Cryptographic Hash Functions: Past, Present and Future

Bart Preneel
Katholieke Universiteit Leuven

29/03/2006
EIDMA SEMINAR COMBINATORIAL THEORY

In this talk we review the design principles for iterated hash functions developed in the last two decades. We start by revisiting the definitions and requirements for hash functions; we also focus on the issues related to parameterisation. Next we discuss the relation between the security of the compression functions and that of the iterated hash functions based on them. In particular, we revisit the results of Merkle-Damgard (collision resistance) and Lai-Massey (preimage resistance). We also present the recent attacks by Felten et al., Kelsey et al., and Joux on iterated hash functions. Finally we will discuss our new results on the applicability of the currently-known cryptanalytic techniques to HMAC constructions based functions of the MD4 and SHA family.