Cryptology ePrint Archive: Report 2011/442

Another Look at Tightness

Sanjit Chatterjee and Alfred Menezes and Palash Sarkar

Abstract: We examine a natural, but non-tight, reductionist security proof for deterministic message authentication code (MAC) schemes in the multi-user setting. If security parameters for the MAC scheme are selected without accounting for the non-tightness in the reduction, then the MAC scheme is shown to provide a level of security that is less than desirable in the multi-user setting. We find similar deficiencies in the security assurances provided by non-tight proofs when we analyze some protocols in the literature including ones for network authentication and aggregate MACs. Our observations call into question the practical value of non-tight reductionist security proofs. We also exhibit attacks on authenticated encryption and disk encryption schemes in the multi-user setting.

Category / Keywords: cryptographic protocols /

Publication Info: Also available at http://anotherlook.ca

Date: received 14 Aug 2011, last revised 8 Jan 2012

Contact author: ajmeneze at uwaterloo ca