CORR 2000-55

Provably Secure Implicit Certificate Schemes

D.R.L. Brown*, R. Gallant*, S.A. Vanstone

Abstract Optimal mail certificates, introduced in [11], are efficient types of implicit certificates which offer many advantages over traditional (explicit) certificates. For example, an optimal mail certificate is small enough to fit on a two-dimensional digital postal mark together with a digital signature. This paper defines a general notion of security for implicit certificates, and proves that optimal mail certificates are secure under this definition.