Cryptology ePrint Archive: Report 2011/352

Bi-Deniable Public-Key Encryption

Adam O'Neill and Chris Peikert and Brent Waters

Abstract: In CRYPTO 1997, Canetti \etal put forward the intruiging notion of \emph{deniable encryption}, which (informally) allows a sender and/or receiver, having already performed some encrypted communication, to produce `fake' (but legitimate-looking) random coins that open the ciphertext to another message. Deniability is a powerful notion for both practice and theory: apart from its inherent utility for resisting coercion, a deniable scheme is also noncommitting (a useful property in constructing adaptively secure protocols) and secure under selective-opening attacks on whichever parties can equivocate. To date, however, known constructions have achieved only limited forms of deniability, requiring at least one party to withhold its randomness, and in some cases using an interactive protocol or external parties.

In this work we construct \emph{bi-deniable} public-key cryptosystems, in which both the sender and receiver can simultaneously equivocate; we stress that the schemes are noninteractive and involve no third parties. One of our systems is based generically on ``simulatable encryption'' as defined by Damg{\aa}rd and Nielsen (CRYPTO 2000), while the other is lattice-based and builds upon the results of Gentry, Peikert and Vaikuntanathan (STOC 2008) with techniques that may be of independent interest. Both schemes work in the so-called ``multi-distributional'' model, in which the parties run alternative key-generation and encryption algorithms for equivocable communication, but claim under coercion to have run the prescribed algorithms. Although multi-distributional deniability has not attracted much attention, we argue that it is meaningful and useful because it provides credible coercion resistance in certain settings, and suffices for all of the related properties mentioned above.

Category / Keywords: public-key cryptography / Deniable encryption, noncommitting encryption, simulatable encryption, lattice cryptography

Publication Info: Full version of paper appearing in CRYPTO 2011

Date: received 30 Jun 2011, last revised 15 Sep 2011

Contact author: cpeikert at cc gatech edu

Available formats: PDF | BibTeX Citation

Note: Included missing section on bi-deniability in the identity-based setting.

Version: 20110915:124106 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]