CORR 2001-15

Some observations on the theory of cryptographic has functions

D.R. Stinson

Abstract In this paper, we study several issues related to the notion of "secure" hash functions. Several necessary conditions are considered, as well as a popular sufficient condition (the so-called random oracle model). We study the security of various problems that are motivated by the notion of a secure has functions. these problems are analyzed in the random oracle model, and we prove that the obvious trivial algorithms are optimal. As well, we look closely at reductions between various problems. In particular, we consider the important question "does preimage resistance imply collision resistance?" Finally, we study the relationship of the security of has functions built using the merkle-Damgård construction to the security of the underlying compression function.