CORR 99-44

Certification of Secure RSA Keys

S.R. Blackburn* and Steven D. Galbraith

Abstract In environments using RSA schemes, a Certification Authority (CA) is often used to bind a user's public key to their identity. The paper proposes a method of RSA key generation which convinces the CA that a user's key has been well generated, i.e. that the resulting RSA problem is hard with overwhelming probability. This is achieved by involving both the user and the CA in the key generation process in such a way that the CA does not obtain significant information about the user's secret RSA decryption key.