Journal of Network and Computer Applications 36 (2013) 927–932

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

New identity-based three-party authenticated key agreement protocol with provable security

Hu Xiong [a,b,c,*], Zhong Chen [b], Fagen Li [a]

[a] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, PR China
[b] Key Laboratory of Network and Software Security Assurance of the Ministry of Education, Institute of Software, School of Electronics Engineering and Computer Science, Peking University, Beijing, PR China
[c] State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, PR China

ARTICLE INFO

Article history:
Received 5 November 2011
Received in revised form
13 June 2012
Accepted 13 October 2012
Available online 23 October 2012

Keywords:
Information security
Authentication
Key agreement
Three-party
Identity-based
Provable security

ABSTRACT

Key agreement allows multi-parties exchanging public information to create a common secret key that is known only to those entities over an insecure network. In the recent years, several identity-based (ID-based) authenticated key agreement protocols have been proposed and most of them broken. In this paper, we formalize the security model of ID-based authenticated tripartite key agreement protocol and propose a provably secure ID-based authenticated key agreement protocol for three parties with formal security proof under the computational Diffie–Hellman assumption. Experimental results by using the AVISPA tool show that the proposed protocol is secure against various malicious attacks.

1. Introduction

Key agreement is one of the fundamental cryptographic primitives which allows two or more parties to exchange information over an adversatively controlled insecure network and agree upon a common session key. After that, this session key may be used for later secure communication among these parties. As the basic building block for constructing secure, complex, higher-level protocols, key agreement protocol receives a lot of concern from academe and industry. To establish a session key between two parties, the first well known key agreement protocol has been proposed by Diffie and Hellman (1976). However, their original Diffie–Hellman protocol does not offer authentication between the two communicating entities and it is vulnerable against active man-in-the-middle attack. Over the past years, dozens of approaches have been proposed to solve the problem in terms of improving security and efficiency of protocols (Dutta and Barua, 2005; Menezes et al., 1997; Sood et al., 2011; Li and Hwang, 2010).

One research line of key agreement is to generalize the two-party key agreement into multi-party setting, amongst which the three-party case receives much interest. An elegant three-party key agreement protocol using bilinear pairings along with the application in broadcast networks have been proposed in Joux's (2000) pioneering work. However, just like the basic Diffie–Hellman protocol, Joux's protocol is also insecure against the man-in-the-middle attack. To address this issue, Al-Riyami and Paterson (2003) and Shim (2003a) presented several protocols to resist the man-in-the-middle attack appears in Joux's protocol independently. However, all of these protocols are presented in traditional public key infrastructure (PKI), in which each participant must obtain and verify other user's certificate before using its public key. It is generally considered to be costly to use and manage the certificates in traditional PKI.

To simplify the complicated certificate management in PKI, Shamir (1984) introduced the notion of ID-based cryptography, where the public key of each user is easily computable from this user's identity. While the private key corresponding to that identity is computed and issued secretly to the user by a trusted third party called private key generator (PKG). In this way, ID-based cryptography eliminates the need of certificates. Since Zhang et al.'s pioneering work (Zhang et al., 2002; Liu et al., 2003), ID-based three-party authenticated key agreement protocol has rapidly emerged and been well-studied as well recently. After that, Shim and Woo (2005) showed that Zhang et al. 's protocol was insecure against an unknown key-share attack and gave an improved protocol. But later Shim–Woo's improved protocol was found to have security weakness itself (Chou et al., 2006). Nalla (2003) then gave a more efficient construction, which was broken by Shim (2003b) later. An ID-based three-party

* Corresponding author at: School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, PR China. Tel.: +86 10 62765807; fax: +86 10 62758279.
E-mail address: xionghu.uestc@gmail.com (H. Xiong).

1084-8045/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2012.10.001

authenticated key agreement protocol with k-resilience was presented by Tso et al. (2005). However, Lim et al. (2007) and Lim and Lee (2007) showed that the Tso et al.'s construction is insecure and proposed a fix. Most recently, Hölbl et al. (2010) proposed two most efficient ID-based three-party authenticated key agreement protocols up to now. Unfortunately, Nose (2011) showed that the first protocol does not offer known session key security and the second protocol is vulnerable to the insider attack. Until now, all ID-based three-party authenticated key agreement protocols are broken. A main issue with regard to the weakness of these protocols refers to the way the security analysis is conducted: the security model is not made clear, and there is not formal analysis of the claimed security properties. Therefore, provable security, which precisely defines the way an attacker interacts with the protocol in a clear mathematical model, is theoretically and also practically meaningful to guarantee the security of authentication protocols. In fact, it is challenging to design an efficient and provably secure ID-based three-party authenticated key agreement protocols. Here, we formalize the security model of ID-based three-party authenticated key agreement protocol and propose an efficient authentication protocol based on bilinear pairing. Our protocol's overhead is lower than that of Hölbl's protocol in both computation and communication. Furthermore, our new protocol is provably secure in the random oracle model under the Computational Diffie–Hellman assumption and has been validated by the AVISPA (Clarke et al., 1999; AVISPA, 2006)formal validation tool to show its security against various malicious attacks.

The rest of this paper is organized as follows. A brief review of some basic concepts and security notions used in our scheme is described in Section 2. In Section 3, we propose a new ID-based three-party authenticated key agreement protocol with the security proof. In Section 4, the comparison between our proposed protocol and related work is conducted. Finally, the conclusions are given in Section 5.

2. Preliminaries

In this section, we will review some fundamental backgrounds required in this paper.

2.1. Mathematical backgrounds

Let $\mathbb{G}_1$ denote an additive group of prime order q and $\mathbb{G}_2$ be a multiplicative group of the same order. Let P be a generator of $\mathbb{G}_1$, and $\hat{e}$ be a bilinear map such that $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following properties:

1. Bilinearity: For all $P,Q \in \mathbb{G}_1$, and $a,b \in \mathbb{Z}_q$, $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$.
2. Non-degeneracy: $\hat{e}(P,P) \neq 1_{\mathbb{G}_2}$.
3. Computability: It is efficient to compute $\hat{e}(P,Q)$ for all $P,Q \in \mathbb{G}_1$

We note that the discrete logarithm problems in $\mathbb{G}_1$ and $\mathbb{G}_2$ are hard (in a sense made precise in Boneh and Franklin, 2001) and refer to Joux (2000), Boneh and Franklin (2001), Barreto et al. (2002), and Boneh et al. (2004) for a more all-around description of how these groups, pairings and other parameters should be chosen in practice for efficiency and security. Many pairing-based cryptographic protocols are based on the hardness of the following problems (Joux, 2000; Boneh et al., 2004).

Definition 1. Given $\{P,Q\} \in \mathbb{G}_1$, the Discrete Logarithm (DL) Problem consists of computing $n \in \mathbb{Z}_q$ such that $P=nQ$ whenever such n exists.

Definition 2. Given a tuple $\{P,aP,bP\} \in \mathbb{G}_1$, for some random values $a,b \in \mathbb{Z}_q$ the Computational Diffe–Hellman (CDH) Problem consists of computing the element abP.

Definition 3. Given $\{P,xP,yP,zP\} \in \mathbb{G}_1$ for some random values $x,y,z \in \mathbb{Z}_q$, the Bilinear Diffie–Hellman (BDH) Problem consists of computing $\hat{e}(P,P)^{xyz} \in \mathbb{G}_2$.

Definition 4. Given a tuple $\{P,aP,bP\} \in G$ for some random values $a,b \in \mathbb{Z}_p$, the Divisible CDH (DCDH) Problem consists of computing the element $ab^{-1}P$.

As for the relationship between CDH problem and DCDH problem, we have the following theorem (Bao et al., 2003).

Theorem 1. *DCDH problem is equivalent to CDH problem, i.e., by solving two instances of DCDH problem, one can solve an instance of CDH problem.*

2.2. Security definitions

2.2.1. Algorithms of an ID-based tripartite authenticated key-agreement protocol

An ID-based authenticated key-agreement protocol for three parties consists of three polynomial-time algorithms: setup, extract and key agreement. These algorithms are defined as follows.

Setup: This algorithm is run by PKG. It takes as input a security parameter l and returns a master-key and a list of system parameters *params*.

Extract: This algorithm is also run by PKG. It takes as input the parameter list *params*, master-key and an entity's identity ID_i, to produce and issue the entity's private key S_{ID_i} to ID_i secretly.

Key Agreement: This is a probabilistic polynomial-time interactive algorithm which involves three entities A, B and C. The inputs are the system parameters *params* for A, B and C, plus $\{S_{ID_A},ID_A\}$ for A, $\{S_{ID_B},ID_B\}$ for B and $\{S_{ID_C},ID_C\}$ for C. Here, S_{ID_i} is the private key of i, and ID_i is the identity of i, where $i \in \{A,B,C\}$. Eventually, if the protocol does not fail, A B and C obtain a secret session key $K_{ABC} = K_{BAC} = K_{CAB} = K$.

2.2.2. Security model

Motivated by the model of Cao et al. (2010) and modified Bellare–Rogaway model (mBR model) (Bellare and Rogaway, 1993), we present a security model for ID-based tripartite authenticated key agreement protocols. The security of our protocol Π is defined by the following game between a challenger $\mathcal{CH}$ and an adversary $\mathcal{A}$. We use the oracle $\Pi^s_{i,j,k}$ to represent the s-th instance between participants i, j and k in a session. At the beginning of the game, $\mathcal{CH}$ runs the Setup algorithm, takes as input a security parameter l to obtain the master-key and the system parameters *params*. After that, $\mathcal{CH}$ sends *params* to $\mathcal{A}$ and keeps the master-key secret.

$\mathcal{A}$ is modelled by a probabilistic polynomial-time turing machine. All communications go through the adversary $\mathcal{A}$. Participants only respond to the queries by $\mathcal{A}$ and do not communicate directly among themselves. $\mathcal{A}$ can relay, delete, modify, interleave or delete all the message flows in the system. Note that $\mathcal{A}$ is allowed to make a polynomial number of queries, including one Test query defined as follows.

- Corrupt(ID_i): On input an identity ID_i, $\mathcal{CH}$ outputs the private key S_{ID_i} of participant i. The adversary can issue this query at any time regardless of whether ID_i is currently executing the protocol or not. This oracle captures the idea that damage due to loss of ID_i's private key should be restricted to those sessions where ID_i will participate in the future. This oracle not only represents the notion of forward secrecy but also