Computer security
Cryptography module: Public key cryptography

Ignacio Cascudo

Digital signatures definition

A digital signature scheme has three algorithms

- **Key generation** $KGen(1^\lambda)$:
  Input: a "security parameter" λ (length of the keys).
  Output: a pair (pk, sk) of public key and private (or secret) key.
  Will be run by Alice
- **Signing** $Sig(m, sk)$:
  Input: A message m and private key sk.
  Output: A signature σ.
  Will be run by Alice
- **Verification** $Ver(m, \sigma, pk)$:
  Input: A message m, a signature σ and public key pk.
  Output: A decision bit 0/1 (0: reject, 1: accept).
  Will be run by Bob

Correctness requirement

For every (pk, sk) generated by *KGen*, for every message m

$$Ver(m, Sig(m, sk), pk) = 1$$

I.e., signatures of a message with *Sig* (using a certain secret key) are accepted by the verification algorithm with the corresponding public key.

Comparison to MACs

Advantages:

- Publicly verifiable
- Transferable
- Non-repudiation

Disadvantages:
Slower than MACs

Security

- Intuitively: Nobody can create signatures of messages that are accepted with *pk*, without knowing *sk*.
- But also: Nobody should modify an already signed message so that it is accepted (without knowing *sk*).
- Note that the attacker may have seen many other messages signed with *sk* before.
- Maybe she has even made Alice sign messages of the attacker's choice.
- Notion: Unforgeability under chosen message attacks.