CORR 2001-50

A Small Subgroup Attack on a Key Agreement Protocol of Arazi

Dan Brown and Alfred Menezes

Abstract In 1993, Arazi presented akey agreement protocol that integrates the Deffie-Hellman key agreement protocol and the digital signature algorithm (DSA). In this note, we present a small subgroup attack on Arazi's protocol whereby an attacker can learn another entity's DSA private key. The attack illustrates the importance of public-key validation, i.e., checking that group elements received from another party do indeed have the prescribed order. The attack also demonstrates that extreme care must be exercised when two or more cryptographic protocols are combined to design a new protocol.