Cryptology ePrint Archive: Report 2011/693

A non-interactive deniable authentication scheme in the standard model

Bin Wang ,Qing Zhao and Ke Dai

Abstract: Deniable authentication protocols enable a sender to authenticate a message to a receiver such that the receiver is unable to prove the identity of the sender to a third party. In contrast to interactive schemes, non-interactive deniable authentication schemes improve communication efficiency. Currently, several non-interactive deniable authentication schemes have been proposed with provable security in the random oracle model. In this paper, we study the problem of constructing non-interactive deniable authentication scheme secure in the standard model without bilinear groups. An efficient non-interactive deniable authentication scheme is presented by combining the Diffie-Hellman key exchange protocol with authenticated encryption schemes. We prove the security of our scheme by sequences of games and show that the computational cost of our construction can be dramatically reduced by applying pre-computation technique.

Category / Keywords: public-key cryptography /

Date: received 20 Dec 2011

Contact author: jxbin76 at yahoo cn

Available formats: PDF | BibTeX Citation

Version: 20111223:122155 (All versions of this report)

Discussion forum: Show discussion | Start new discussion
