Efficient Certificateless One-Pass Key Agreement Protocols

Yasmine Abouelseoud

Abstract— **Key agreement is an essential component in any cryptosystem. In this paper, a new certificateless two-party key agreement protocol is proposed. The protocol involves only one pass of exchanged messages, thus saving both time and bandwidth. The protocol provides implicit authentication of the identities of the two communicating parties. This protocol is extended for three participants, which has important applications in e-commerce and auditing sessions. The security properties and the performance of the protocols are analyzed, revealing their superiority compared to other schemes in literature. This promotes their use in practical scenarios such as in mobile communications.**

Index Terms— **Certificateless Cryptosystems, Key Agreement (KA), Authentication, Bilinear Maps**

I. INTRODUCTION

Security is a major concern in communications networks. The first step is generally the establishment of a shared secret between the communicating parties. It has become common practice to agree on this secret over a public channel through the use of public key cryptography. The first known key agreement (KA) protocol is the Diffie-Hellman protocol [1]. However, this protocol is susceptible to man-in-the-middle attack as there is no means of authenticating the identities of the participants.

Authentication is achieved through the use of long-term keys. Traditionally, each entity has its own private key and the corresponding public key is computed by applying a one-way trapdoor function to the private key. Public key cryptosystems are classified into traditional public key infrastructures (PKI) with certificates, identity-based systems and certificateless systems. In a traditional PKI, each user chooses its private key uniformly at random and derives the corresponding public key. A certifying authority (CA) issues certificates for the public keys of the users to provide the link between a user's public key and its identity. The certificate includes a digital signature generated by the CA over the public key. However, the management of certificates is problematic. Identity-based cryptosystems then emerged as a practical solution to eliminate the need for certificates [2]. In ID-based cryptosystems, the user's public key is any piece of identifying information, such as its email address, and the private key is then derived from the public key by the key generation center (KGC). The problem with ID-based cryptosystems is the inherent key escrow property. Certificateless cryptosystems are public key cryptosystems where a KGC is also employed to help an entity generate its private key. Yet, it only generates a partial private key. To derive the full private key, an entity combines this partial private key with some secret piece of information. Consequently, the key escrow problem is resolved.

The majority of authenticated key agreement protocols can be classified as one-round protocols or one-pass (key transport) protocols. In one-round protocols, participants contribute an equal share to the session key and they exchange their shares. In the latter class of protocols, one of the communicating parties (the initiator) generates the session key and the other entities use their long-term keys along with some piece of information sent from the initiator to derive it. One-pass protocols are more efficient than one-round protocols from the viewpoints of bandwidth and computations. However, one-round protocols are more secure. It is also noteworthy that protocols consisting of more than one round exist, but this degrades the performance from the viewpoints of bandwidth and time.

Moreover, key agreement protocols are classified according to the number of participants. The main classes are two-party schemes, three-party (or tripartite) schemes and group key agreement protocols involving more than three parties.

Authenticated versions of the two-party Diffie-Hellman protocol, over traditional public key infrastructures, have been developed in literature. Perhaps, the MTI protocols are among the earliest one-round protocols to avoid man-in-the-middle attack [3]. The MQV protocol represents an improvement to the MTI protocols with regard to efficiency and security [4]. Just and Vaudenay in [5] presented a framework for building up multi-pass key agreement protocols from simple one-pass protocols.

The tripartite version of the Diffie-Hellman protocol is a two rounds protocol and thus it is inefficient. Joux was later able to develop a one-round three-party protocol based on bilinear maps in 2001 [6]. However, this protocol is not authenticated and thus it cannot avoid man-in-the-middle attack. Al-Riaymi and Paterson suggested four tripartite authenticated key agreement protocols over traditional PKI offering tradeoffs between efficiency and security [7]. Lin-Lin protocol is a secure tripartite scheme [8], whose security properties have been further enhanced by Lim et al. in [9].

Smart [10] proposed his two-party ID-based authenticated KA protocol based on combining the ideas of Boneh and Franklin

Manuscript received February 2014; revised May 2014. This work was supported in part by Faculty of Engineering, Alexandria University in Egypt.

Y. Abouelseoud is an associate professor of Engineering Mathematics, Faculty of Engineering, Alexandria University, Alexandria, Egypt. (corresponding author: phone: 0201003727019; e-mail: yasmine.abouelseoud@ gmail.com).

[11] with the idea of the tripartite key agreement of Joux [6]. Chen and Kudla [12] developed a more efficient scheme than Smart's protocol. Another efficient ID-based KA protocol has been developed by McCullagh and Barreto in 2005 [13]. Two one-pass authenticated key agreement protocols between two entities have been developed by Okamoto et al. for ID-based cryptosystems [14].

In 2002, Zhang et al. proposed a one round, explicitly authenticated tripartite KA protocol for establishing multiple shared session keys for ID-based cryptosystems [15]. Nalla and Reddy also presented three ID-based three-party protocols; however, their schemes are only implicitly authenticated [16]. Security enhancements then followed by introducing the use of ID-based signatures as suggested by Nalla [17] and Shim [18].

Certificateless cryptosystems have recently gained the attraction of researchers. The first certificateless authenticated KA protocol was proposed by Al-Riyami and Paterson in 2003 [19]. Other one-round certificateless KA protocols for establishing a session key between two parties include the schemes in [20, 21]. In this paper, two new authenticated key transport protocols are proposed for certificateless cryptosystems. The first protocol involves two entities, while the second one is a tripartite scheme.

The rest of the paper is organized as follows. In the next section, the basic mathematical concepts are covered and the computationally hard problems upon which the security of the proposed protocols rests are defined in Section III. Security attributes for one-pass protocols are listed in Section IV. Two related schemes are reviewed in Section V. In Section VI, the proposed two-party protocol and the tripartite protocol are presented together with their proofs of consistency. The performance and the security of the proposed protocols are analyzed in Section VII. A comparative study between the proposed two-party protocol and the schemes reviewed in Section 5 appears in Section VIII. Finally, Section IX concludes the paper.

II. MATHEMATICAL BACKGROUND

In this section, essential mathematical tools are reviewed; namely, bilinear maps and elliptic curves.

A. *Bilinear Maps*

Bilinear maps and their properties are provided in what follows. More details can be found in [22,23]. Consider two groups G_1 (additive) and G_2 (multiplicative) of the same prime order q, and P a generator for G_1. A symmetric pairing is a computable map between these two groups.

For our purpose, let e be a symmetric bilinear map $e : G_1 \times G_1 \rightarrow G_2$, which satisfies the following three properties.

1- Bilinear: if $P, Q, R \in G_1$ and $a, b \in Z_q^*$ then

$e(aP, bQ) = e(P, Q)^{ab}, e(P+Q, R) = e(P, R).e(Q, R)$

2- Non-degenerative: there exist non-trivial points $P, Q \in G_1$ both of order q such that $e(P, Q) \neq 1$.

3- Computable: if $P, Q \in G_1$ and $e(P, Q) \in G_2$, then e is efficiently computable in polynomial time.

Bilinear maps were used at first in cryptanalysis [24,25]. Subsequently, they found positive applications in the development of an efficient tripartite key agreement protocol by Joux [6] and many identity-based schemes [11,12,13].

B. *Elliptic Curves*

The only known instantiations of bilinear maps are the Weil pairing and the Tate pairing which are defined over elliptic curves [11,22,26]. The modified Weil/Tate pairing with torsion maps define symmetric bilinear maps [6]. An elliptic curve E over a finite field F_p is defined by the Weirestrass equation as given in [27]: $y^2 = x^3 + ax^2 + bx + c$ where $a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2 \neq 0$ and $x \in F_p$ with p a prime greater than 3.

It may seem that elliptic curves require double the storage needed to store elements in a finite field. However, a point over an elliptic curve is usually stored in compressed format. In compressed format, the x-coordinate is only stored together with a single bit indicating whether the positive or negative square-root of $x^3 + ax^2 + bx + c$ is the designated y-coordinate. Yet, this adds to the computational burden associated with manipulating points over elliptic curves since the square-root needs to be computed using Tonelli-Shanks algorithm [23].

III. HARD COMPUTATIONAL PROBLEMS

The security of the proposed protocols relies on the fact that the solution of the following problems is not feasible in polynomial time.

- Discrete Logarithm Problem (DLP): Given the element $k_1 = g^a \in Z_p^*$, find a.
- Diffie-Hellman Problem (DHP): Given the two elements $k_1 = g^a \in Z_p^*$ and $k_2 = g^b \in Z_p^*$, compute $g^{ab} \bmod p$.

Similar definitions could be provided for elliptic curves groups. It is noteworthy that the DLP over elliptic curves is more difficult than that for finite fields. This allows the use of keys of smaller size in the order of 160 bits instead of 256-bit keys used for cryptosystems defined over traditional finite fields.

Bilinear Diffie-Hellman Problem (BDHP): Given the tuple (P,aP,bP,cP), compute $e(P, P)^{abc}$.

IV. SECURITY ATTRIBUTES OF A ONE-PASS KEY AGREEMENT PROTOCOL

The attributes used to assess the security of a one-pass key agreement protocol are summarized below [14,28].

Known-Key Security: Each run of the key agreement protocol should result in a unique session key so that the compromise of a previous session key does not compromise other session keys.

Sender's Key Compromise Impersonation: If an adversary is in possession of the sender's long-term private key, it can surely impersonate A, but it should not be able to impersonate other entities in the presence of A. In a one-pass key agreement protocol, it is clear that if the receiver's long-term private key is compromised, then the adversary can impersonate any entity to B if the ephemeral secret of the initiator is not explicitly authenticated.

Sender's Forward Secrecy: It is the property that refers to the inability of an adversary with access to the private key of a sender to compromise the secrecy of previously established session key(s) of the sender. Sender's forward secrecy is weaker than the standard notion of (partial) forward security for one round authenticated key agreement protocols [29].

No Key Control: No party can force the key to a pre-specified value.

V. Related Work

Two recent one-pass certificateless key agreement protocols [28,30] are reviewed in this section. They are later used in our comparative study that appears in Section VIII.

A. Setup and Long-term Keys Generation

The two schemes have quite similar setup and long-term keys generation algorithms, which are described below.

Setup: Let G_1 be a cyclic additive group generated by P, whose order is a prime q, G_2 be a cyclic multiplicative group of the same order q, and $e: G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing. This algorithm runs as follows:

1. Choose a random master-key $s \in Z_q^*$ and set $P_{pub} = sP$.
2. Choose cryptographic hash functions including $H_1 : \{0,1\}^* \rightarrow G_1$.

Partial-Private-Key-Extract: This algorithm accepts an identity $ID_i \in \{0,1\}^*$ and generates the partial private key for the user as follows.

1. Compute $Q_i = H_1(ID_i)$.
2. Output the partial private key $D_i = s\, Q_i$.

Set-Secret-Value: This algorithm takes as input the public system parameters and a user's identity ID_i, and selects a random integer $x_i \in Z_q^*$. It outputs x_i as the user's secret value.

Set-Private-Key: This algorithm takes as input the system public parameters, a user's partial private key D_i and the user's secret value x_i. The output of the algorithm is the private key $S_i = (x_i, D_i)$.

Set-Public-Key: This algorithm accepts the system-wide parameters and a user's secret value x_i to produce the user's public key $P_i = x_iP$.
Assume the sender A has the private key $S_A = (x_A, D_A)$ and the public key $P_A = x_AP$. The receiver B has the private key $S_B = (x_B, D_B)$ and the public key $P_B = x_BP$.

B. Chen's et al. Session Key Agreement Module

The protocol runs as follows [30]:

1. A picks a random number $r \in Z_q^*$ and computes $U = r\, Q_A$ and sends U to B.
2. Then, A and B can establish their session key as follows:
   a. A first computes $h = H_2(U)$ and $Q_B = H_1(ID_B)$, then computes $K_{AB} = H_3(ID_A, ID_B, P_A, P_B, U, r\, P_B, \alpha)$, where H_2 and H_3 are cryptographic hash functions and $\alpha =$ $(e(D_A, Q_B)e(Q_A, P_B)^{\,x_A})^{r+h}$).
   b. B first computes $h = H_2(U)$ and $Q_A = H_1(ID_A)$, then computes $K_{BA} = H_3(ID_A, ID_B, P_A, P_B, U,$ x_B $U, \beta)$, where $\beta = e(U + h\, Q_A ,\ x_B\, P_A + D_B)$.

C. Zhang's et al. Session Key Agreement Algorithm

In this scheme, the sender (A) and the receiver (B) proceed as follows [28]:

1. A picks a random number $r \in Z_q^*$ and computes $U = r\, Q_A$ and sends (ID_A, P_A , U) to B.
2. A and B can establish their shared session key as follows:
   a. A computes $K_{AB} = H_2(ID_A, ID_B, P_A, P_B, U,\ rP_B, x_AP_B, e(D_A , Q_B), e(P_{pub}, Q_B)^r)$, where H_2 is a cryptographic hash function.
   b. B computes $K_{BA} = H_2(ID_A, ID_B, P_A, P_B, U,\ x_BU, x_BP_A, e(Q_A , D_B), e(U, D_B))$.

VI. The Proposed Key Agreement Protocols

In this section, a new tripartite key transport protocol is developed. First, the basic protocol between two parties is presented and then it is extended to three parties building on the idea of Joux's protocol [6].The protocol consists of three modules: the setup, the long-term keys generation, and the session key generation.

A. System Setup

On input a security parameter ℓ_1, this algorithm is responsible for the generation of the system-wide public parameters including an elliptic curve E over Z_p where p is a large prime number, a generator point P of a subgroup of points on $E(Z_p)$ of prime order q denoted as G_1, and a suitable bilinear map $e: G_1 \times G_1 \rightarrow G_2$ such as the modified Weil/Tate pairing is chosen, where G_2 is a finite field extension of Z_p. The key generation center (KGC) also selects a secret master key $s \in Z_q^*$ and computes the corresponding master public key $P_{pub} = sP \bmod p$. Finally, two one-way cryptographic hash functions are selected: $H_1 : \{0,1\}^* \times G_1 \times G_1 \rightarrow Z_q^*$ and $H_2 : \{0,1\}^* \times G_1 \times G_1 \rightarrow \{0,1\}^{\ell 2}$ where ℓ_2 is another security parameter.

B. Long-term Keys Generation

Each user who wishes to join the system randomly chooses an integer $x_i \in Z_q^*$ and computes the corresponding public key $Y_i = x_i\ P \bmod p$. It then submits its identifying information (ID$_i$) as well as its public key to the KGC who then sends the partial secret key $s_i = r_i + h_i\ s \bmod q$ through a secure channel, where $h_i = H_1(ID_i, Y_i, R_i = r_i P)$. The user accepts its partial private key if the following equation holds: $s_i P = R_i + h_i\ P_{pub}$. The private key of a user consists of the pair (x_i, s_i) and the corresponding public key pair is (Y_i, R_i) [31].

C. Basic Two-Party Session Key Generation

First, a one-pass key agreement protocol for establishing a shared key between two parties is described. The sender (A) proceeds as follows.

1. Entity A chooses a random integer $a \in Z_q^*$.
2. It computes $T_A = a\ P \bmod p$.
3. It computes $h_B = H_1(ID_B, Y_B, R_B)$
4. It computes the session key
   $K_{AB} = (a + s_A)(R_B + h_B P_{pub}) + x_A Y_B$
5. It sends the tuple $(ID_A, T_A, h = H_2(ID_A, T_A, K_{AB}))$ to entity B.

The receiver (B) proceeds as follows.

1. It computes the session key as
   $$K_{BA} = s_B(T_A + R_A + h_A P_{pub}) + x_B Y_A$$
2. It verifies whether $h = ?\, H_2(ID_A, T_A, K_{BA})$

The correctness of this protocol is justified below. It is shown that $K_{BA} = K_{AB}$.

$$\begin{aligned} K_{BA} &= s_B(T_A + R_A + h_A P_{pub}) + x_B Y_A \\ &= s_B(T_A + s_A P) + x_A x_B P \\ &= s_B(a + s_A)P + x_A Y_B \\ &= (a + s_A)(R_B + h_B P_{pub}) + x_A Y_B = K_{AB} \end{aligned}$$

D. Tripartite Session Key Generation

The above scheme is extended to three-parties as demonstrated below. The initiator (A) of the protocol carries out the following steps.

1. A random integer $a \in Z_q^*$ is chosen.
2. It computes $T_A = a\ P \bmod p$.
3. The session key is computed as
   $$K_A = e(R_B + h_B P_{pub}, R_C + h_C P_{pub})^{(a+s_A)} .e(Y_B, Y_C)^{x_A}$$
   where $h_B = H_1(ID_B, Y_B, R_B)$ and $h_C = H_1(ID_C, Y_C, R_C)$)
4. It sends the tuple $(ID_A, T_A, h = H_2(ID_A, T_A, K_A))$ to both receivers (B and C) through a broadcast channel.

The receiver (B) proceeds as follows.

1. It computes the session key as
   $$K_B = e(R_A + T_A + h_A P_{pub}, R_C + h_C P_{pub})^{s_B} .e(Y_A, Y_C)^{x_B}$$
2. It verifies whether $h = ?\, H_2(ID_A, T_A, K_B)$.

Similar steps are carried out by the other recipient(C).

The consistency of the proposed scheme lies in proving the correctness of the key recovery equation used by the receivers. The proof is provided below for entity B and similar arguments hold for entity C since the roles of B and C are symmetric in this protocol.

$$\begin{aligned} K_B &= e(R_A + T_A + h_A P_{pub}, R_C + h_C P_{pub})^{s_B} .e(Y_A, Y_C)^{x_B} \\ &= e(T_A + s_A P, R_C + h_C P_{pub})^{s_B} .e(x_A P, Y_C)^{x_B} \\ &= e(aP + s_A P, R_C + h_C P_{pub})^{s_B} .e(x_B P, Y_C)^{x_A} \\ &= e(s_B P, R_C + h_C P_{pub})^{(a+s_A)} .e(Y_B, Y_C)^{x_A} = K_A \end{aligned}$$

VII. Performance Analysis and Security Analysis

In this section, the performance of the two proposed protocols is analyzed and the security attributes are examined.

A. Computational Burden

On the sender's side, the two-party scheme involves four scalar point multiplications, two point additions over an elliptic curve and two hashing operations. As for the receiver, it performs three scalar point multiplications, three point additions and two hashing operations. For frequently communicating users, with enough secure storage, savings could be achieved. The values of $x_A Y_B$ and $s_B P$ can be pre-computed and stored on the sender's side, while the receiver pre-computes the values of $x_B Y_A$ and $s_A P$ and stores them. Additionally, h_B and h_A can also be pre-computed and thus reducing the number of hashing operations.

In the tripartite scheme, the sender performs three scalar point multiplications, two pairing evaluations, two point additions, two exponentiations in G_2 and three hashing operations. On the receiver's side, the scheme involves two pairing evaluations, three point additions, two exponentiations in G_2 and three hashing operations. Similar savings in computations can be achieved as those described for the two-party scheme for frequently communicating parties using pre-computed stored values.

B. Security Properties

In what follows, the security arguments for the two-party scheme are provided.

Known-Key Security: The knowledge of a previous session key does not compromise the security of other session keys because each protocol run involves choosing a random number (a). Thus, knowing $T_A = a\,P$ and $K_A = (a + s_A)\, s_B\, P + x_A Y_B$, it is computationally infeasible to compute a new key $K'_A = (a' + s_A)\, s_B\, P + x_A Y_B$ without the knowledge of s_A according to the Diffie-Hellman assumption.

Sender's Key Compromise Impersonation: If the sender's long-term secret key is compromised, the adversary in possession of this key will not be able to impersonate a receiver B to A. This is because it cannot compute the session key without the knowledge of the short-term key (a). However, if the adversary is the initiator in another run, it can impersonate B (the sender) to A (the receiver) as demonstrated below.

$$T_B = b\,P,\;\; K_B = (b + s_A)\,(R_B + h_B P_{pub}) + x_A Y_B$$

Sender's Forward Secrecy: If the initiator's long-term private key is compromised, the session keys in previous runs of the protocol remain secret as the key computation also involves a short-term (ephemeral) key; that is, the random number (a).

No Key Control: Though entity A is the only one contributing to the session key calculation, yet it cannot force it to a pre-specified value since this would involve the solution of instances of the discrete logarithm problem. Moreover, the final value of the key may be derived through a suitable one-way hash function.

Similar security arguments hold for the tripartite scheme.

VIII. A Comparative Study

In this section, the performance and security properties of the proposed two-party protocol are compared to other recent one-pass key agreement protocols in literature.

The performance is measured in terms of the computations involved in the session key generation phase. It is assumed that the parties communicate frequently with enough secure storage available to them in Table I. The following abbreviations are used in Table I and Table II.

PA: pairings evaluated by A,
PB: pairings evaluated by B,
SA: scalar point multiplications by A,
SB: scalar point multiplications by B,
EA: exponentiations in G_2 by A.

TABLE I. A COMPARISON OF COMPUTATIONAL LOAD WITH PRE-COMPUTATIONS

Operation Scheme	PA	PB	SA	SB	EA
Proposed	0	0	2	1	0
Zhang [28]	0	1	2	1	1
Chen [30]	0	1	2	2	2

In Table II, the computations needed without pre-computations are provided.

TABLE II. PERFORMANCE EVALUATED WITHOUT PRE-COMPUTATIONS

Operation Scheme	PA	PB	SA	SB	EA
Proposed	0	0	4	3	0
Zhang [28]	2	2	3	2	1
Chen [30]	2	1	2	2	2

It is clear from the above tables that the proposed protocol outperforms the other two schemes. It is noteworthy that the proposed protocol additionally provides the same level of security as the other two schemes and additionally provides key confirmation. Thus, the proposed scheme is more preferred in practical scenarios.

IX. Conclusions

Certificateless one-pass key agreement protocols are known for their efficiency compared to other categories of key agreement protocols. Consequently, this class of key agreement protocols attracted the attention of many researchers. In this paper, a new two-party protocol and a new tripartite protocol, which belong to this class, have been proposed. The security analysis of the protocols revealed that they satisfy the standard security requirements for a one-pass key agreement protocol. The proposed two-party protocol is superior to other protocols in literature from the computational viewpoint as demonstrated in the comparative study presented above. Moreover, the proposed protocol easily lent itself to being extended for three parties which finds applications in e-commerce, where the three entities are the customer, the merchant and the bank.

Certificateless protocols avoid the difficulties associated with certificates management that exist in traditional public key infrastructures (PKI). Additionally, the signature verification step is no longer needed. This step is implicitly included in any certificate-based scheme. The proposed protocols should be used in scenarios, where one (or two) of the communicating parties (to act as the receiver(s)) is a highly-secure end. Actually, this is almost the case in applications such as mobile communications, authorized access to databases and in e-commerce transactions.

References

[1] W. Diffie & M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22(6), pp. 644-654, 1976.

[2] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", In Advances in Cryptology- CRYPTO 1984, LNCS 0196, Springer-Verlag, 1984.

[3] T. Matsumoto, Y. Takashima and H. Imai, "On Seeking Smart Public-key Distribution Systems", In Transactions of the IECE of Japan, E69, pp. 99-106, 1986.

[4] A. Menezes, M. Qu and S. Vanstone, "Some New Key Agreement protocols providing implicit authentication", Workshop on Selected Areas in Cryptography (SAC'95), 1995, pp. 22-32.

[5] M. Just and S. Vaudenay, "Authenticated Multi-party Key Agreement", In Proceedings of Advances in Cryptology, Eurocrypt'96, 1996.

[6] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman", In Proceedings of the Fourth Algorithmic Number Theory Symposium, LNCS 1838, pp. 385-394, Springer-Verlag, 2000.

[7] Sattam S. Al-Riyami and Kenneth G. Paterson, "Authenticated Three Party Key Agreement Protocols from Pairings", Cryptology ePrint Archive, Report 2002/035, 2002.

[8] Lin, Chu-Hsing and Hsiu-Hsia Lin, "Secure One-round Tripartite Authenticated Key Agreement Protocol from Weil Pairing", In Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA 2005), 2005.

[9] Lim, M., S. Lee, Y. Park and H. Lee, "An Enhanced One-Round Pairing-based Tripartite Authenticated Key Agreement Protocol", Computational Science and its Applications, ICCSA 2007, LNCS 4706: 503-513, 2007.

[10] N. P. Smart, "An Identity-based Authenticated Key Agreement Protocol Based on the Weil Pairing", In Electronic Letters, 38, pp. 630-632, 2002. Also available at http://www.iacr.org/2001/111.

[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing", In Advances in Cryptology- CRYPTO 2001, LNCS 2139, Springer, 2001.

[12] L. Chen and C. Kudla, "Identity Based Authenticated Key Agreement Protocols from Pairings", Cryptology ePrint Archive, Available at http://eprint.iacr.org/2002/184, 2002.

[13] N. McCullagh and P. S. L. M. Barreto, "A New Two-Party Identity-Based Authenticated Key Agreement", In Proceedings of CT-RSA 2005, LNCS 3376, pp. 262-274, Springer-Verlag, 2005. Also available at http://eprint.iacr.org/2004/122.

[14] T. Okamoto, R. Tso and E. Okamoto, "One-Way and Two-Party Authenticated ID-Based Key Agreement Protocols Using Pairing", Modeling Decisions for Artificial Intelligence, LNCS 3558, pp. 122-133, 2005.

[15] F. Zhang, S. Liu, K. Kim, "ID-based oneround authenticated tripartite key agreement protocol with pairings", Cryptology ePrint Archive, Report 2002/122, 2002.

[16] D. Nalla and K. C. Reddy, "ID-Based Tripartite Authenticated Key Agreement Protocols from Pairings", Cryptology ePrint Archive, Available at http://eprint.iacr.org/2003/004, 2003.

[17] D. Nalla, "ID-based tripartite key agreement with signatures", Cryptology ePrintArchive, Report 2003/144, 2003.

[18] K. Shim, "Cryptanalysis of ID-based Tripartite Authenticated Key Agreement Protocols", Cryptology ePrint Archive, Report 2003/115, 2003.

[19] S. Al-Riyami and K. Paterson, Certificateless public key cryptography, Asiacrypt-2003, Lecture Notes in Computer Science, vol. 2894, pp. 452-473, Springer-Verlag, 2003.

[20] C. M. Swanson, Security in key agreement: Two-party certificateless schemes, Master's thesis, University of Waterloo, 2008. http://hdl.handle.net/10012/4156.

[21] G. Lippold, C. Boyd, and J. Gonz´alez Nieto, "Strongly secure Certificateless Key Agreement", In Pairing '09: Proceedings of the 3rd International Conference on Pairing-Based Cryptography, volume 5671 of Lecture Notes in Computer Science, pp. 206–230, Berlin-Heidelberg, Springer-Verlag, 2009.

[22] A. Joux, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems", In Proceedings of the Fifth Algorithmic Number Theory Symposium, LNCS, Springer-Verlag, 2002.

[23] B. Lynn, On the Implementation of Pairing-Based Cryptosystems, PhD thesis, Stanford University, 2007.

[24] A. Menezes, T. Okamoto and S. Vanstone, "Reducing Elliptic Curve Logarithm to Logarithms in a Finite Field", IEEE Transactions on Information Theory, vol. 39, pp. 1639-1646, 1993.

[25] G. Frey and H. Ruck, "A Remark Concerning *m*-divisibility and the Discrete Logarithm Problem in the Divisor Class Group of Curves", Mathematics of Computation, vol. 62, pp. 865-874, 1994.

[26] V. Miller, The Weil Pairing and Its Efficient Calculation, Journal of Cryptology, vol. 17(4), pp. 235-262, 2004.

[27] N. Koblitz, A. Menezes and S. Vanstone, The State of Elliptic Curve Cryptography, In Designs, Codes and Cryptography, vol. 19, pp. 173-193, Kluwer Academic Publishers, Boston, 2000.

[28] L. Zhang, "Provably Secure Certificateless One-Way and Two-Party Authenticated Key Agreement Protocol", ICISC 2012, LNCS vol. 7839, pp. 217-230, Springer-Verlag, 2013.

[29] Blake-Wilson, S., D. Johnson & A. Menezes, "Key Agreement Protocols and their Security Analysis", Proceedings of the 6th IMA International Conference on Cryptography and Coding. LNCS vol. (1355): 30-45. Springer, UK, 1997.

[30] W. Chen et al., "Certificateless One-Way Authenticated Two-Party Key Agreement Protocol", Proceedings of 2009 Fifth International Conference on Information Assurance and Security, IEEE Computer society, pp. 483-486, 2009.

[31] M. Geng and F. Zhang, "Provably Secure Certificateless Two-Party Authenticated Key Agreement Protocol Without Pairing", In International Conference on Computational Intelligence and Security, pages 208-212, 2009.