Differential cryptanalysis of hash functions — overview and recent results

Eli Biham
Computer Science Department, Technion, Haifa, Israel

September 21, 2007

Abstract: In this talk we will give an overview of differential cryptanalysis of hash functions, starting with the first attacks on Snefru to the latest attacks on SHA-1. In addition, recent results on Snefru will be presented, as well as insights on the relation between padding, preimages of the compression function, and preimages of the hash function.