available at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Two proposed identity-based three-party authenticated key agreement protocols from pairings

*Marko Hölbl**, *Tatjana Welzer*, *Boštjan Brumen*

Faculty of Electrical Engineering and Computer Science, University of Maribor, Smetanova ulica 17, 2000 Maribor, Slovenia

ARTICLE INFO

Article history:
Received 3 August 2009
Received in revised form
31 August 2009
Accepted 31 August 2009

Keywords:
Authentication
Key agreement
Bilinear pairing
Three-party
Authenticated identity-based key agreement protocol

ABSTRACT

The use of pairings has been shown promising for many two-party and three-party identity-based authenticated key agreement protocols. In recent years, several identity-based authenticated key agreement protocols have been proposed and most of them broken. In this paper, we propose two three-party identity-based authenticated key agreement protocols applying bilinear pairings. We show that the proposed protocols are secure (i.e. conform to defined security attributes) while being efficient.

1. Introduction

Key agreement protocols are used to establish a common session key for encrypting communications between two or multiple parties. In 1976, Diffie and Hellman (1976) proposed the first key agreement protocol which enabled two parties to establish a session key. However, it did not offer authentication and was susceptible to the man-in-the-middle attack. Since then, different approaches and protocols have been developed to solve the problem, improve security and efficient of protocols (Dutta and Barua, 2005; Menezes et al., 1997).

A research direction in key agreement protocol aims to generalize two-party key agreement sets to multi-party key agreement sets. A special case of multi-party key agreement protocols are three-party (or tripartite) protocols. The pioneer work in the field was conducted by Joux (2000), who showed how to implement a three-party key agreement protocol using pairings. Since in his protocol only one broadcast is required, Joux's protocol is suitable for practical implementation. However, just like the Diffie–Hellman protocol, Joux's protocol does not provide authentication and thus is vulnerable to the man-in-the-middle attack. To solve the problem Al-Riyami and Paterson (2002) presented several protocols some of which use pairing. Their protocols assure authenticity through use of certificates issued by a Certificate Authority (CA). The session keys are generated by both ephemeral (short-term) keys and static (long-term) keys. The signature of the CA assures that only the entities which are in possesion of the static keys are able to compute the session keys. Still, in a certificate system the participants must first verify the certificates before using the public key of a user, which requires a large amount of computing time and storage.

* *Corresponding author*. Tel.: +386 2 220 7361; fax: +386 2 220 7272.
E-mail address: marko.holbl@uni-mb.si (M. Hölbl).
0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.08.006

Hence, an infrastructure is needed to establish and manage the key pairs and certificates, often referred to as certificate-based public key infrastructure (PKI).

As an alternative to certificate-based PKIs, Shamir (1985) introduced the concept of a identity-based cryptosystem, in which the user's public key is an easily calculated function of her identity (e.g. social security number, etc.), while the user's private key can be calculated for her by a trusted party referred to as Private Key Generator (PKG). The identity-based public key cryptosystem simplifies the process of key management and can be an alternative of certificate-based PKI. In such cryptosystems, entity A can send encrypted messages to entity B by using her identity information even before B obtains her private key from the PKG. Hence, the idea also provides a way to construct authenticated key agreement protocols.

Recently, bilinear pairings have found positive application in cryptography (Boneh and Franklin, 2003; Boneh et al., 2004; Joux, 2000; Sakai et al., 2005) and can also be used for constructing identity-based cryptographic protocols. Many identity-based cryptographic protocols for two and three-party setting have been proposed using bilinear pairings. Some examples are Boneh and Franklin's (2003) identity-based encryption scheme, identity-based authentication key agreement protocol by Smart (2002), McCullagh and Barreto (2005) and several identity-based signatures schemes (Cha and Cheon, 2003; Paterson, 2002; Sakai et al., 2005). For both protocols flaws which lead to attacks were published (Cheng et al., 2005; Choo, 2005; Shim, 2003a). Moreover, Choo et al. (2005) pointed out the flaws in the security proof of the ''McCullagh–Barreto's protocol.

In 2002, Smart (2002) published the first two-party identity-based authenticated key agreement protocol using pairings. Later, several protocols were proposed and some have been broken. For comprehensive surveys of two-party identity-based authenticated key agreement protocols using pairings refer to Boyd and Choo (2005), Chen et al. (2007), Dutta et al. (2004), Dutta and Barua (2005). Additionally, several new proposed protocols were presented and are not included in the surveys (Chow and Choo, 2007; Huang and Cao, 2008; Lim et al., 2008; Oh et al., 2007; Wang et al., 2007). Almost simultaneously to Smart, Zhang, Liu and Kim introduced the first three-party identity-based authenticated key agreement protocol using pairings (Zhang et al., 2002). Afterwards many protocols for three-party settings were published (Nalla, 2003; Nalla and Reddy, 2003; Shim, 2003b; Shim and Woo, 2005). Some attacks and the corresponding improvements were presented (Shim, 2003b; Shim and Woo, 2005), but later these improvements were found to have security weaknesses themselves (Chou et al., 2006).

In this paper we examine three-party authenticated key agreement protocols using pairing operations. The main contribution includes the proposal of two one round three-party identity-based authenticated key agreement protocols using pairings, which feature all security attributes (Chen and Kudla, 2003; Nalla and Reddy, 2003) and are efficient. Additionally, to corroborate the security and efficiency of the proposed protocols, we compare our proposed protocols to all existing three-party authenticated key agreement protocol regarding security and efficiency.

The rest of the paper is organized as follows: Section 2 briefly explains preliminary concepts, i.e. bilinear maps, the associated computational problems, the security and efficiency criteria; i.e. security attributes desired for sound authenticated key agreement protocols and properties regarding efficiency. Our proposed protocols are described in Section 3 with the corresponding security and efficiency discussion. In Section 4 the efficiency and security comparison of the proposed protocols and competitive protocols is conducted. Finally, a conclusion is drawn in Section 5.

2. Preliminaries

First, we briefly describe preliminaries which are needed later in the paper. We give the basic definition and properties of bilinear pairings, the computational problems which are fundamental when discussing identity-based authenticated key agreement protocols, security attributes desired for sound authenticated key agreement protocols and efficiency properties.

2.1. Bilinear maps

We describe in a more general format the basic definition and properties of the pairing. More details can be found in Joux (2000) and Boneh and Franklin (2003).

Let P denote a generator of $\mathbb{G}_1$, where $\mathbb{G}_1$ is an additive group of large order q and let $\mathbb{G}_2$ be a multiplicative group with $|\mathbb{G}_1| = |\mathbb{G}_2|$. A pairing is a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ which has the following properties:

1. *Bilinearity*: Given $Q,W,Z \in \mathbb{G}_1$, we have $\hat{e}(Q,W+Z)=\hat{e}(Q,W)\cdot\hat{e}(Q,Z)$ and $\hat{e}(Q+W,Z)=\hat{e}(Q,Z)\cdot\hat{e}(W,Z)$.

   Therefore for any $q, b \in \mathbb{Z}_q$: $\hat{e}(aQ, bW) = \hat{e}(Q, W)^{ab} = \hat{e}(abQ, W) = \hat{e}(Q, abW) = \hat{e}(bQ, W)^{a}$.

2. *Non-degenerative*: $\hat{e}(P, P) \neq 1$, where 1 is the identity element of $\mathbb{G}_2$.
3. The map $\hat{e}$ is efficiently computable.

In practice $\mathbb{G}_1$ is a subgroup of the group of points on an elliptic curve over a finite field, e.g. $E(\mathbb{F}_p)$. Then $\mathbb{G}_2$ is a subgroup of a multiplicative group of a related finite field. Usually $\mathbb{G}_1$ has around 2^{160} elements and $\mathbb{G}_2$ is a subgroup of $E(\mathbb{F}_{p^r})$, where r is the embedding degree and p^r has about 1024 bits. If r is increased, the pairing's computational efficiency decreases.

The map $\hat{e}$ can be derived by modifying the Weil pairing (Frey et al., 1999) (both inputs are of the same cyclic group) or the Tate pairing (Menezes et al., 1993) (related inputs are in the left hand side of the pairing map) on an elliptic curve over $\mathbb{F}_p$. The computational effort of the Tate pairing is less than of the Weil pairing. However, both need to be modified since the pairing may always output $1 \in \mathbb{G}_2$ on the right side of the pairing.

A more detailed explanations of topics regarding bilinear maps, the Weil and Tate pairings, the aspects implementation and selection of suitable curves can be found in Boneh and