CORR 2002-06

Generic Groups, Collision Resistance, ECDSA

Daniel R.L. Brown*

Abstract Proved here is the sufficiency of conditions to ensure the Elliptic Curve Digital Signature Algorithm (ECDSA) existentially unforgeable by adaptive chosen-message attacks.The sufficient conditions include (i) a uniformity property and collision-resistance for the underlying has function, (ii) pseudo-randomness in the private key space for the ephemeral private key generator, (iii) generic treatment of the underlying group, and (iv) a further condition on how the ephemeral public keys are mapped into the private key space. For conditions are weaker than the corresponding sufficient conditions and used in the security proofs here, but others are identical. Despite the similarity between DSA and ECDSA, the main result is not appropriate for DSA, because the fourth condition above seems to fail for DSA. (The corresponding necessary condition is plausible for DSA, but is not proved here nor is the security of DSA proved assuming this weaker condition.) Brickell et al. [11], Jakobsson et al. [29] and Pointcheval et al. [44] only consider signature schemes that include the ephemeral public key in the has input, which ECDSA does not do, and moreover, assume a condition on the has function stronger than the first condition above. this work seems to be the first advance in the provable security of ECDSA.