Susilo, Willy; Mu, Yi

Deniable ring authentication revisited. (English) Zbl 1103.68539


Summary: Ring signatures allow a signer in an ad-hoc group to authenticate a message on behalf of the group without revealing which member actually produced the signature. Recently, this notion has been extended by Naor by introducing Deniable Ring Authentication: it is possible to convince a verifier that a member of an ad-hoc subset of participants is authenticating a message without revealing which member has issued the signature, and the verifier ∨ cannot convince any third party that message \( m \) was indeed authenticated. Unfortunately, the scheme proposed by M. Naor [Lect. Notes Comput. Sci. 2442, 481–498 (2002; Zbl 1026.94549)] requires an interactive protocol, which requires an assumption that an anonymous routing channel (eg. MIX-net) exists. Having this restriction, the primitive cannot be used in practice without the existence of the anonymous routing channel. In this paper, we introduce a non-interactive version of deniable ring authentication. This work proposes a deniable ring authentication without any interactive protocol required. We present a generic construction that can convert any existing ring signature schemes to deniable ring authentication schemes. Our generic construction combines any ring signature scheme with an ID-based chameleon hash function. We also present three ID-based chameleon hash functions and show that our schemes outperform the construction proposed by G. Ateniese and B. de Medeiros [Lect. Notes Comput. Sci. 3110, 164–180 (2004; Zbl 1105.94302)].

For the entire collection see [Zbl 1052.68004].

MSC:

68P25 Data encryption (aspects in computer science)
94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing

Full Text: DOI