EFFICIENT DIGITAL PUBLIC-KEY SIGNATURES WITH SHADOW

Louis Guillou * & Jean-Jacques Quisquater **

(*) CCETT, Rue du Clos-Courtel, B.P. 59, F-35510 Cesson-Sévigné, France.

(**) Philips Research Laboratory Brussels, Avenue Van Becelaere, 2, B-1170 Brussels, Belgium.

Abstract

This paper describes a strictly deterministic digital signature scheme using public-key cryptosystems. This scheme is in discussion inside a working group of ISO on signature schemes (TC97/SC20/WG2). A working draft has been written and accepted recently (with formal modifications to be added). By this presentation we hope to receive useful remarks for improving this scheme. This scheme is the fastest known scheme for the *verification* of signature (only one square plus some very easy operations).

We introduce the notion of signatures with *shadow* – that is, when the signature is mathematically attached together the message to sign – and with *imprint* – that is, where the message and the signature are two separate entities.

This scheme is RSA-based and, in some aspects, is a variant of Rabin-Williams schemes. However, if the scheme is correctly implemented, it is immune against the attacks by chosen messages. The technique is well-known: You introduce a redundancy in the message before you sign with your secret function. This trick permits to the secret function to be defined nearly nowhere: The multiplicative attack of Davida, for instance, is then without effect.

The original part of the paper is an effective and efficient proposition for the function of redundancy and its uses and a structured way to sign and to verify with a weak dependence from the functions. If you use the RSA or one of its variants, you are in a context where each known optimisation is possible.

The function of redundancy is defined in such a way that the system resists to any known attack; moreover the redundancy is used, if necessary, to identify the correct message from the possible ones when you verify the signature . Indeed, in the scheme of Williams, the operation of signature needs a square root: The message thus needs to be a quadratic residue. A useful result is that from the set $\{a, -a, a/2, -a/2\}$, there is one and only one quadratic residue . So, in fact, you can detect the unique quadratic residue from this set then you extract the square root of this one. The redundancy is also used to indicate the length of the signed message (if the message is short) or of the hashed value of the message.

Many useful details will be given in the full paper.

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, p. 223, 1988.