CORR 2001-13

Provably Secure Distributed Schnorr Signatures and a (t, n) Threshold Scheme for Implicit Certificates

D.R. Stinson & R. Strobl*

Abstract In a (t, n) threshold digital signature scheme, t out of n signers must co-operate to issue a signature. We present an efficient and robust (t, n) threshold version of Schnorr's signature scheme: i.e., existentially unforgeable under adaptively chosen message attacks. The signature scheme is then incorporated into a (t, n) threshold scheme for implicit certificates. We prove the implicit certificate scheme to be as secure as the distributed Schnorr signature scheme.