Cryptology ePrint Archive: Report 2011/046

Lower and Upper Bounds for Deniable Public-Key Encryption

Rikke Bendlin and Jesper Buus Nielsen and Peter Sebastian Nordholt and Claudio Orlandi

Abstract: A deniable cryptosystem allows a sender and a receiver to communicate over an insecure channel in such a way that the communication is still secure even if the adversary can threaten the parties into revealing their internal states after the execution of the protocol. This is done by allowing the parties to change their internal state to make it look like a given ciphertext decrypts to a message different from what it really decrypts to. Deniable encryption was in this way introduced to allow to deny a message exchange and hence combat coercion.

Depending on which parties can be coerced, the security level, the flavor and the number of rounds of the cryptosystem, it is possible to define a number of notions of deniable encryption. In this paper we prove that there does not exist any non-interactive receiver-deniable cryptosystem with better than polynomial security. This also shows that it is impossible to construct a non-interactive bi-deniable public-key encryption scheme with better than polynomial security. Specifically, we give an explicit bound relating the security of the scheme to how efficient the scheme is in terms of key size. Our impossibility result establishes a lower bound on the security. As a final contribution we give constructions of deniable public-key encryption schemes which establishes upper bounds on the security in terms of key length. There is a gap between our lower and upper bounds, which leaves the interesting open problem of finding the tight bounds.

Category / Keywords: public-key cryptography / deniable encryption

Publication Info: Full version of an ASIACRYPT 2011 paper.

Date: received 25 Jan 2011, last revised 13 Sep 2011

Contact author: jbn at cs au dk

Available formats: PDF | BibTeX Citation

Version: 20110913:121655 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]