A Novel ID-based Authenticated Group Key Agreement Protocol Using Bilinear Pairings

Lung-Chung Li
Center for General Education, Chang Gung University, Taiwan; Department of Computer Science and Engineering, Yuan Ze University,Taiwan
lcli@mail.cgu.edu.tw

Yao-Pin Tsai
Department of Computer Science and Engineering, Yuan Ze University,Taiwan
bv2ol@ms2.hinet.net

Ru-Sheng Liu
Department of Computer Science and Engineering, Yuan Ze University,Taiwan
csrobinl@saturn.yzu.edu.tw

Abstract

Recently, several ID-based authenticated group key agreement (AGKA) crytosystems based on bilinear pairings have been proposed. It is an increasingly active research area because of the simplicity of the public key management and the efficiency. However most of the group key agreement protocols have the security and performance weakness. In this paper, we propose an authenticated group key agreement protocol with perfect forward secrecy that requires only one round without verifying signatures. We show that our scheme satisfies all known security requirements, and therefore it is more secure and efficient than other protocols.

1. Introduction

Group key agreement protocols allow two or more parties to agree on a common group key and exchange information among themselves over an insecure channel. A key agreement which provides mutual key authentication among parties is called an authenticated key agreement (AKA). The authenticated group key agreement (AGKA) protocol applications proliferate in many modern collaborative and distributed environments. As a consequence, the design of a secure and efficient protocol for group key agreement has received much attention as significant research area.

In 2000, Joux [1] presented a tripartite key agreement protocol based on parings over the elliptic curves, but this scheme suffers from the man-in-the-middle attack because it does not authenticate the communicating parties. Barua et al. [2] attempted to extend Joux's tripartite protocol to an ID-based AGKA (ID-AGKA) protocol, but their scheme requires $(\log_3 n)$ rounds. Recently, Choi et al.[3] and Du et al. [4] proposed two ID-AGKA protocols from bilinear pairings and BD [5] schemes. However, Zhang and Chen [6] showed an impersonation attack on these two protocols. To prevent such an attack, they suggest adding a time parameter to the message being signed. However, SHIM [7] showed that the protocol is still insecure against insider colluding attacks. In 2006, Lin et al. [8] proposed a multiparty key agreement protocol, but their protocol has disadvantages in number of rounds, pairing-computation and communication bandwidth.

In this paper we shall propose an ID-AGKA protocol which provides authentication without verifying the signatures. Furthermore, our protocol provides perfect forward secrecy and requires only one round, therefore it is more secure and efficient than other known ones.

The rest of this paper is organized as follows. We define the security attributes for an AGKA protocol in section 2. Section 3 introduces the basic concepts of bilinear pairings, the modified ID-PKI with system setup and key extraction. Section 4 proposes our ID-AGKA protocol. The protocol analysis is then proposed in section 5. Finally we give a conclusion in section 6.

2. Security attributes

A secure authenticated group key agreement protocol is desired to have the following attributes [9][10]:

Implicit Key Authentication: An n-party key agreement protocol provides implicit key authentication if each member in the set of protocol parties is assured that no party outside the set can learn the group secret key.

Perfect Forward Secrecy: A protocol is said to have

perfect forward secrecy if compromise of long-term keys of all the participating users does not compromise past session keys.

Known Session Key Security: Resistance to known session key security is the property that each run produces a different session key and compromise of past session keys does not allow compromise of future session keys.

Key-Compromise Impersonation: When *A*'s private key is compromised, it may be desirable that this event does not enable an adversary to impersonate other entities to *A*.

Unknown Key-Share: In an unknown key-share attack, an adversary convinces a group of entities that they share a key with the adversary, whereas in fact the key is shared between the group and another party.

No Key Control: It should not be possible for any of the participants or an adversary to force the session key to a pre-selected value or predict the value of the session key.

3. ID-based public key infrastructure with pairing

In this section, we briefly describe the concepts of bilinear pairings and discrete logarithm problem. Then we modify the ID-PKI with new system setup and key extraction algorithms.

3.1 Bilinear pairings and DL problem

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. We assume that the discrete logarithm problems (DLP) in both G_1 and G_2 are hard. Let $e: G_1 \times G_1 \to G_2$ be a pairing which satisfies the following conditions:

1. Bilinear: $e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$ and $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$ or $e(aP, bQ) = e(P, Q)^{ab}$.
2. Non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

We note that the Weil [13] and Tate [23] pairings associated with supersingular elliptic curves or abelian varieties can be modified to create such bilinear maps.

Discrete Logarithm Problem (DLP): Given two group elements P and Q, find an integer n, such that $Q = nP$ whenever such an integer exists.

We assume through this paper that DLP is intractable, which means there is no polynomial time algorithm to solve DLP with non-negligible probability.

In practice, G_1 will be the point group on an elliptic curve or the Jocobian group of a hyperelliptic curve over finite field, and G_2 will denote a subgroup of the multiplicative group of a finite field.

3.2 Modified ID-PKI

We consider the scenario where there is a key generation center (KGC) to setup the system parameters and extract the users' private keys. The basic operations consist of system setup and private key extraction. The KGC runs Bilinear Diffie-Hellman (BDH) parameter generator to generate two groups G_1, G_2 and a bilinear pairing $e: G_1 \times G_1 \to G_2$, which we described above. P is the generator of G_1, $H_1: \{0,1\}^* \to Z_q^*$ is a cryptographic hash function, $H_2: G_1 \to G_q$, $H_3: G_2 \to G_q$ are other two hash functions.

System Setup: KGC chooses a random number $s \in Z_q^*$ as the KGC's private key. $P_{pub} = sP$ is the KGC's public key. Then the KGC publishes system parameters

$$< q, G_1, G_2, \hat{e}, P, P_{pub}, H_1, H_2, H_3 >$$

Key Extraction: A user submits his identity information ID_i to KGC. KGC computes $I_i = H_1(ID_i)\ (1 \le i \le n)$ and user's public and private key pair: $Q_i = (I_i + s)P$, $S_i = (I_i + s)^{-1} P$. Then KGC sends this key pair to the user $U_i\ (1 \le i \le n)$ securely.

4. Proposed ID-AGKA protocol

In this section, we generate the pair-wise key first which is used to compute the group session key afterward, then present our ID-based one round authenticated group key agreement protocol enlightened by the modified ID-based public key infrastructure described in section 3.

Let $U_1, U_2, \cdots, U_n$ be the users who are going to agree to a session key and each has a unique identifier $ID_i\ (1 \le i \le n)$. With the ID-based public key infrastructure, each entity $U_i\ (1 \le i \le n)$ has its long-term public and private key pair (Q_i, S_i).

4.1 Pair–wise key agreement protocol

A pair-wise key agreement protocol allows two parties to establish their session keys and use the keys to encrypt the communications between them. Besides, the pair-wise keys will be used to assist in computing our secure ID-AGKA Protocol in section 4.2

In order to provide perfect forward secrecy, we use the modified McCullagh and Barreto scheme [11] to generate our pair-wise keys as follows:

Each user $U_i\ (1 \le i \le n)$ randomly chooses his ephemeral key $x_i \in Z_q^*$, computes $X_{i,j} = x_i(I_j P + P_{pub})\quad (1 \le j \le n, j \ne i)$ and sends $X_{i,j}$ to the user $U_j\ (1 \le j \le n, j \ne i)$.

After exchange the ephemeral values, all users can compute their pair–wise keys:

$$K_{i,j} = \hat{e}(P,P)^{x_i} \cdot \hat{e}(X_{j,i}, S_i) + \hat{e}(X_{j,i}, S_i)^{x_i}$$
$$= \hat{e}(P,P)^{x_i + x_j} + \hat{e}(P,P)^{x_i x_j} \quad (1 \le i, j \le n, i \ne j)$$

The above pair-wise key agreement protocol satisfies the following security properties: known session key security, no key-compromise impersonation, perfect forward secrecy, no unknown key-share, no key control.

4.2 ID-AGKA protocol

In this section, we present our ID-AGKA protocol as follows:

Round 1:

1. Each user $U_i\ (1 \le i \le n)$ randomly chooses two ephemeral keys $a_i, L_i \in Z_q^*$.
2. Each user U_i computes $T_{i,j} = a_i Q_j$ $(1 \le j \le n, j \ne i)$.
3. Each user U_i constructs a polynomial with degree n-1 as $B_i(x) = b_{i_{n-1}} x^{n-1} + b_{i_{n-2}} x^{n-2} \cdots + b_{i_1} x + L_i$ passing points $(j, H_2(Q_j))$, $(n+j, H_3(K_{i,j}))$, $1 \le j \le n, j \ne i$ and $(0, L_i)$.
4. Each user U_i sends $T_{i,j}$ to the user $U_j\ (1 \le j \le n, j \ne i)$.

Group Key Computation:

1. Upon the receipt of $T_{i,j}\ (1 \le i \le n, i \ne j)$ from other users, each user $U_j\ (1 \le j \le n)$ uses the pair–wise session keys $K_{j,i}$ to recover keys $L_i\ (1 \le i \le n, i \ne j)$ by computing polynomial $B_i(x)$ of degree n-1 that passes points $(j, H_2(Q_j))$ $1 \le j \le n, j \ne i$, and point $(n+j, H_3(K_{j,i}))$, then gets $L_i = B_i(0)$. (Note that each user can compute L_i without the need for any prior message exchange).
2. After recovering all the keys L_i $(1 \le i \le n, i \ne j)$, each user U_j calculates $L = L_1 + L_2 + \cdots + L_n$, and then computes the group session key:

$$SK = SK_j = \hat{e}(a_j Q_j + \sum_{\substack{i=1 \\ i \ne j}}^{n} T_{i,j}, LS_j)$$
$$= \hat{e}(Q_j, S_j)^{(a_1 + a_2 + \cdots + a_n)L}$$
$$= \hat{e}(P,P)^{(a_1 + a_2 + \cdots + a_n)L}$$

5. Protocol analysis

In this section, we provide security analysis for our proposed ID-AGKA protocol and then analyze its performance.

5.1 Security analysis

In this section, we analyze the security attributes depicted in section 2 for the proposed ID-AGKA protocol.

Implicit Key Authentication: The group session key is computed by each user's ephemeral and long-term private keys. So, the users are assured that no other users except the partners who have the private keys can learn the group session key.

Known Session Key Security: Each run of the protocol computes a unique session key which depends on the ephemeral private keys a_i and $L_i\ (1 \le i \le n)$.

Perfect Forward Secrecy: Suppose an adversary compromises two or more users' long-term private keys $S_i\ (1 \le i \le n)$ .Given the messages $T_{k,i} = a_k Q_i\ (1 \le k \le n, k \ne i)$, he can compute $\hat{e}(\sum_{1 \le k \le n, k \ne i}^{n} T_{k,i}, S_i) = \hat{e}(P,P)^{\sum_{1 \le k \le n, k \ne i} a_k}$, and from the message $T_{i,j} = a_i Q_j\ (1 \le i, j \le n, i \ne j)$, he can compute $\hat{e}(T_{i,j}, S_j) = \hat{e}(P,P)^{a_i}$ .So the adversary can compute $\hat{e}(P,P)^{(a_1 + a_2 + \cdots + a_n)}$. However, he cannot compute L without the pair–wise session key $K_{j,i}\ (1 \le j, i \le n, j \ne i)$. Therefore, the adversary cannot compute the group session key. In other

words, our protocol provides perfect forward secrecy.

No Key-compromise Impersonation: Suppose that $U_i's$ long-term private key $S_i (1 \le i \le n)$ is disclosed. An adversary E wants to masquerade as the U_j to all other users. E can choose ephemeral key a_j, compute $T_{j,i}$ and send it to the user U_i. But he cannot compute the SK_i without $U_i's$ ephemeral keys a_i and pair-wise keys $K_{i,j}$ $(1 \le j \le n, j \ne i)$ to compute L. In the meantime, E cannot compute the SK_j without knowing $U_j's$ long-term private key S_j.

No Unknown Key-share: This attack hardly works unless the adversary learns the private key of some entity.

No Key Control: The group session key in the protocol is determined by all members, so that neither party alone can control the outcome of the session key. No one can restrict it to lie in some predetermined value.

5.2 Performance analysis

We compare our ID-AGKA protocol with three other protocols, Barua's ID-AGKA [2], Du's ID-AGKA [4], and Lin's protocol [8] in terms of communication and computation costs.

We use notations as follows:

- Round: The total number of rounds.
- Scalar: The total number of scalar multiplications.
  (namely computing kP, where $P \in G_1$).
- Pairings: The total number of pairing computations.
- Bandwidth: The total number of messages sent by users.

Table 1. Comparison of AGKA protocols

Protocol	Round	Scalar	Pairings	Bandwidth
Barua's ID-AGKA [2]	$\lceil \log_3 n \rceil$	$\le 9(n-1)$	$\le 5n\lceil \log_3 n \rceil + 3$	<5n(n-1)
Du's ID-AGKA [4]	2	n(n+5)	4n	3(n-1)
Lin's AGKA [8]	2	n	2n	2n
Our ID-AGKA	1	n^2	n	n-1

As shown in Table 1, our protocol has better performance than the other protocols. Because pairing is a very heavy operation compared with the point scalar, exponentiation and hash operations, even if our protocol needs a little more scalar multiplications, our protocol has absolute advantages in number of rounds, pairing-computation and communication bandwidth compared with Barua's , Du's and Lin's protocols.

6. Conclusion

We have proposed a secure, efficient and scalable ID-based one round authenticated group key agreement protocol using bilinear pairings. Our protocol focuses on round, bandwidth efficiency and provides perfect forward secrecy. The proposed scheme improves on the security and performance of previously known AGKA protocols.

7. References

[1] A. Joux, "A one round protocol for tripartite Diffie-Hellman", Proc. ANTS IV, LNCS 1838, pp.385–394, Springer-Verlag, 2000.

[2] R. Barua, R. Dutta, and P. Sarkar, "Extending Joux's protocol to multi party key agreement", Indocrypt'03, LNCS 2904, pp.205–217, Springer-Verlag, 2003.

[3] K. Choi, J. Hwang, and D. Lee, "Efficient ID-based group key agreement with bilinear maps", PKC'04, LNCS 2947, pp.130–144, Springer-Verlag, 2004.

[4] X. Du, Y. Wang, J. Ge and Y. Wang, "ID-based Authenticated Two Round Multi-Party Key Agreement", Cryptology ePrint Archive: Report 2003/247.

[5] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system", Advances in Cryptology-EURO-CRYPT'94, Lecture Notes in Computer Science, Springer-Verlag, Berlin Germany, 1994.

[6] F.G. Zhang and X.F. Chen, "Attack on Two ID-based Authenticated Group Key Agreement Schemes", Cryptology ePrint Archive: Report 2003/259.

[7] Kyung-Ah SHIM, "Further Analysis of ID-Based Authenticated Group Key Agreement Protocol from Bilinear Maps", IEICE TRANS. VOL.E90-A, NO.1 JANUARY 2007.

[8] C. H. Lin, H. H. Lin, J. H. Chang, "Multiparty Key Agreement for Secure Teleconferencing", Systems, Man and Cybernetics, 2006. ICSMC '06. IEEE International Conference on Volume 5, pp. 3702-3707

[9] S. Blake-Wilson, D. Johnson and A. Menezes," Key

Agreement Protocols and their Security Analysis", the Sixth IMA International Conference on Cryptography and Coding, Cirencester, England, 1997.

[10] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. CRC Press, 1996.

[11] N. McCullagh and P.S.L.M. Barreto, "A new two-party identity-based authenticated key agreement", In Topics in Cryptology – CT-RSA 2005, Springer-Verlag LNCS 3376, 262–274, 2005.

[12] R. Dutta, R. Barua, and P. Sarkar, "Provably secure authenticated tree based group key agreement", ICICS'04, LNCS 3269, pp.92–104, Springer-Verlag, 2004.

[13] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing", In Advances in Cryptology – Crypto'2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer-Verlag, 2001.

[14] L. Chen, Z. Cheng, and N.P. Smart, "Identity-based key agreement protocols from pairings", Cryptology ePrint Archive, Report 2006/199, Available at http://eprint.iacr.org/2006/199.pdf, 2006.

[15] A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.

[16] Lein Ham and Shoubao Yang, "ID-Based Cryptographic Schemes for User Identification, Digital Signature", and Key Distribution, IEEE Journal on Selected Areas in Communications, Vol. 11, No. 5, June 1993.

[17] Neal Koblitz , "Elliptic Curve Cryptosystems, Mathematics of Computation", Vol. 48, No. 177. (Jan., 1987), pp. 203-209.

[18] L. Chen and C. Kudla, "Identity Based Authenticated Key Agreement from Pairings", Cryptology ePrint Archive, Report 2002/184, 2002.

[19] N. Smart, "An Identity Based Authenticated Key Agreement Protocol Based on the Weil Pairings", Electronics Letter, Vol 38, pp 630-632, 2002.

[20] Mike Burmester and Yvo Desmedt, "A secure and efficient conference key distribution system, In I.B.Damgard", editor, Advances in Cryptology-EURO-CRYPT'94, Lecture Notes in Computer Science, Springer-Verlag, Berlin Germany, 1994.

[21] B. E. Jung, "An Efficient Group Key Agreement Protocol", IEEE communications letters, Vol.10, No. 2, pp. 106-107, Feb. 2006

[22] M. Manulis, "Contributory Group Key Agreement Protocols, Revisited for Mobile Ad-hoc Groups". In Proceedings of MASS 2005, WSNS 2005. IEEE Computer Society, 2005.

[23] P. S. L. M. Barreto, H. Y. Kim and M. Scott, "Efficient algorithms for pairing-based cryptosystems", Advances in Cryptology – Crypto' 2002, Springer-Verlag, LNCS 2442, 2002, pp. 354-368.

[24] Shimshon Berkovits, "How to Broadcast A Secret", Lecture Notes in Computer Science. Advances inCryptology-EUROCRYPT'91, 1992, 547, 536-541.