A Signature Scheme with Efficient Protocols

Jan Camenisch[1] and Anna Lysyanskaya[2]

[1] IBM Research
Zurich Research Laboratory
CH–8803 Rüschlikon
jca@zurich.ibm.com
[2] Computer Science Department
Brown University
Providence, RI 02912 USA
anna@cs.brown.edu

Abstract. Digital signature schemes are a fundamental cryptographic primitive, of use both in its own right, and as a building block in cryptographic protocol design. In this paper, we propose a practical and provably secure signature scheme and show protocols (1) for issuing a signature on a committed value (so the signer has no information about the signed value), and (2) for proving knowledge of a signature on a committed value. This signature scheme and corresponding protocols are a building block for the design of anonymity-enhancing cryptographic systems, such as electronic cash, group signatures, and anonymous credential systems. The security of our signature scheme and protocols relies on the Strong RSA assumption. These results are a generalization of the anonymous credential system of Camenisch and Lysyanskaya.

1 Introduction

Digital signature schemes are a fundamental cryptographic application, invented together with public-key cryptography by Diffie and Hellman [20] and first constructed by Rivest, Shamir and Adleman [32]. They give the electronic equivalent of the paper-based idea of having a document signed.

A digital signature scheme consists of (1) a key generation algorithm that generates a public key PK and a secret key SK; (2) a signing algorithm that takes as inputs a message m and a secret key SK and generates a signature σ; and (3) a verification algorithm that tests whether some string σ is a signature on message m under the public key PK. Signature scheme exists if and only if one-way functions exist [30,33]. However, the efficiency of these general constructions, and also the fact that these signature schemes require the signer's secret key to change between invocations of the signing algorithm, makes these solutions undesirable in practice.

Using an ideal random function (this is the so-called *random-oracle* model), several, much more efficient signature schemes were shown to be secure. Most notably, those are the RSA [32], the Fiat-Shamir [21], and the Schnorr [34] signature schemes. However, ideal random functions cannot be implemented in

S. Cimato et al. (Eds.): SCN 2002, LNCS 2576, pp. 268–289, 2003.

the plain model [12], and therefore in the plain model, these signature schemes are not provably secure.

Gennaro, Halevi, and Rabin [24] and Cramer and Shoup [16] proposed the first signature schemes whose efficiency is suitable for practical use and whose security analysis does not assume an ideal random function. Their schemes are secure under the so-called *Strong RSA assumption*.

In contrast to these stand-alone solutions, our goal is to construct signature schemes that are suitable as building blocks for other applications.

Consider the use of signature schemes for constructing an anonymous credential system [13,14,15,19,27,7]. While such a system can be constructed from any signature scheme using general techniques for cryptographic protocol design, we observe that doing it in this fashion is very inefficient. Let us explain this point in more detail.

In a credential system, a user can obtain access to a resource only by presenting a credential that demonstrates that he is authorised to do so. In the paper-based world, examples of such credentials are passports that allow us to prove citizenship and authorise us to vote, driver's licenses that prove our ability to drive cars, etc. In the digital world, it is reasonable to imagine that such a credential will be in the form of a digital signature. Let us imagine that the user's identity is his secret key SK. Let us think of a credential as a signature on this secret key.

A credential system is anonymous if it allows users to demonstrate such credentials without revealing any additional information about their identity. In essence, when the user shows up before the verifier and demonstrates that he has a credential, the verifier can infer nothing about who the user is other than that the user has the right credential. Additionally, an anonymous credential system allows the user to obtain a credential anonymously.

Using general zero-knowledge proofs, it is possible to prove statements such as "I have a signature," without saying anything more than that (i.e., without disclosing what this credential looks like). However, doing so requires that the problem at hand be represented as, for example, a Boolean circuit, and then the proof that the statement is true requires a proof that the circuit has a satisfying assignment. This method, however, requires expensive computations beyond what is considered practical.

An additional complication is obtaining credentials in a secure way. The simple solution where the user reveals his identity SK to the credential granting organization, who in turn grants him the credential, is ruled out: we want to allow the user to be anonymous when obtaining credentials as well; we also want to protect the user from identity theft, and so the user's secret key SK should never be leaked to any other party. Here, general techniques of secure two-party computation save the day: the user and the organization can use a secure two-party protocol such that the user's output is a signature on his identity, while the organization learns nothing. But this is also very expensive: general secure two-party computation also represents the function to be computed as a Boolean circuit, and then proceeds to evaluate it gate by gate.