Cryptology ePrint Archive: Report 2011/066

Deniable Encryption with Negligible Detection Probability: An Interactive Construction

Markus Duermuth and David Mandell Freeman

Abstract: Deniable encryption, introduced in 1997 by Canetti, Dwork, Naor, and Ostrovsky, guarantees that the sender or the receiver of a secret message is able to "fake" the message encrypted in a specific ciphertext in the presence of a coercing adversary, without the adversary detecting that he was not given the real message. To date, constructions are only known either for weakened variants with separate "honest" and "dishonest" encryption algorithms, or for single-algorithm schemes with non-negligible detection probability.

We propose a sender-deniable public key encryption system with a single encryption algorithm. We describe a generic interactive construction based on a public key bit encryption scheme that has certain properties, and we give two examples of encryption schemes with these properties, one based on the quadratic residuosity assumption and the other on trapdoor permutations.

Subsequent to the publication of this work in EUROCRYPT 2011, it was shown by Peikert and Waters that, contrary to our initial claim, the proposed scheme does not have negligible detection probability. In this updated version we describe the attack of Peikert and Waters and the error in our original proof. We include the previous version of the paper with the construction and the (incorrect) security theorem.

Category / Keywords: public-key cryptography / Deniable encryption, electronic voting, multi-party computation.

Publication Info: Eurocrypt 2011

Date: received 4 Feb 2011, last revised 18 May 2011

Contact author: dfreeman at cs stanford edu