On-Line/Off-Line Digital Signatures*

Shimon Even
Computer Science Department, Technion—Israel Institute of Technology,
Haifa 32000, Israel
even@cs.technion.ac.il

Oded Goldreich
Department of Applied Mathematics and Computer Science,
Weizmann Institute of Science, Rehovot, Israel
oded@wisdom.weizmann.ac.il

Silvio Micali
Laboratory for Computer Science, Massachusetts Institute of Technology,
545 Technology Square, Cambridge, MA 02139, U.S.A.
silvio@theory.lcs.mit.edu

Communicated by Gilles Brassard
Received 19 August 1992 and revised 21 December 1994

Abstract. A new type of signature scheme is proposed. It consists of two phases. The first phase is performed off-line, before the message to be signed is even known. The second phase is performed on-line, once the message to be signed is known, and is supposed to be very fast. A method for constructing such on-line/off-line signature schemes is presented. The method uses one-time signature schemes, which are very fast, for the on-line signing. An ordinary signature scheme is used for the off-line stage.

In a practical implementation of our scheme, we use a variant of Rabin's signature scheme (based on factoring) and DES. In the on-line phase all we use is a moderate amount of DES computation and a single modular multiplication. We stress that the costly modular exponentiation operation is performed off-line. This implementation is ideally suited for electronic wallets or smart cards.

Key words. Digital signatures, Integer factorization, RSA, DES, One-time signature schemes, Error-correcting codes, Chosen message attack.

1. Introduction

Informally, in a digital signature scheme, each user $U$ publishes a public key while keeping secret a secret key. $U$'s signature of a message $m$ is a value $\sigma$, depending on

---

* A preliminary version appeared in the Proceedings of Crypto 89. Shimon Even was supported by the fund for the Promotion of Research at the Technion.
and his secret key, such that $U$ (using his secret key) can quickly generate $\sigma$ and anyone can quickly verify the validity of $\sigma$, using $U$'s public key. However, it is hard to forge $U$'s signatures without knowledge of his secret key. We stress that signing is a noninteractive process involving only the signer, and that arbitrarily many messages can be signed, with one pair of keys.

Many signature schemes are known. Based on various intractability assumptions, several schemes have been proven secure even against chosen message attack [8], [7], [1], [14], [21]. Unfortunately, in these schemes, the signing process is not sufficiently fast for some practical purposes. Furthermore, even more efficient schemes like RSA [20] and Rabin's scheme of [17] (which achieve a "lower level" of security) are considered too slow for many practical applications (e.g., electronic wallets [5], [4]). In particular, these signature schemes require performing modular exponentiation with a large modulus as part of the signing process, and this in turn requires many modular multiplications. Furthermore, these costly operations can start only once the message to be signed becomes known. Consequently, these signature schemes will become much more attractive if only a few (say, two or three) modular multiplications need to be performed once the message becomes known, while the more costly operations can be preprocessed. This leads to the notion of an on-line/off-line signature scheme.

A New Notion

To summarize, in many applications signatures have to be produced very fast once the message is presented. However, slower precomputations can be tolerated, provided that they do not have to be performed on-line (i.e., once the message to be signed is handed to the signer and while the verifier is waiting for the signature). This suggests the notion of an on-line/off-line signature scheme, in which the signing process can be broken into two phases. The first phase, performed off-line, is independent of the particular message to be signed; while the second phase is performed on-line, once the message is presented. We are interested in on-line/off-line signature schemes in which the off-line stage is feasible (though relatively slow) and both on-line signing and verification are fast.

A General Construction

We present a general construction transforming an ordinary digital signature scheme to an on-line/off-line one. This is done by properly combining three main ingredients:

1. An (ordinary) signature scheme.
2. A fast one-time signature scheme (i.e., a signature scheme known to be unforgeable, provided it is used to sign a single message).
3. A fast collision-free hashing scheme (i.e., a hashing scheme for which it is infeasible to find two strings which hash to the same value).

The essence of the construction is to use the ordinary signature scheme to sign (off-line) a randomly constructed instance of the information which enables one-time signature, and later to sign (on-line) the message using the one-time signature scheme (which is typically very fast). The hashing scheme is most likely to be used in practice for compressing long messages into shorter tags, but it is not essential for the basic construction.