Cryptology ePrint Archive: Report 2011/541

Minimalism in Cryptography: The Even-Mansour Scheme Revisited

Orr Dunkelman, Nathan Keller, Adi Shamir

Abstract: In this paper we consider the following fundamental problem: What is the simplest possible construction of a block cipher which is provably secure in some formal sense? This problem motivated Even and Mansour to develop their scheme in 1991, but its exact security remained open for more than 20 years in the sense that the lower bound proof considered known plaintexts, whereas the best published attack (which was based on differential cryptanalysis) required chosen plaintexts. In this paper we solve this long standing open problem by describing the new Slidex attack which matches the T = \Omega(2^n/D) lower bound on the time T for any number of known plaintexts D. Once we obtain this tight bound, we can show that the original two-key Even-Mansour scheme is not minimal in the sense that it can be simplified into a single key scheme with half as many key bits which provides exactly the same security, and which can be argued to be the simplest conceivable provably secure block cipher. We then show that there can be no comparable lower bound on the memory requirements of such attacks, by developing a new memoryless attack which can be applied with the same time complexity but only in the special case of D=2^{n/2}. In the last part of the paper we analyze the security of several other variants of the Even-Mansour scheme, showing that some of them provide the same level of security while in others the lower bound proof fails for very delicate reasons.

Category / Keywords: foundations / Even-Mansour block cipher, whitening keys, minimalism, provable security, slide attacks, slidex attack, mirror slide attack.

Date: received 2 Oct 2011

Contact author: orr dunkelman at weizmann ac il