Does Lightweight Cryptography Imply Slightsecurity?

Orr Dunkelman

Department of Computer Science

University of Haifa

Haifa, Israel

Abstract:

In recent years, the field of lightweight cryptography has emerged to offer security for constrained environments. A plenitude of cryptographic solutions, from block ciphers, to stream ciphers, and even public key cryptosystems, were suggested. However, due to some of the constraints imposed on lightweight implementations, designers need to take a very unusual point on the security-performance trade-off curve. In this talk we will go over several examples, and see what might go wrong when the optimization is taken one step too far.