An ID-based Authenticated Two Round Multi-Party Key Agreement

Xinjun Du, Ying Wang, Jianhua Ge and Yumin Wang
Key Laboratory of Computer
Networks and Information Security
Xidian University
Xi'an 710071, P.R. China

Abstract:

This paper proposes an ID-based authenticated two round multi-party key agreement among n parties. Several ID-based two-party and tripartite key agreement schemes were proposed recently. Rana Barua attempted to extend Joux's tripartite protocol to multi-party key agreement, but this scheme requires $\lceil \log_3 n \rceil$ rounds. Our two round multi-party key agreement scheme utilizes the idea of the two-round group key exchange protocol of Burmester and Desmedt. The authenticity of the protocol is assured by a special signature scheme, so the messages carrying the information of ephemeral key can be broadcasted authentically by an entity. Security attributes of our protocol are presented, and computational overhead are analyzed as well.

Keywords: multi-party key agreement, Bilinear pairings, Identity-based cryptography

1. Introduction

The first modern protocol for key agreement was the Diffie-Hellman protocol given in the seminal paper [1]. Diffie-Helman key agreement provided the first practical solution to the key agreement problem, allowing two parties never having met in advance or shared keying material, to establish a shared secret by exchanging messages over an open channel. A huge number of two-party key agreement protocols based Diffie-Helman problem have been proposed [2]. However, the basic Diffie-Hellman protocol does not authenticate the two communication entities, hence suffers from the "man-in-the-middle" attack. A number of works have considered solving the problem [3,4,5,6].

Another direction of research on key agreement is to extending the two-party Diffie-Hellman protocol to the multi-party setting, amongst which the three-party case receives much interest. Joux[7] presented an one-round tripartite key agreement protocol using pairings. Joux's protocol did not attempt to authenticate the three communicating entities and is also vulnerable to "man-in the-middle" attack. Lately, Al-Riyami and Paterson presented some authenticated three-party agreement protocols from pairings in [8]. The certificates of the three entities, which are issued by a Certificate Authority (CA), are used to bind an entity's identity with his static keys. However, in a certificate system, before using the public key of a user, the participants must first verify the certificate of the user. As a result, this system requires a large amount of computing time and storage.

Since Shamir [10] asked for identity-based encryption and signature scheme to simplify key management procedures in certificated-based public key infrastructure, many ID-based cryptosystem schemes have been proposed [11]. The bilinear pairings are important tools for construction of ID-based cryptographic schemes. With the construction of ID-based public key cryptosystems, ID-based public key infrastructure can be an alternative for certificate-based public key infrastructures, especially efficient key management. Zhang, Liu and Kim [9] proposed a new

identity-based authenticated three-party key agreement protocol, in which the authenticity is assured by a special signature scheme from pairing. Rana Barua[12] attempted to extend Joux's tripartite protocol to authenticated and unauthenticated multi-party key agreement, but according to the paper this scheme requires $\lceil \log_3 n \rceil$ rounds, and is not scalable.

In this paper, we utilize the idea of the BD protocol [13] and a modified signature scheme [14] to propose a two round multi-party authenticated key agreement protocol based on the ID-based public key infrastructure.

The rest of the paper is organized as follows: The next section briefly explains the bilinear pairing and ID-based public key infrastructure. Section 3 gives a detailed description of our multi-party key agreement protocol. In section 4, a heuristic analysis of this protocol is presented. Section 5 concludes this paper.

2. ID-Based Public Key Infrastructure with Pairing

In this section, we briefly describe the bilinear pairing and BDH assumption. Then the ID-based public key infrastructure based on pairing is presented.

2.1 Bilinear pairings and the Bilinear Diffie-Hellam Assumption

Let G_1 and G_2 be two cyclic groups of order q for some large prime q. G_1 is a cyclic additive group and G_2 is a cyclic multiplicative group. We assume that the discrete logarithm problems 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: $e(aP, bQ) = e(P, Q)^{ab}$,for all $P, Q \in G_1$ and all $a, b \in \mathbb{Z}_q^*$;

(2) Non-degenerate: there exists $P \in G_1$ and $Q \in G_1$, such that $e(P, Q) \neq 1$;

(3) Computability: there is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

Definition 1. The **Bilinear Diffie-Hellman (BDH) Problem** for a bilinear pairing $e: G_1 \times G_1 \to G_2$ is defined as follows: give $P, aP, bP, cP \in G_1$, compute $e(P, P)^{abc} \in G_2$, where $a, b, c \in_R \mathbb{Z}_q^*$. An algorithm $\mathcal{A}$ is said to solve the BDH problem in $< G_1, G_2, e >$ with an advantage of ε, if

$$\Pr[\mathcal{A}(P, aP, bP, cP) = e(P, P)^{abc}] > \varepsilon$$

BDH Parameter Generator: We say that a randomized algorithm $\mathcal{IG}$ be a BDH parameter generator if (1) $\mathcal{IG}$ takes a security parameter $0 < k \in \mathbb{Z}$, (2) $\mathcal{IG}$ runs in polynomial time in k, and (3) $\mathcal{IG}$ outputs the description of two groups G_1, G_2 and the description of a bilinear pairing $e: G_1 \times G_1 \to G_2$ described above.

Bilinear Diffie-Hellman Assumption: We assume that the BDH problem is hard, which means there is no polynomial time algorithm to solve BDH problem with non-negligible probability.

2.2 ID-based Public Key Infrastructure

ID-based public key infrastructure involves a Key Generation Center (KGC) and users. The basic operations consist of **Set Up** and **Private Key Extraction**. KGC runs 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 are described above. It chooses an arbitrary generator $P \in G_1$ and defines two cryptographic hash functions: $H: \{0,1\}^* \to \mathbb{Z}_q^*, H_1: \{0,1\}^* \to G_1$.

— **Set Up**: KGC chooses a random number $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$. Then the KGC publishes system parameters $params = \{G_1, G_2, q, P, P_{pub}, H, H_1\}$, and keep s as master-key.

— **Private Key Extraction**: A user submits his identity information ID to KGC. KGC computer the user's public key as $Q_{ID} = H_1(ID)$, and returns his private key $S_{ID} = sQ_{ID}$.

3. ID-based Authenticated Multi-party Key Agreement Protocol

In this section, we present an ID-based authenticated multi-party key agreement protocol enlightened by the idea of the BD protocol [13].

Let $ID_1, ..., ID_n$ be the entities which are going to agree to some session keys and each has a unique identifier $ID_i, 1 \le i \le n$. With the ID-based public key infrastructure, each entity has its public key and private key: $Q_i = H_1(ID_i)$ and $S_i = sQ_i$. The pair (Q_i, S_i) is the entity i's static key pairs.

The protocol is as follows:

1. Each entity $ID_i, 1 \le i \le n$, generates its ephemeral key $N_i \in \mathbb{Z}_q^*$ and broadcasts $z_i = N_i P$, $T_i = H(z_i)S_i + N_i P_{pub}$.

2. Each entity ID_i verifies:

$$e(\sum_{j \in \{1,...,n\} \setminus \{i\}} T_j, P) = e(\sum_{j \in \{1,...,n\} \setminus \{i\}} (H(z_j)Q_j + z_j), P_{pub}).$$

Then, it computes and broadcasts $X_i = e(P_{pub}, N_i(z_{i+1} - z_{i-1}))$.

3. Each entity ID_i now computes the key $K = e(P_{pub}, nN_i z_{i-1}) \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdots X_{i-2}$.

Note: All indexes are modulo n.

The bilinearity of e makes it easy to see that the shared session key is:

$$K = e(P, P)^{(N_1N_2+N_2N_3+\cdots N_nN_1)s}.$$

4. Analysis of the proposed protocol

4.1 Authenticity of the protocol

From the protocol we can see the authenticity of $z_i, 1 \le i \le n$ are achieved by the authenticators $T_i, 1 \le i \le n$. The authenticators are computed by the entities using their static private keys $S_i, 1 \le i \le n$. T_i can also be considered to be the entity ID_i's signature for the message z_i. As a consequence, the authenticity of the key agreement protocol is assured by the security of the ID-based signature scheme, which relies on the ID-based public key infrastructure introduced in Section 2. Without loss of generality, the entity ID_i is the signer.

Signing: Suppose that the message to be signed is $m = NULL$. The signature of the message is $H(N_iP)S_i + N_iP_{pub}$.

Verification: After getting a message m and its signature T_i, the verifier accepts the signature if and only the following equation holds:

$$e(T_i, P) = e(H(z_i)Q_i + z_i, P_{pub})$$

This signature scheme is secure against existential forgery under an adaptively chosen message attack in the random oracle model. The proof is similar to the Scheme 4 in [14]. Here, we give a brief security analysis. Suppose that there is polynomial time probabilistic Turing machine E which takes z_i and Q_i as input, and output an existential forgery of a signature from the entity ID_i with a non-negligible probability. Then we show there is a polynomial time algorithm E' can solve the weak version of Diffie-Hellman problem. The hash function H is considered to be a random oracle. According to the Forking Lemma [15], E can get two forgeries of the signature for the same message $m : T_i$ and $\hat{T}_i$. We have

$$T_i = H(m, z_i)S_i + sz_i \quad \text{and} \quad \hat{T}_i = H'(m, z_i)S_i + sz_i.$$

It follows that

$$T_i - \hat{T}_i = (H(m, z_i) - H'(m, z_i))S_i$$

then

$$e(T_i - \hat{T}_i, P) = e(Q_i, P_{pub})^{H(m,z_i)-H'(m,z_i)}.$$

From the above equation, we can see the polynomial time algorithm $E^{'}$ can invert the pairing, i.e. there is a polynomial time algorithm $f: G_2 \to G_1$. Let g be a generator of G_2, then $g^{'} = e(f(g), f(g))$ is also a generator of G_2. Furthermore, $e(f(g^{\lambda}), f(g^{\mu})) = g^{'\lambda\mu}$. That is given g^{λ} and g^{μ}, we can computed $g^{'\lambda\mu}$ and have hence solved an instance of the weak Diffie-Hellman problem in G_2.

4.2 Security of session keys

Proposition 1 *The secrecy of the session keys produced by the protocol relies on the assumption of hardness of BDH problem.*

Proof: First, we let $\alpha = e(P_{pub}, P)$ and $z_i^{'} = e(P_{pub}, z_i) = \alpha^{N_i}, 1 \le i \le n$. Then we modify the protocol as follows.

1. Each entity $ID_i, 1 \le i \le n$, generates its ephemeral key $N_i \in \mathbb{Z}_q^*$ and broadcasts $z_i^{'} = \alpha^{N_i}$.
2. Each entity ID_i computes and broadcasts $X_i = (z_{i+1}^{'} / z_{i-1}^{'})^{N_i}$.
3. Each entity ID_i now computes the session key $K = (z_{i-1}^{'})^{nN_i} \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdots X_{i-2}$.

This protocol is a basic BD protocol [13] and its security has been proven in the standard model [16]. So the messages broadcasted in step 2 provide nothing about the session key, especially the value $(z_{i-1}^{'})^{nN_i}$, to an adversary. We also can see:

$$(z_{i-1}^{'})^{nN_i} = e(P_{pub}, N_{i-1}P)^{nN_i} = e(P, P)^{N_{i-1}N_i s}.$$

Due to the bilinearity of the pairing, the entities do not exchange ephemeral keys $N_i, 1 \le i \le n$, but $N_i P, 1 \le i \le n$ in our protocol. But given $\{P, N_i P, N_{i-1} P, sP\}$, it is hard to determine $e(P, P)^{sN_i N_{i-1}}$, which relies on the assumption of hardness of BDH problem. □

The protocol also has the other security attributes: Known session key session security, Perfect forward security, No key-compromise impersonation, No key control etc. The definitions of these security attributes can be founded in [17].

4.3 Performance analysis

Table 1 gives a comprehensive idea about the number of computations per entity in our protocol. The basic computations include: Scalar Multiplication and Addition over G_1, Exponentiation over G_2, Hashing and Pairing.

Scalar Multiplication	Addition	Exponentiation	Hashing	Pairing
$n+3$	$3n-2$	$n-1$	$n-1$	4

Table 1. Computation overhead per entity

5. Conclusion

In this paper, we proposed an ID-based authenticated multi-party agreement protocol. The resulting key is determined by the ephemeral keys and the master-key of the TA. The authenticity of the protocol is assured by a digital signature scheme. The protocol is only need two rounds and is a round-optimal protocol.

Reference

[1] W. Diffie and M. Hellman. New directions in cryptography. IEEE Trans. Info. Th., 22, 644-654, 1976.

[2] A. Menezes, P.C. Van Oorschot and S. Vanstone. Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997.

[3] S. Blake-Wilson and A. Menezes. Authenticated Diffie-Hellman Key Agreement Protocols. Proceedings of the 5th Annual Workshop on Selected Areas in Cryptography(SAC'98), LNCS 1556, Springer-Verlag, pp.339-361, 1999.

[4] L. Law, A. Menezes, M.Qu, J.Solinas and S. Vanstone. An efficient protocol for authenticated key agreement. Technical Report CORR 98-05, Department of C & O, University of Waterloo, 1998.

[5] T. Matsumoto, U. Takashima and H. Imai. On seeking smart public-key distribution systems. Trans. IECE of Japan, E69, pp. 99-106, 1986.

[6] B. Song and K. Kim. Two-Pass Authenticated Key Agreement Protocol with Key Confirmation, Proc. of Indocrypt 2000, LNCS 1977, pp.237-249, Springer-Verlag, 2000.

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

[8] S. Al-Riyami and K. Paterson. Authenticated three party key agreement protocols from pairings. Cryptology ePrint Archive, Report 2002/035, available at http://eprint.iacr.org/2002/035.

[9] F. Zhang, S. Liu and K. Kim. ID-Based One Round Authenticated Tripartite Key Agreement Protocol with Pairings. Cryptology ePrint Archive, Report 2002/122, 2002.

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

[11] Martin Gagne. Identity-Based Encryption: a Survey. RSA Laboratories Cryptobytes, Vol. 6, No. 1, Spring 2003.

[12] Rana Barua, Ratna Dutta and Palash Sarkar. Extending Joux's Protocol to Multi Party Key Agreement. Cryptology ePrint Archive, Report 2003/190, 2003.

[13] 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.

[14] F. Hess. Exponent Group Signature Schemes and Efficient Identity Based Signature Schemes Based on Pairings. Cryptology ePrint Archive, Report 2002/012, 2002.

[15] D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures,

Journal of cryptology, No. 13, pp.361-396, 2000.
[16] Jonathan Katz and Moti Yung. Scalable Protocols for Authenticated Group Key Exchange. Advances in Cryptology-CRYPTO2003, pp 110-125, Springer-Verlag, 2003.