Cryptology ePrint Archive: Report 2011/343

Another Look at Security Definitions

Neal Koblitz and Alfred Menezes

Abstract: We take a critical look at security models that are often used to give "provable security" guarantees. We pay particular attention to digital signatures, symmetric-key encryption, and leakage resilience. We find that there has been a surprising amount of uncertainty about what the "right" definitions might be. Even when definitions have an appealing logical elegance and nicely reflect certain notions of security, they fail to take into account many types of attacks and do not provide a comprehensive model of adversarial behavior.

Category / Keywords:

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

Date: received 23 Jun 2011, last revised 29 Sep 2011

Contact author: ajmeneze at uwaterloo ca