Cryptology ePrint Archive: Report 2011/581

Standard Security Does Not Imply Security Against Selective-Opening

Mihir Bellare and Rafael Dowsley and Brent Waters and Scott Yilek

Abstract: We show that no commitment scheme that is hiding and binding according to the standard definition is semantically-secure under selective opening attack (SOA), resolving a long-standing and fundamental open question about the power of SOAs. We also obtain the first examples of IND-CPA encryption schemes that are not secure under SOA, both for sender corruptions where encryption coins are revealed and receiver corruptions where decryption keys are revealed. These results assume only the existence of collision-resistant hash functions.

Category / Keywords: Commitment schemes, encryption, impossibility results, attacks

Publication Info: A preliminary version appears on EUROCRYPT 2012. This is the full version.

Date: received 26 Oct 2011, last revised 18 Jan 2012

Contact author: mihir at eng ucsd edu