Fail–Stop Signatures

José Abel González Silva
CINVESTAV–IPN

This poster presents a fail–stop signature scheme, in which signing a message block requires two modular multiplications and verification requires less than two modular exponentiations. Furthermore a construction is shown of an undeniable signature scheme, which is unconditionally secure for the signer, and which allows the signer to convert undeniable signatures into fail–stop signatures.