Computer Networks 89 (2015) 32–43

Contents lists available at ScienceDirect

Computer Networks

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

Identity-based secure group communications using pairings

Francesco Rossi [a], Giovanni Schmid [b,*]

[a] Department of Science and Technology, University of Naples Parthenope, Centro Direzionale, Isola C4, Naples 80143, Italy
[b] High Performance Computing and Networking Institute, National Research Council, via P. Castellino 111, Naples 80131, Italy

ARTICLE INFO

Article history:
Received 21 August 2014
Revised 15 April 2015
Accepted 9 July 2015
Available online 17 July 2015

Keywords:
Identity-based cryptography
Pairing-based signatures
Group key agreement

ABSTRACT

Identity-based secure group communications are relevant for distributed environments, whenever a group of peers needs to autonomously perform secure interactions in the context of an application, offered as a service by a trusted third party. A ground tool to enable secure group communications is authenticated group key agreement; indeed, once established a group secret key, integrity and confidentiality of group communications can be enforced thanks to symmetric cryptography.

In this paper, we discuss the construction and implementation of identity-based signature schemes that make use of bilinear pairing to get shorter signatures, and their application to authenticated group key agreement. Besides the introduction of two new signature schemes, the aim of this contribution would be to show that through such schemes one can get implementations for identity-based secure group communications that scale sufficiently well with respect to the number of involved parties. We run a set of experiments that corroborate our expectations.

1. Introduction

The concept of identity-based cryptography was introduced by Shamir [25]. The innovation was the use of identity attributes instead of public keys for data encryption and signature, thus avoiding the generation and management of user public key certificates. That can significantly reduce the complexity and overheads introduced by asymmetric cryptography in case of large scale distributed system.

In particular, identity-based cryptography fits very well the deployment and trust models subtended whenever secure group communications need to be autonomously set up in the context of an application offered as a service by a trusted third party.

Examples of such distributed environments include social and collaborative networks over the Internet and special-purpose networks such as wireless ad-hoc networks (WANETs).

From a security point of view, group communications root in authenticated *group key agreement* (GKA) [20]; indeed, once established an authentic group key, data integrity and confidentiality among the group of communicating parties can be enforced easily and efficiently thanks to state-of-the-art symmetric cryptography. However, authenticated GKA protocols are demanding cryptographic tools, both in terms of network bandwidth and computational resources. At the time being, there are no implementations for secure group communications that scale well so to be applied in large networks.

Besides the advantages tied to ID-based cryptography, GKA protocols can improve their performance thanks to elliptic curve cryptography. Therefore, it is important to have identity-based signature (IBS) schemes that can be implemented on elliptic curves. The IBS scheme introduced in [25] should be implementable on elliptic curves, since this scheme is based on the RSA transformation, and an elliptic

* Corresponding author. Tel.: +39 81 6139529; fax: +39 81 6139531.
E-mail address: giovanni.schmid@cnr.it (G. Schmid).

http://dx.doi.org/10.1016/j.comnet.2015.07.007
1389-1286/

counterpart of such transformation was introduced in [8]. In a better way, we dispose also of an identity-based counterpart of the digital signature standard ECDSA [14], since the BNN-IBS scheme of [2] is based on a Schnorr-type signature.

However, a further performance gain, especially relevant as it relates to the length of the signature of messages and thus to the communication costs of protocols, can be obtained using elliptic curves for which it is possible to consider discrete logarithm systems with a bilinear structure. Short signatures can be very important in low-bandwidth communication environments, such as low-data-rate, wireless networks (LR-WPANs) [31], which are increasingly being used to build WANETs.

In this paper, we discuss the construction and implementation of IBS schemes which make use of bilinear pairings to get shorter signatures, and their application to authenticated group key agreement. Besides the introduction of two new IBS schemes that can be considered the identity-based counterparts of the BLS [4] and ZSS [30] conventional signature schemes, the aim of our contribution would be to show that through such schemes one can get implementations for identity-based secure group communications that scale sufficiently well with respect to the number of involved parties.

The paper is organized as follows. Section 2 discusses signature schemes related to the ones introduced in the present work. Section 3 outlines some notions and notations that are used throughout the rest of the paper. In Section 4 we describe the algorithmic framework for ID-based short signatures and introduce two new such schemes, proving that they are existentially unforgeable under adaptive chosen-message attacks. In Section 5 we illustrate the Java environment that we have implemented in order to assess the performance of our schemes and their effectiveness in the context of secure group communications. Section 6 summarizes the results of various tests we have done thanks to the environment described in the previous section. Finally, in Section 7 we draw conclusions and sketch out future work.

2. Related work

The two identity-based signature (IBS) schemes introduced in the present work were derived from the Boneh–Lynn–Shacham (BLS) [4] and the Zhang–Safavi-Naini–Susilo (ZSS) [30] ordinary signature schemes. The BLS scheme was introduced to get shorter signatures than the *standard signature algorithm* [18] over elliptic curves (ECDSA) [14]. It allows indeed for about half-size signatures than ECDSA since its signature, after point compression (see Section 3.5), consists of the x-coordinate of a single point in a cyclic group $\mathbb{G}$ of prime order l, instead of the two x-coordinates of points in the same group required by the ECDSA. However, that comes at the expense of more workload for the verifier, since signature verification in the BLS scheme requires a comparison between two pairing computations, whilst in the ECDSA it just requires compairing the x-coordinates of two points in $\mathbb{G}$. Thus, the BLS scheme can be a valid alternative to the ECDSA, especially in low-bandwidth communication environments, but only if the overhead required for signature verifications does not undo the better performance in communication. The ZSS scheme is actually a modification of the BLS scheme which requires just one pairing computation for signature verification instead of two, since one pairing computation involves only public parameters of the KGC, and can be precomputed.

At least at our current knowledge, the above state of affairs exists with minor modifications in the identity-based setting, too. The only known IBS scheme based on a Schnorr-type signature is the BNN-IBS scheme of [2], and its elliptic curve version does not require any pairing computation to verify a signature, which composes of two points of $\mathbb{G}$ plus two integers in $\mathbb{Z}_l^* = \{1, \ldots, l-1\}$. On the other hand, a signature in the BLMQ-IBS scheme of [1] composes of one element in $\mathbb{G}$ and one integer in $\mathbb{Z}_l^*$, at the price of one pairing computation for the verifier. Thus, through the compression of points available for groups over elliptic curves, the BLMQ-IBS scheme allows for about half-size signatures than BNN-IBS, but with some overhead in computation for the verifier.

Signatures of roughly the same length as BLMQ-IBS can be obtained with the GS-IBS of [12], but at the cost of two more pairing computations. However, the security of scheme GS-IBS follows from the hardness of the co-CDH problem (see Section 3), whilst that of the BLMQ-IBS scheme relies on a stronger and somewhat unusual hardness assumption.

Our IBS schemes attain the same signature lengths, and require just two and one pairing computations, respectively. Moreover, their security can be proved on the basis of the "standard" assumption of the hardness of the co-CDH problem.

3. Preliminaries

In this section we briefly review some basic facts about discrete logarithms, elliptic curves and bilinear pairings, pointing out notations and assumptions that will be used in the sequel. More details about these topics can be found for example in [16,26].

3.1. Finite fields and DL systems

If $\mathbb{F}_q = \mathbb{F}_q(+, \cdot)$ denotes a field with q elements, then it follows that $q = p^d$, where p is a prime number called the *characteristic* of the field, and d is a positive integer called its *extension degree*. The $q-1$ non zero elements of $\mathbb{F}_q$ form an abelian group w.r.t. multiplication, which has many applications in cryptography; it is often denoted as $\mathbb{F}_q^* = \mathbb{F}_q^*(\cdot)$. Each $P \in \mathbb{F}_q^*$ admits a least positive integer l such that $P^l = 1$, which is called the *order* of P and divides $q-1$. Moreover, if $\varphi(n)$ denotes the number of positive integers $i < n$ such that $\gcd(i, n) = 1$, there are exactly $\varphi(q-1)$ elements $G \in \mathbb{F}_q^*$ having order $l = q-1$. Each such G is called a *generator* of $\mathbb{F}_q$, since $\langle G \rangle = \{G^i : i = 1, \ldots q-1\} = \mathbb{F}_q^*$.

We will suppose from now to choose $P \in \mathbb{F}_q^*$ in such way that its order l is prime, so that l is a prime factor of $q-1$ and $\gcd(l, q) = 1$. The cyclic multiplicative group generated by any of such P, $\langle P \rangle = \{P^i : i = 1, \ldots, l\}$, is a subgroup of $\mathbb{F}_q^*$ which has order l and exhausts all nonzero residue classes modulo l. Thus, we can consider the following problem in $\langle P \rangle$:

Definition 1 (Discrete logarithm problem)**.** Let $P \in \mathbb{F}_q^*$ be of prime order l. The *discrete logarithm* (DL) problem in $\mathbb{G} = \langle P \rangle$ is as follows: given $Q \in \mathbb{G}$, find $x \in \mathbb{Z}_l$ such that $Q = P^x$. The