CORR 2000-54

The Exact Security of ECDSA

Daniel R.L. Brown*

Abstract The provable security results of Pointcheval et al [4, 12] for certain discrete logarithm based signature schemes are all in the random oracle model, where the has function employed is modeled by an idealized has function. These security results are not applicable to the widely standardized DSA and ECDSA signature schemes, unless the schemes are modified so that the signer hashes both the message and the random group element generated, rather than just the message. the provable security results of Jakobsson and Schnorr [10] for certain discrete logarithm based signature schemes work in the combined generic group model of Shoup [13] and the random oracle model. In this paper, we prove that ECDSA is secure against existential forgery by adaptive chosen-message attack if the elliptic curve group is modeled by a generic group and if the has function employed is collision-resistant. We also provide an exact security analysis of our proof. Since our proof works in a model which is weaker than the combined model of [10], our proofs give a stronger security assurance. Curiously, our proof technique does not appear to be applicable to proving the security of DSA.