CORR 2000-39

Formal Security Proofs for a Signature Scheme with Partial Message Recovery

Daniel R.L. Brown* & Don B. Johnson*

Abstract The Pintsov-Vanstone signature scheme with partial message recovery (PVSSR) is a variant of the Schnorr and Nyberg-Rueppel signature schemes. It produces very short signatures on messages with intrinsic redundancy. At 80 bits of security, cryptographic overhead (message expansion) ranges from 20 to 30 bytes, depending on the amount of intrinsic redundancy in the message being signed. (In comparison, an ECDSA signature with the same domain parameters would have an overhead of about 40 bytes.) This article gives a formal proof of the security of PVSSR, which reduces the difficulty of existential forgery to the difficulty of the discrete logarithm problem. The proof works in the random oracle model (which assumes an ideal hash function) combined with an ideal cipher model. Suggested instantiations for the ciphers in cryptographic applications are symmetric encryption primitives, such as 3DES or AES. A second proof is given, in which the random oracle model is replaced by the generic group model. A third proof permits the cipher to be XOR, by working in both the random oracle model and the generic group model.