ISSN 1392–124X (print), ISSN 2335–884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2016, T. 45, Nr. 1

Secure Certificateless Two-Party Key Agreement with Short Message

Han-Yu Lin

Department of Computer Science and Engineering, National Taiwan Ocean University,
Keelung, 202, Taiwan
e-mail: lin.hanyu@msa.hinet.net

crossref http://dx.doi.org/10.5755/j01.itc.45.1.12595

Abstract. Two-party key agreement protocol allows two communication parties to share a common key for secure communication. Constructed from the certificateless public key cryptography (CL-PKC), a certificateless key agreement (CL-KA) protocol can not only solve the key escrow problem inherited from identity-based systems, but also avoid the troublesome issue of certificate management. Although the topic of two-party CL-KA has been extensively studied during past few years, it is unknown whether such a protocol can be achieved with only one exchanged message. In this paper, we put this idea into practice and propose a new one-round CL-KA for two-party. Specifically, each party of the proposed protocol only has to transmit one group element for sharing a session key and still maintains low computational costs. Moreover, we analyze the security of our scheme in the extended Canetti-Krawzcyk (eCK) security model.

Keywords: two-party; certificateless; key agreement; eCK security model; public key system.

1. Introduction

In public communication networks such as the Internet, transmitted messages can be easily intercepted or eavesdropped by any malicious adversary. To protect the confidentiality of network communication, two communication parties can first agree on a common session key and then use it for subsequent encryption/decryption. Without the knowledge of this shared session key, no one can learn the information of transmitted messages. The procedure for generating the shared session key is thus referred to as the key exchange or key agreement protocols.

In 1976, Diffie and Hellman [3] introduced the first public key system for solving the key exchange problem. In this system, each user owns a self-chosen private key and a corresponding public one. The former is kept secret by the user while the latter is publicly accessible to anyone. Based on the intractability of discrete logarithm problems (DLP), it is computationally infeasible for any third party to derive the session key from intercepted messages. However, the Diffie-Hellman key exchange protocol is vulnerable to the man-in-the-middle attack [15, 16], and the authenticity of obtained public keys has to be verified with the assistance of additional certificate.

In 1984, Shamir [13] came up with the famous identity-based system in which the public key of each user is straightly his public identifier and the related private key is computed by the system authority (SA) with a trapdoor function. Without this trapdoor secret, no one can derive any user's private key from his public one. It is obvious that such a system has the drawback of key escrow and the SA must be trusted.

In 2003, Al-Riyami and Paterson [1] introduced the certificateless public key cryptography (CL-PKC) in which the key generation center (KGC) only has limited control over users' private keys. Meanwhile, the authenticity of public keys can be guaranteed without additional public key certificate. Based on CL-PKC, in 2006, Mandt [10, 11] proposed certificateless key agreement (CL-KA) protocols for two-party. He also showed that his protocol could be utilized for generating keys between members of distinct domains. Later, Wang et al. [21] and Shi and Li [14] separately proposed more efficient CL-KA protocols. In 2008, Xia *et al.* [22] pointed out that Mandt's scheme could not satisfy the security requirement of key-compromise impersonation (KCI) resilience and further proposed an improved protocol.

In 2009, Swanson and Jao [18] analyzed the security of previous CL-KA protocols and showed that Wang *et al.'s* scheme [21] is vulnerable to the KCI attack and the Shi-Li protocol [14] could not withstand the man-in-the-middle attack. Besides, they introduced the first formal security model for two-party CL-KA protocols. Their model was based on the extended Canetti-Krawczyk (eCK) model [6] for traditional authenticated key exchange.

In the same year, Lippold *et al.* [7] addressed the first provably secure one-round CL-KA protocol. They claimed that as long as each party still has one uncompromised secret, the confidentiality of shared session key can be ensured. That is, even if a malicious KGC knows the ephemeral secrets of both communication parties, it is unable to derive the information of shared session key.

To improve the computational efficiency of Lippold *et al.*'s protocol, in 2010, Liu *et al.* [8] proposed a new CL-KA protocol and also analyzed the security of their work in the eCK model. In 2011, Mokhtarnameh *et al.* [12] employed an alternative key generation technique to propose an enhanced CL-KA protocol. Considering group-oriented applications, some researchers [4, 9, 19] are also devoted to the design of certificateless group key agreement (CL-GKA) protocols.

In this paper, we focus on the two-party CL-KA protocol and will address a new construction. As all of existing related mechanisms require each party to send more than one message for computing a session key, we will present an alternative protocol to prove the feasibility of utilizing only one exchanged message. Further, we will also show that the proposed protocol exhibits all necessary security attributes in the eCK model.

2. Preliminaries

In this section, we state the computational assumptions along with the security requirements and definitions of our CL-KA protocol.

2.1. Computational Assumptions

Bilinear Pairing [20]

Let ($\boldsymbol{G}_1$, +) and ($\boldsymbol{G}_2$, ×) separately be an additive and a multiplicative group of the same prime order q and P an arbitrarily generator of $\boldsymbol{G}_1$. The notation of "aP" expresses that P added to itself a times. A mapping e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ is a cryptographic bilinear map which satisfies the following properties:

(i) ***Bilinearity:***

For all $P, Q, R \in \boldsymbol{G}_1$ and some $a, b \in Z_q^*$, we have

$e(aP, bQ) = e(P, Q)^{ab}$;

$e(P + R, Q) = e(P, Q)e(R, Q)$;

$e(P, R + Q) = e(P, R)e(P, Q)$;

(ii) ***Non-degeneracy:***

If P is a generator of $\boldsymbol{G}_1$, then $e(P, P)$ is a generator of $\boldsymbol{G}_2$, which also implies $e(P, P) \neq 1$.

(iii) ***Computability:***

Given P, $Q \in \boldsymbol{G}_1$, the value of $e(P, Q)$ can be efficiently computed by a polynomial-time algorithm.

Elliptic Curve Discrete Logarithm Problem; ECDLP

The ECDLP is, given an instance $(P, A) \in \boldsymbol{G}_1^2$ where P is a generator and $A = aP$ for some $a \in Z_q^*$, to compute a.

Elliptic Curve Discrete Logarithm (ECDL) Assumption

For every probabilistic polynomial-time algorithm A, every positive polynomial $Q(\cdot)$ and all sufficiently large k, the algorithm A can solve the ECDLP with the advantage at most $1/Q(k)$, i.e.,

$\Pr[A(P, aP) = a; a \leftarrow Z_q, (P, aP) \leftarrow \boldsymbol{G}_1^2] \leq 1/Q(k)$.

The probability is taken over the uniformly and independently chosen instance and over the random choices of A.

Definition 1. *The (t, ε)-ECDL assumption holds if there is no polynomial-time adversary that can solve the ECDLP in time at most t and with the advantage ε.*

Bilinear Diffie-Hellman Problem; BDHP

The BDHP is, given an instance $(P, A, B, C) \in \boldsymbol{G}_1^4$ where P is a generator, $A = aP$, $B = bP$ and $C = cP$ for some $a, b, c \in Z_q$, to compute $e(P, P)^{abc} \in \boldsymbol{G}_2$.

Bilinear Diffie-Hellman (BDH) Assumption

For every probabilistic polynomial-time algorithm A, every positive polynomial $Q(\cdot)$ and all sufficiently large k, the algorithm A can solve the BDHP with the advantage at most $1/Q(k)$, i.e.,

$\Pr[A(P, aP, bP, cP) = e(P, P)^{abc}; a, b, c \leftarrow Z_q, (P, aP, bP, cP) \leftarrow \boldsymbol{G}_1^4] \leq 1/Q(k)$.

The probability is taken over the uniformly and independently chosen instance and over the random choices of A.

Definition 2. *The (t, ε)-BDH assumption holds if there is no polynomial-time adversary that can solve the BDHP in time at most t and with the advantage ε.*

2.2. Security Requirements

A secure key agreement protocol should satisfy the following security requirements [2]:

(i) ***Known-key secrecy:*** The unique session key generated in one round should be independent with those created in other rounds, which also means that the compromise of the latter cannot affect the security of the former.

(ii) ***Forward secrecy:*** In case that the private key of some party is compromised, the confidentiality of previously constructed session keys is still fulfilled.

(iii) ***Perfect forward secrecy:*** Even if the private keys of all parties are compromised, the security of previously generated session keys is unaffected.

(iv) ***KGC forward secrecy:*** The exposure of KGC's master secret key cannot endanger the security of previously created session keys.

(v) ***Key-compromise impersonation (KCI) resilience:*** Any adversary should not be able to impersonate a legitimate user to share a session key with another one whose private key is compromised.

(vi) ***Unknown key-share resilience:*** When the party A is sharing a session key with another party B, he won't misthink that the key is shared with the party C.

(vii) ***No key control:*** Each session key should be cooperatively determined by both the communication parties, rather than anyone solely.

(viii) ***Known session-specific temporary information security:*** The exposure of random numbers utilized in one round cannot affect the security of shared session key.

2.3. Security Definitions

In 2009, Swanson [17] addressed the security model for CL-KA protocol by modifying the eCK model. Then Lippold *et al.* [7] further presented an extension of Swanson's security model. Generally speaking, in a certificateless scheme, each party owns three secrets including (1).the partial private key issued by the KGC, (2).a self-chosen private key and (3).the ephemeral secrets utilized in each session. In our security model, the adversary is allowed to reveal at most two secrets, i.e., each party still keeps one uncompromised secret. We will show that even with such a stronger adversary, the proposed CL-KA protocol still achieves the level of security below.

Definition 3. *(Type I secure CL-KA protocol). A CL-KA protocol is Type I secure if there is no probabilistic polynomial-time adversary that can derive the session key with non-negligible advantage after revealing at most two secrets of each party.*

Definition 4. *(Type II secure CL-KA protocol). A CL-KA protocol is Type II secure if there is no probabilistic polynomial-time adversary that can derive the session key with non-negligible advantage after revealing the master secret key of KGC and one additional secret of each party.*

3. The Proposed CL-KA Protocol

In this section, we present our CL-KA protocol. The proposed scheme is composed of five phases including Setup, Partial private key extraction, Keygen, Message exchange and Key computation. Details of each phase are described as follows:

- ***Setup***

Taking as input 1^k, the KGC selects two groups $(\boldsymbol{G}_1, +)$ and $(\boldsymbol{G}_2, \times)$ of the same prime order q. Let P be a generator of order q over $\boldsymbol{G}_1$, e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ a bilinear pairing and H_1: $\{0, 1\}^* \rightarrow \boldsymbol{G}_1$ and H_2: $\{0, 1\}^* \times \{0, 1\}^* \times \boldsymbol{G}_1^{\ 2} \times \boldsymbol{G}_2^{\ 3} \times \boldsymbol{G}_1 \rightarrow \{0, 1\}^n$ for some integer $n > 0$, collision resistant hash functions. The system publishes public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, q, P, e, H_1, H_2\}$. The master secret key (msk) of KGC is s and the corresponding public key is computed as $P_{KGC} = sP$.

- ***Partial private key extraction***

Taking as input msk, $params$, and a user identity $ID \in \{0, 1\}^*$, the KGC computes the partial private key for ID as

$$D_{ID} = sH_1(ID), \qquad (1)$$

and then returns it to the user via a secure channel.

- ***Keygen***

Each user chooses a random numbers $x_{ID} \in Z_p^{\ *}$, sets his private key as (D_{ID}, x_{ID}) and computes the public key as

$$Y_{ID} = x_{ID}P. \qquad (2)$$

- ***Message exchange***

Let users A and B attempt to create a shared common key. They first choose $r_a, r_b \in_R Z_p^{\ *}$, respectively, and exchange the following messages:

$$A \rightarrow B{:}\ E_A = r_aY_a, \qquad (3)$$

$$B \rightarrow A{:}\ E_B = r_bY_b. \qquad (4)$$

- ***Key computation***

Upon receiving the exchanged message, they can compute

$$K_1 = e(H_1(ID_B), P_{KGC})^{x_a r_a} = e(D_B, E_A), \qquad (5)$$

$$K_2 = e(D_A, E_B) = e(H_1(ID_A), P_{KGC})^{x_b r_b}, \qquad (6)$$

$$K_3 = e(D_A, H_1(ID_B)) = e(H_1(ID_A), D_B), \qquad (7)$$

$$K_4 = r_a x_a E_B = r_b x_b E_A = r_a x_a r_b x_b P, \qquad (8)$$

$$K = H_2(ID_A, ID_B, E_A, E_B, K_1, K_2, K_3, K_4). \qquad (9)$$

Here, K is the constructed secret key for both A and B. In Eq. (9), the hash function of H_2 takes as inputs eight parameters. The first two parameters (ID_A, ID_B) stand for the identities of communicated parties. (E_A, E_B) are the exchanged messages for both parties in current session. (K_1, K_2, K_3, K_4) are used to withstand types I and II adversaries.

4. Security Analysis and Comparison

We show that the proposed scheme satisfies all the security requirements stated in Section 2.2 along with the security definitions mentioned in Section 2.3.

Additionally, the performance evaluation with previous protocols is also made.

(i) ***Known-key secrecy:*** In the message exchange phase of our protocol, each party has to choose a random number for sharing a common key. Therefore, the created session key is unique and the exposure of previous session keys will not compromise the one of current session.

(ii) ***Perfect forward secrecy:*** Since each session key is incorporated with two random numbers, any adversary who even knows the private keys of both communication parties still faces the difficulty of ECDLP to derive the session key.

(iii) ***KGC forward secrecy:*** If an adversary has the knowledge of KGC's master secret key, he can derive the partial private key of each party. However, he cannot utilize it to compute the private key of each user. Consequently, the confidentiality of session keys will not be compromised.

(iv) ***Key-compromise impersonation resilience:*** Assume that an adversary having the private key x_a of Alice attempts to impersonate Bob for sharing a common key with Alice. Nevertheless, he still lacks (x_b, D_A) for computing valid (K_2, K_3).

(v) ***Unknown key-share resilience:*** As the identities of communication parties and the exchanged messages are also included in the session key, each party can confirm that only the intended subject can derive the shared session key.

(vi) ***No key control:*** It can be seen that each session key is cooperatively determined by the random numbers, the short-term and long-term private keys of both parties. Hence, the requirement of no key control is satisfied in the proposed protocol.

(vii) ***Known session-specific temporary information security:*** Even if the chosen random numbers are compromised, any adversary cannot successfully derive the shared session key without knowing the private keys of communication parties.

Theorem 1. *The CL-KA protocol is Type I secure.*

Proof: Assume that an adversary A is able to compromise at most two secrets for each communication party in the proposed scheme. We show that even if there is such an adversary, the shared session key of our protocol will not be compromised in the following cases:

Case 1. If the adversary A gets (r_a, x_a, r_b, x_b), i.e, users A and B separately keep D_A and D_B, he will face the BDHP to compute $K_3 = e(D_A, H_1(ID_B))$.

Case 2. If the adversary A obtains (D_A, x_a, r_b, x_b) or (D_A, r_a, r_b, x_b), i.e, users A and B separately keep (r_a, D_B) or (x_a, D_B), he cannot compute $K_1 = e(D_B, E_A)$ and $K_4 = r_a x_a r_b x_b P$ due to the intractability of both the BDHP and ECDLP.

Case 3. If the adversary A learns (r_a, x_a, D_B, x_b) or (r_a, x_a, D_B, r_b), i.e, users A and B separately keep (D_A, r_b) or (D_A, x_b), he also faces both the BDHP and ECDLP to compute $K_2 = e(D_A, E_B)$ and $K_4 = r_a x_a r_b x_b P$.

Case 4. If the adversary A has the knowledge of (D_A, r_a, D_B, x_b) or (D_A, x_a, D_B, r_b), i.e, users A and B separately keep (x_a, r_b) or (r_a, x_b), he must solve the ECDLP for deriving $K_4 = r_a x_a r_b x_b P$.

Case 5. If the adversary A obtains (D_A, r_a, D_B, r_b) or (D_A, x_a, D_B, x_b), i.e, users A and B separately keep (x_a, x_b) or (r_a, r_b), he also unable to compute $K_4 = r_a x_a r_b x_b P$ without solving the ECDLP.

Theorem 2. *The proposed CL-KA protocol is Type II secure.*

Proof: Assume that a malicious KGC is able to compromise one additional secret for each communication party in the proposed scheme. We show that even if there is such a malicious KGC, the shared session key of our protocol will not be compromised in the following cases:

Case 1. If the KGC obtains (r_a, x_b) or (x_a, r_b), he will face the ECDLP to derive $K_4 = r_a x_a r_b x_b P$.

Case 2. Similarly, if the KGC learns (r_a, r_b) or (x_a, x_b), he also cannot derive $K_4 = r_a x_a r_b x_b P$ under the protection of ECDLP.

To evaluate the performance of our protocol, we compare the proposed scheme with previous related works including Lippold *et al.*'s (LBN for short) [7], Liu *et al.*'s (LXX for short) [8] and Mokhtarnameh *et al.*'s (MHM for short) [12] protocols. For facilitating the following comparison, some used notations are defined below:

B: the time for computing a bilinear pairing operation;

E: the time for computing an exponentiation;

M: the time for computing a point multiplication;

$|x|$: the bit-length of x;

The detailed comparisons are listed as Table 1. Note that the computation of $e(H_1(ID_i), P_{KGC})$ and $e(D_i, H_1(ID_j))$ can be precomputed as they are common values. From this table, it can be seen that only the MHM scheme is slightly better than ours in terms of computational costs. Nevertheless, our protocol requires the shortest communication message, i.e., one group element, among all compared works. Since all compared schemes and ours are one-round protocols, they achieve only implicit authentication. It is possible to achieve explicit authentication with three half rounds according to Krawczyk's literature [5].

5. Conclusions

Based on the CL-PKC, in this paper, we proposed a secure one-round certificateless two-party key agreement protocol. In the proposed scheme, each party only has to exchange one group element for creating a shared session key and still maintains low computational costs. Additionally, we analyzed our protocol in the eCK security model to demonstrate its robustness against possible attacks and the fulfillment of crucial security attributes and definitions. Although the proposed protocol fails to exhibit the best computational costs among all existing works, it does prove the feasibility to reach a secure two-party CL-KA with only one exchanged group element.

Table 1. Comparisons among the proposed and other protocols

Protocol **Item**	**LBN**	**LXX**	**MHM**	**Ours**
Security model	eCK	eCK	eCK	eCK
Authentication type	Implicit	Implicit	Implicit	Implicit
#Exchanged messages	2	2	2	1
Length of communication messages for each party	$2\|\boldsymbol{G}_1\|$	$2\|\boldsymbol{G}_1\|$	$2\|\boldsymbol{G}_1\|$	$\|\boldsymbol{G}_1\|$
Computational costs for each party	10B + 5E	2B + 4M + 2E	B + 3M	B + M + E

Acknowledgements

The author would like to thank the anonymous reviewers for their valuable comments. This work was supported in part by the Ministry of Science and Technology of Republic of China under the contract number MOST 104-2221-E-019-018.

References

[1] **S. S. Al-Riyami, K. G. Paterson.** Certificateless public key cryptography. *Advances in Cryptology – ASIACRYPT 2003*, Springer-Verlag, pp. 452-473.

[2] **S. Blake-Wilson, D. Johnson, A. Menezes.** Key agreement protocols and their security analysis. In: *Proceedings of the 6th IMA International Conference on Cryptography and Coding,* LNCS, 1355, Springer Berlin, 1997, pp. 30-45.

[3] **W. Diffie, M. Hellman.** New directions in cryptography. *IEEE Transactions on Information Theory,* 1976, Vol. IT-22, No. 6, 644-654.

[4] **S. H. Islam, A. Singh.** (2015) Provably secure one-round certificateless authenticated group key agreement protocol for secure communications. *Wireless Personal Communications*, 2015, Vol. 85, No. 3, 879-898.

[5] **H. Krawczyk.** HMQV: a high-performance secure Diffie-Hellman protocol. *Cryptology ePrint Archive*, 2005/176, 2015, on http://eprint.iacr.org/2005/176.

[6] **B. A. LaMacchia, K. Lauter, A. Mityagin.** Stronger security of authenticated key exchange. In: *Proceedings of the 1st International Conference on Provable Security (ProvSec 2007)*, LNCS, 4784, Springer-Verlag Heidelberg, pp. 1-16.

[7] **G. Lippold, C. Boyd, J. G. Nieto.** Strongly secure certificateless key agreement. In: *Proceedings of Pairing 2009,* LNCS, 5671, Springer-Verlag Heidelberg, pp. 206-230.

[8] **W. Liu, C. Xu, J. Xu.** Certificateless two party key agreement protocol. In: *Proceedings of 2010 International Conference on Multimedia Information Networking and Security*, 2010, pp. 520-525.

[9] **C. F.Lu, T. C. Wu, C. L. Hsu.** Certificateless authenticated group key agreement scheme with privacy-preservation for resource-limited mobile devices. *International Journal of Innovative Computing Information and Control,* 2012, Vol. 8, No. 1(B), 599-615.

[10] **T. K. Mandt.** *Certificateless Authenticated Two-Party Key Agreement Protocols*. Master Thesis, Department of Computer Science and Media Technology, 2006, Gjøvik University College.

[11] **T. K. Mandt, C. H. Tan.** Certificateless authenticated two-party key agreement protocols. *Advances in Computer Science - ASIAN 2006*, Secure Software and Related Issues, LNCS, 4435, 2008, Springer Berlin, pp. 37-44.

[12] **R. Mokhtarnameh, S. B. Ho, N. Muthuvelu.** An enhanced certificateless authenticated key agreement protocol. In: *Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT)*, 2011, pp. 802-805.

[13] **A. Shamir.** Identity-based cryptosystems and signature schemes. *Advances in Cryptology – CRYPTO'84*, Springer-Verlag, 1984, pp. 47-53.

[14] **Y. Shi, J. Li.** Two-party authenticated key agreement in certificateless public key cryptography. *Wuhan University Journal of Natural Sciences*, 2007, Vol. 12, No. 1, 71-74.

[15] **W. Stallings.** Cryptography and Network Security: Principles and Practices, 4th. Ed., 2005, Prentice Hall.

[16] **M. Stamp.** Information Security: Principles and Practice, 2006, Wiley & Sons.

[17] **C. M. Swanson.** *Security in Key Agreement: Two-Party Certificateless Schemes*. Master Thesis, University of Waterloo, 2009. On: http://uwspace.uwaterloo.ca/bitstream/10012/4156/1/Swanson_Colleen.pdf

[18] **C. Swanson, D. Jao.** A study of two-party certificateless authenticated key agreement protocols. In: *Proceedings of 10th International Conference on Crypto-*

logy in India (INDOCRYPT 2009), LNCS, 5922, Springer-Verlag, pp. 57-71.

[19] **J. Teng, C. Wu.** A provable authenticated certificateless group key agreement with constant rounds. *Journal of Communications and Networks*, 2012, Vol. 14, No. 1, 104-110.

[20] **Y. Tian, C. Peng, J. Ma.** Publicly verifiable secret sharing schemes using bilinear pairings. *International Journal of Network Security*, 2012, Vol. 14, No. 3, 142-148.

[21] **S. Wang, Z. Cao, L. Wang.** Efficient certificateless authenticated key agreement protocol from pairings. *Wuhan University Journal of Natural Sciences*, 2006, Vol. 11, No. 5, 1278-1282.

[22] **L. Xia, S. Wang, J. Shen, G. Xu.** Breaking and repairing the certificateless key agreement protocol from ASIAN 2006. *Wuhan University Journal of Natural Science*, 2008, Vol. 13, No. 5, 562-566.

Received June 2015.