Information Sciences 179 (2009) 1647–1656

Contents lists available at ScienceDirect

Information Sciences

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

On the transferability of private signatures

Javier Herranz *

Dept. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya, C. Jordi Girona, 1-3, E-08034 Barcelona, Spain

ARTICLE INFO

Article history:
Received 10 April 2008
Received in revised form 20 January 2009
Accepted 21 January 2009

Keywords:
Digital signatures
Designated verifiers
Transferable signatures

ABSTRACT

In some situations, a user wants to sign a message in such a way that only a designated verifier is convinced of the validity of the signature, whereas other users cannot distinguish whether the signer has signed this message at all. In some cases, the signer may want to preserve this level of privacy forever, which means that the initial verifier should not be able to convince anyone else of the fact that the signer signed the message. In some other cases, the signer may want to give the initial verifier the possibility to transfer his conviction to someone else (maybe to everybody), when/if desired.

In this paper we review this notion of private signatures, focusing on the level of transferability desired by the signer. We first consider the two extreme cases (non-transferability and complete transferability) which can be generically and efficiently solved by using very basic cryptographic primitives, as we show in this paper. Then we consider a case with partial transferability, for which we propose a generic solution based on the primitive of distributed ring signatures.

1. Introduction

Digital signatures provide authentication, integrity and non-repudiation to digital communications. One of the standard properties of basic digital signatures is *universal verifiability*, which means that everybody can verify the validity of a published signature, by using the public key of the signer. However, this property is not always desirable, e.g. in scenarios such as contract signing or electronic voting. For this reason, some kinds of signature schemes with additional properties were introduced, to allow the signer to restrict the verifiability of his signatures. Some examples are: *undeniable* signatures [5], where interaction with the signer is necessary in order to verify the validity of a signature; *confirmer signatures* [6], where verification is possible only after interacting with the signer or with a designated confirmer; *designated verifier signatures* [12,21], where only a designated verifier is convinced of the validity of a signature, and he cannot convince anyone else of this fact.

In this work we are not interested in signatures which require interaction with some entity (e.g. the own signer, or a confirmer) to be verified. We consider practical situations where a signer A wants to compute a private signature, which can be verified, initially, only by a designated person B. Other users, even after seeing the private signature, do not obtain any information about the signature; in other words, they cannot distinguish if a string of bits contains a valid signature by A on a certain message, or if it is just a random string of bits (containing for example a signature on another message). Contract signing and electronic voting offer some examples of real situations where this kind of signatures could be applied. For example, when two companies are signing a contract, each company can issue a signature to convince only the other company of the fact that it agrees with the contents of the contract. In an electronic voting system, a voter may want to privately reveal his vote to someone, in order to influence in his vote, without letting him transfer this signature to someone else, or maybe only to a specific subset of users.

* Tel.: +34 934016015; fax: +34 934015981.
E-mail address: jherranz@ma4.upc.edu

0020-0255/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2009.01.023

These examples already show that, once the private signature has been computed and published (so that only the verifier is convinced of the authorship of the signature), there are different possibilities concerning the "future life" of the signature. This is captured by the *transferability* level of the signature. The most restrictive case is *non-transferability*: the initial verifier B will never be able to convince anyone else of the fact that the signer A issued a certain private signature. This can be desirable for situations where the information contained in the signed message is very sensitive. The least restrictive case is *complete transferability*: the signer A gives to the initial verifier B the possibility to transfer the signature (i.e., his conviction) to everybody else, if (and when) B wants. This situation can happen when the information in the signed message is more sensitive for B than for A, and so B must decide if other users should be aware of the fact that A has signed this message.

Of course, there is a wide room between these two extreme situations for transferability. In general, we could refer to these intermediate situations as signatures with *restricted transferability*: the signer A allows the verifier B to transfer his conviction, if some conditions or restrictions are satisfied. For example, A can impose the set of users to whom B can transfer a signature, or A can impose the period of time for which such a transfer is possible, or A can impose some condition(s) on the content of the messages whose signatures can be transferred. In the aforementioned example of contract signing, one of the companies A can privately sign his agreement on the contract to the other company B, allowing B to transfer this signature to a specified set of external parties (a judge, a related company, etc.), only during a specific period of time.

1.1. Our contribution

In this paper we consider private signatures with different levels of transferability. For each of the cases, we formalize the security properties that must be required to the corresponding signature schemes. These requirements include privacy, different notions of unforgeability, and different notions related to the transferability property. For the extreme situations (non-transferability and complete transferability), we explain some generic constructions which result in private signature schemes with the desired properties. In the case of non-transferable private signatures, they are equivalent to strong designated verifier signatures (SDVS), widely studied in the cryptographic literature. For the case of completely transferable private signatures, we give a new efficient and generic construction, which employs very basic cryptographic primitives: a signature scheme, a key derivation function and a symmetric encryption scheme. We also explain a variant of our generic construction, which allows the signer to securely open a private signature, when desired, converting it into a universally verifiable signature. Finally, for intermediate levels of transferability, we consider the case where the signer specifies the subset of users to whom the signature can be transferred by the verifier. We propose a generic construction for this functionality, which uses the primitive of distributed ring signature as a building block.

1.2. Organization of the paper

The rest of the paper is organized as follows. In Section 2, we review the cryptographic primitives which will appear in the description of the generic constructions of the other sections: symmetric encryption schemes, digital signatures and distributed ring signatures. The following three sections are devoted to private signatures with different levels of transferability: non-transferable signatures in Section 3, completely transferable signatures in Section 4, and signatures with restricted transferability in Section 5. We conclude the work in Section 6.

2. Preliminaries

In this section we review some cryptographic primitives which will play a central role in the generic constructions of private signatures that we will propose throughout the rest of the paper.

2.1. Symmetric encryption

In a symmetric encryption scheme, two users (the sender and the receiver of the message) must previously agree in a common and secret key K. This can be done by means of a physical meeting, or by using some key agreement protocol which uses asymmetric (or public key) cryptography as a basic tool. An example is the well-known Diffie–Hellman key exchange protocol [7], which has been extended and modified to admit a formal security proof.

Once this key K has been securely obtained, each execution of the encryption scheme (E, D) consists of two protocols. The encryption protocol E takes as inputs a plaintext m and K, and produces as output a ciphertext c. The decryption protocol D takes as inputs a ciphertext c and K, and outputs a plaintext $\tilde{m}$. For correctness, we require $D(E(m, K), K) = m$, for any key K and any plaintext m.

Regarding security, we will consider symmetric encryption schemes which enjoy the strongest security level: indistinguishability of plaintexts under a chosen-ciphertext attack. This means that any adversary $\mathscr{A}_{sym}$ succeeds only with probability (or advantage) negligibly greater than 1/2, in the following game:

(1) A challenger generates at random a secret key K for the scheme (E, D).
(2) $\mathscr{A}_{sym}$ chooses two plaintexts m_0 and m_1, and sends them to the challenger.