CORR 2001-63

Security of Signature Schemes in a Multi-User Setting

Alfred Menezes & Nigel Smart*

Abstract This paper considers the security of signature schemes in the multi-user setting. We argue that the well-accepted notion of security for signature schemes, namely existential unforgeability against adaptive chosen-message attacks, is not adequate for the multi-user setting. We extend this security notion to the multi-user setting and show that signature schemes proven secure in the single-user setting can, under reasonable constraints, also be proven secure in the multi-user setting.