Cryptology ePrint Archive: Report 2012/727

On the Impossibility of Sender-Deniable Public Key Encryption

Dana Dachman-Soled

Abstract: The primitive of deniable encryption was first introduced by Canetti et al. (CRYPTO, 1997). Deniable encryption is a regular public key encryption scheme with the added feature that after running the protocol honestly and transmitting a message m, both Sender and Receiver may produce random coins showing that the transmitted ciphertext was an encryption of any message m' in the message space. Deniable encryption is a key tool for constructing incoercible protocols, since it allows a party to send one message and later provide apparent evidence to a coercer that a different message was sent. In addition, deniable encryption may be used to obtain \emph{adaptively}-secure multiparty computation (MPC) protocols and is secure under \emph{selective-opening} attacks. Different flavors such as sender-deniable and receiver-deniable encryption, where only the Sender or Receiver can produce fake random coins, have been considered.

Recently, several open questions regarding the feasibility of deniable encryption have been resolved (c.f. (O'Neill et al., CRYPTO, 2011), (Bendlin et al., ASIACRYPT, 2011)). A fundamental remaining open question is whether it is possible to construct sender-deniable Encryption Schemes with super-polynomial security, where an adversary has negligible advantage in distinguishing real and fake openings.

The primitive of simulatable public key encryption (PKE), introduced by Damg{\aa}rd and Nielsen (CRYPTO, 2000), is a public key encryption scheme with additional properties that allow oblivious sampling of public keys and ciphertexts. It is one of the low-level primitives used to construct adaptively-secure MPC protocols and was used by O'Neill et al. in their construction of bi-deniable encryption in the multi-distributional model (CRYPTO, 2011). Moreover, the original construction of sender-deniable encryption with polynomial security given by Canetti et al. can be instantiated with simulatable PKE. Thus, a natural question to ask is whether it is possible to construct sender-deniable encryption with \emph{super-polynomial security} from simulatable PKE.

In this work, we investigate the possibility of constructing sender-deniable public key encryption from the primitive of simulatable PKE in a black-box manner. We show that, in fact, there is no black-box construction of sender-deniable encryption with super-polynomial security from simulatable PKE. This indicates that the original construction of sender-deniable public key encryption given by Canetti et al. is in some sense optimal, since improving on it will require the use of non-black-box techniques, stronger underlying assumptions or interaction.

Category / Keywords: foundations / sender-deniable encryption, simulatable PKE, black-box separation

Date: received 28 Dec 2012

Contact author: dadachma at microsoft com