t_A (R_B + h_B P_{pub})]$

B computes $K_{BA} = s_B [T_A + t_B (R_A + h_A P_{pub})]$

Following equation shows the equivalency of K_{AB} and K_{BA} as the shared secret.

$K_{AB} = s_A[T_B + t_A(R_B + h_B P_{pub})]$

$= t_B s_A s_B P + t_A s_A s_B P$

$= s_B[T_A + t_B(R_A + h_A P_{pub})]$

$= K_{BA}$

The final session key will be the output of driven function of this shared secrets and some public/private values.

IV. THE PROPOSED PROTOCOL

In this paper, we could propose a secure Identity-Based Key Agreement protocol that does not rely on Bilinear Pairings. In this section, we introduce our work in detail. Similar to other considered Pairing-Free Identity-Based Key Agreement protocols, our proposed protocol consists of four main phases named "setup", "extraction", "exchange", and "computation".

SETUP. Similar to the reviewed works, in this phase the Master-Key $s \in_r \mathbb{Z}^*_q$ and Params $< q, \mathbb{F}_q, E/\mathbb{F}_q, G, P, P_{Pub}, H_1, H_2 >$ will be generated by using the taken security parameter where $H_1: \{0,1\}^* \times G \rightarrow \mathbb{Z}^*_q$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}^*_q$ (the other parameters in Params are the same as what have been introduced in the previous section). It is worth to remind that Master-Key will be kept confidential for PKG while Params are publicly known to all involving users.

EXTRACTION. In this phase, each user such as i who possesses ID_i identifier can refer to PKG to obtain the corresponding Private-Key. To generate the user's Private Key, PKG randomly chooses $r_i \in_r \mathbb{Z}^*_q$, then computes $R_i = r_i P$, $h_i = H_1(ID_i, R_i)$ and $s_i = r_i + h_i s \pmod q$ then returns $< R_i, s_i >$ as a Private Key to the user. Note that all users such as i who possesses ID_i identifier, randomly chooses $p_i \in_r \mathbb{Z}^*_q$, then computes $P_i = p_i P$, $q_i = s_i + H_2(ID_i)p_i$, and $Q_i = q_i P$. By considering that two users such as A and B, are going to agree on a session key, EXCHANGE and COMPUTATION phases are as followed:

EXCHANGE. Before applying EXCHANGE phase, communicating participants, A and B, transmit items, $< R_A, P_A >$ and $< R_B, P_B >$, respectively. This transmission occurs one time before the first session key establishment. Afterward, EXCHANGE phase can be performed frequently as followed:

(1) User A chooses a random $t_A \in_r \mathbb{Z}^*_q$, and computes the key token $T_A = ((t_A s_A)(s_A + H_2(ID_A)p_A))[S_B + H_2(ID_B)P_B]$ then transfer T_A, R_A, P_A to the user B.

(2) User B chooses a random $t_B \in_r \mathbb{Z}^*_q$, and computes the key token $T_B = ((t_B s_B)(s_B + H_2(ID_B)p_B))[S_A + H_2(ID_A)P_A]$ then transfer T_B, R_B, P_B to the user A.

COMPUTATION. In this phase, user A and user B can compute the shared secret as follows:

A computes $K_{AB} = (t_A s_A) T_B$

B computes $K_{BA} = (t_B s_B) T_A$

Following equation shows the equivalency of K_{AB} and K_{BA} as the shared secret.

$K_{AB} = (t_A s_A)((t_B s_B)(s_B + H_2(ID_B)p_B))[s_A + H_2(ID_A)P_A]$

$= (t_B s_B)((t_A s_A)(s_A + H_2(ID_A)p_A))[s_B + H_2(ID_B)P_B]$

$= K_{BA}$

The final session key will be the output of key driven function of this shared secrets and some public/private values.

V. EFFICIENCY COMPARISON

In this section, we compare our proposed protocol with other existing two-party Authenticated Key Agreement protocols in the scope of Identity-Based PKC. As mentioned in INTRODUCTION, due to the high computational cost of Bilinear Pairings [11,18], recent Identity-Based Key Agreement protocols utilize cryptographic operations over elliptic curve based algebraic groups. As shown in TABLE I the required time for computation of ECC-based scalar multiplication is at least twenty times less than performing Bilinear Pairing operation [14]. Therefore, in this section we focus on comparison of our proposed protocol with related Pairing-free works in the area of Identity-Based two-party Authenticated Key Agreement protocols.

TABLE I. REQUIRED TIME FOR COMPUTATION OF TWO CRYPTOGRAPHIC OPERATIONS [14]

Operation	Time in milliseconds
Pairing	20.01
ECC-based scalar multiplication	0.83

TABLE II demonstrates computational costs of group operations [19]. Here, it is assumed that complexity of performing Modular Multiplication is the unit of other operations' complexity.

TABLE II. COMPUTATIONAL COSTS OF GROUP OPERATIONS[19]

Notation	Definition and Conversion
T_{MM}	Time complexity for executing the modular multiplication
T_{SM}	Time complexity for executing the elliptic curve scalar multiplication $1T_{SM} \approx 29T_{MM}$
T_{PA}	Time complexity for executing the elliptic curve point addition , $1T_{PA} \approx 0.12T_{MM}$
T_{IN}	Time complexity for executing the modular inversion operation, $1T_{IN} \approx 11.6T_{MM}$

TABLE III. EFFICIENCY COMPARISON BETWEEN OUR PROPOSED PROTOCOL AND OTHER EXISTING ONES

Authors	Exchange and Computation from A entity viewpoint	Efficiency Consideration	Computational cost unit
Cao et al. [14]	$T_A = t_A P,\ T_B = t_B P$ $K^1_{AB} = s_A\ T_B + t_A\ (R_B + h_B P_{pub})$ $K^2_{AB} = t_A\ t_B P$	4 Exponentiation (Scalar Multiplication) 1 point addition	126.12
Islam et al. [15]	$T_A = t_A(R_A + h_A P_{pub})$ $, T_B = t_B(R_B + h_B P_{pub})$ $K_{AB} = s_A[T_B + t_A(R_B + h_B P_{pub})]$	3 Exponentiation (Scalar Multiplication) 1 point addition	87.12
Our proposed Protocol	$T_A = ((t_A s_A)(s_A + H_2(ID_A)p_A))[S_B + H_2(ID_B)P_B]$ $T_B = ((t_B s_B)(s_B + H_2(ID_B)p_B))[S_A + H_2(ID_A)P_A]$ $K_{AB} = (t_A s_A)\,T_B$	2 Exponentiation (Scalar Multiplication) 2 Modular Multiplication	60

In continue to what explained above, we are going to compare our proposed protocol with two related works that have been introduced before. The proposed protocol by Cao et al. in [14] consists of four scalar multiplications and one point addition. In addition, Islam and Biswas in [15] proposed a two-party Identity-Based Key Agreement protocol which has only three scalar multiplications and one point addition. TABLE III shows the excellence of our proposed protocol in compare with the mentioned works. As shown in TABLE III, our proposed Pairing-free Key Agreement protocol is significantly more efficient since it just requires two modular multiplications, two scalar multiplications and without requiring any point addition for one of communicating users. According to the mentioned computational costs in TABLE II, overall computational complexity of the proposed protocol by Cao et al. [14] is approximately 126.12 T_{MM}, while overall computational complexity of the proposed protocol by Islam et al. [15] is approximately 87.12 T_{MM}. However, overall computational complexity our proposed protocol is approximately 60 T_{MM}, which is considerably less expensive than the related ones.

VI. CONCLUSION

In recent years, many researchers have tried to propose Pairing-free schemes in order to decrease the overall computational cost of Key Agreement protocols. Several works have been done in the field of Identity-Based Key Agreement protocols. In this paper, we propose a Pairing-free authenticated two-party Key Agreement protocol in the context of Identity-Based PKC. The results show that the proposed protocol requires less computational cost in comparison with existing related works

REFERENCES

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

[2] A. Shamir. “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. “Identity Based Encryption From The Weil Pairing”. Advances In Cryptology—Crypto. 2001.

[4] N.P. Smart. “An identity based authenticated key agreement protocol based on the Weil pairing”. Electro. Lett. 38, pp. 630–632. 2002.

[5] L. Chen, C. Kudla. “Identity based authenticated key agreement from pairings”. In: IEEE Computer Security Foundations Workshop, pp.219–233. 2003.

[6] Q. Yuan, S.A. Li. “A new efficient ID-based authenticated key agreement protocol”. Cryptology ePrint Archive, Report 2005/309. 2005.

[7] E. Ryu, E. Yoon, K.Yoo. “An efficient ID-based authenticated key agreement protocol from pairings”. In: Networking 2004, pp. 1458–1463. Springer, Heidelberg, LNCS 3042. 2004.

[8] N. McCullagh, P.S.L.M. Barreto. “A new two-party identity- based authenticated key agreement”. In: Topics in Cryptology—CT- RSA2005, pp. 262-274 Springer, Heidelberg, LNCS3376. 2005.

[9] K. Shim. “Efficient ID-based authenticated key agreement protocol based on the Weil pairing”. Electron Lett 39, pp. 653–654. 2003.

[10] Y. Wang. “Efficient Identity-Based And Authenticated Key Agreement Protocols”. Transactions On Computational Science Xvii. 2013.

[11] L. Chen, Z. Cheng, NP. Smart. “Identity-Based Key Agreement Protocols From Pairings” .International journal of information security– Springer. 2007.

[12] SM. Ghoreishi, S. Abd Razak, IF. Isnin, H. Chizari. “New Secure Identity-Based and Certificateless Authenticated Key Agreement protocols without Pairings”. In Proceedings of 2014 International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur, MALAYSIA, pp. 188-192. 2014.

[13] SM. Ghoreishi, IF. Isnin, S. Abd Razak, H. Chizari. “A novel secure two-party Identity-Based Authenticated Key Agreement protocol without Bilinear Pairings”. In Proceedings of 4th World Congress on Information and Communication Technologies (WICT), Malacca, MALAYSIA, pp. 251-258. 2014.

[14] X. Cao, W. Kou, X. Du. “A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges”, Information Sciences. 180: pp. 2895−2903. 2010.

[15] SK Hafizul Islam, G.P. Biswas. “An improved pairing-free identity-based authenticated key agreement protocol based on ECC”. Procedia Engineering, Volume 30, pp. 499-507. 2012.

[16] J. Capco. " Weil Pairings On Elliptic Curves".2003.

[17] J. Tate. "Duality Theorems In Galois Cohomology Over Number Fields", Proceedings of the international congress of mathematicians (Stockholm, 1962), Djursholm: Inst. Mittag-Leffler. 1963.

[18] F. Zhang, R. Safavi-Naini, W. Susilo. “An efficient signature scheme from bilinear pairings and its applications”. In Proceedings of PKC 2004.

[19] S.H. Islam, G.P. Biswas. “A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks”, Ann. Telecommun., 67 (11–12) , pp. 547–558. 2012.