Information Sciences 293 (2015) 182–195

Contents lists available at ScienceDirect

Information Sciences

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

Certificateless one-pass and two-party authenticated key agreement protocol and its extensions ☆

Lei Zhang

Shanghai Key Laboratory of Trustworthy Computing, Software Engineering Institute, East China Normal University, Shanghai, China

ARTICLE INFO

Article history:
Received 5 June 2013
Received in revised form 25 March 2014
Accepted 12 September 2014
Available online 22 September 2014

Keywords:
Key agreement
Authentication
Certificateless cryptography
One-pass

ABSTRACT

An authenticated key agreement protocol is used to share a secret key for encrypting data being transferred between two or more parties over a public network. In this paper, we study one-pass and two-party authenticated key agreement protocols in certificateless public key cryptography. We first define a security model for certificateless one-pass and two-party authenticated key agreement protocols and then propose a concrete certificateless one-pass and two-party authenticated key agreement protocol which has low transmission overhead. Our protocol captures several common security requirements that a one-pass and two-party authenticated key agreement protocol should satisfy. We prove the security of our protocol under the computational Diffie–Hellman, square computational Diffie–Hellman and gap bilinear Diffie–Hellman assumptions in the random oracle model. Two extensions with better security attributes are also proposed.

1. Introduction

For two entities to communicate securely over open networks, it is essential for them to authenticate one another and establish a common session key. Key agreement (KA) allows two or more parties agree on such a common session key in a way that both influence the outcome. The first publicly known key agreement protocol is the Diffie–Hellman protocol [8]. However, the basic Diffie–Hellman protocol does not consider the attacks from active adversaries who have control over the channel. Several weaknesses were later reported on the Diffie–Hellman protocol, e.g., the man-in-the-middle attack [14]. This is because the Diffie–Hellman protocol does not authenticate the two communication entities. Authenticated KA [26,27] aims to resist the attacks from active adversaries and enables two or more parties to establish a shared session key over an insecure channel.

Authenticated KA protocols are studied in several cryptosystems, e.g., traditional public key cryptosystem, identity-based public key cryptosystem (ID-PKC) [21] and certificateless public key cryptography (CL-PKC) [1,28] in recent years. However, in traditional public key cryptosystem, the management of certificates is usually a big problem. ID-PKC is introduced to eliminate the certificate management in traditional public key cryptosystem. In ID-PKC, the public key of an entity is just its identity (such as its IP address). However, in ID-PKC, a trusted authority PKG is directly responsible for the generation of all the private keys in the system, there is an inherent key escrow facility in the system. CL-PKC may successfully solve the key escrow problem in ID-PKC. In CL-PKC, a trusted authority KGC is also employed to help an entity to generate its private key. However, it only generates a partial private key for the entity. To derive the full private key, the entity combines its

☆ Parts of this paper appeared in [25].

E-mail address: leizhang@sei.ecnu.edu.cn

http://dx.doi.org/10.1016/j.ins.2014.09.022
0020-0255/

partial private key with some secret information to generate its actual full private key. In this way, the key escrow problem is avoided, since the KGC does not know the whole private key of the entity. In other words, the KGC cannot represent the entity to do cryptographical operations without being detected.

Two party KA protocols can be classified into three types [19], i.e., *non-interactive*, *one-pass* and *one-round*. The basic Diffie–Hellman protocol [8] is a one-round KA protocol, in which both entities require to transmit information to each other during the protocol. Generally, one-round (authenticated) KA protocol offers better security properties than other two types of KA protocols. In a non-interactive KA protocol, no information needs to be transmitted between two entities. The classical static Diffie–Hellman protocol [8] is an example of a non-interactive one. In that protocol, an entity A can compute a shared key with another entity B knowing only the public key of B (and its own private key). However, the session key generated in a non-interactive KA is derived only from long-term private keys. Hence, they cannot offer any form of forward secrecy. In a one-pass KA protocol (e.g., one-pass HMQV [6]), only one entity is required to transmit information to the other during the protocol. One-pass KA protocols are very useful in the condition when the trade-off between security and efficiency is considered. When a message needs to be encrypted with a session key, they require two less message flows than the one-round protocols and at the same time provide better security properties than the non-interactive ones.

Authenticated one-pass and two-party KA protocols are first studied in traditional public key cryptosystem. However, the complexity of managing certificates imposes a huge cost in the widespread adoption of cryptography. In [9,18,19,22], several identity-based one-pass and two-party authenticated KA protocols are proposed. However, the protocols presented in [18,22] only provide authentication for the receiver instead of both. Further, in above identity-based one-pass and two-party authenticated KA protocols, the PKG can always compute the session key due to the key escrow problem. An authenticated KA protocol in CL-PKC may overcome the key escrow problem in ID-PKC. The first certificateless authenticated KA protocol was proposed by Al-Riyami and Paterson [1]. Later, several certificateless two-party authenticated KA protocols [10,12,13,15,16,20,27] have been presented. Among them, the authors in [13,20,27] defined the security models for certificateless authenticated KA protocols respectively. These protocols require both entities to transmit information to the other. Therefore, they are one-round KA protocols. The first certificateless one-pass and two-party authenticated KA protocol is presented in [5]. However, no formal security analysis is provided for the protocol in [5].

1.1. Our contribution

In the early version of this paper [25], we first proposed a formal security model for certificateless one-pass and two-party authenticated KA protocols. Our model captures the common security requirements [19], i.e., *known-key security*, *unknown key-share*, *random number compromise security*, *sender's key-compromise impersonation* and *sender's forward security* (see Section 3.1) that a one-pass and two-party authenticated KA protocols should satisfy as well as the abilities of Type I and Type II adversaries (see Section 3.2). Then we proposed a concrete certificateless one-pass and two-party authenticated KA protocol based on bilinear maps. Our protocol is efficient and has low communication cost. Under the Gap Bilinear Diffie–Hellman (GBDH) assumption, we proved that the proposed protocol satisfies the security requirements of known-key security, unknown key-share, random number compromise, against Type I adversary.

In this version, we prove that the proposed protocol meets all the security requirements against Type I and Type II adversaries under the assumptions that the computational Diffie–Hellman, square computational Diffie–Hellman and gap bilinear Diffie–Hellman problems are hard. Further, most of the existing one-pass and two-party authenticated KA protocols (including ours) may only satisfy the security requirements of *sender's key-compromise impersonation*, *sender's forward security*. We note that these two security requirements are weaker than the standard definition of *key-compromise impersonation* and *forward security* for one round KA protocols respectively. In this paper, we also propose two extensions of our basic protocol to achieve better security attributes. The extended protocols may achieve the standard *key-compromise impersonation* property and partially realize the property of *forward security*.

1.2. Paper organization

The rest of the paper is organized as follows. Section 2 gives some preliminaries. In Section 3, we introduce the security model for certificateless one-pass and two-party authenticated KA protocols. Our efficient certificateless one-pass and two-party authenticated KA protocol is proposed in Section 4. In Section 5, we prove the security of our protocol. Section 6 proposes two extensions of our basic protocol. Section 7 concludes our paper.

2. Preliminaries

2.1. Bilinear maps

Let G_1 be an additive group of prime order q and G_2 be a multiplicative group of the same order. Let P denote a generator of G_1. A map $\hat{e} : G_1 \times G_1 \longrightarrow G_2$ is called a bilinear map if it satisfies the following properties: