Hash Functions and Error-Correcting Codes

Bart Preneel

K.U.Leuven

Cryptographic hash functions and MAC algorithms are widely used to protect data. In the past decade, they have been at the focus of attention of cryptographers because of a series of impressive attacks on commonly used standards. Hash functions and MAC algorithms map inputs of arbitrary size to outputs of fixed lengths; they have as goal that any small modification to their inputs should result in a large modification of the output. In some sense, they are dual to error-correcting codes, which have as goal to allow to bring together inputs that have small modifications. In this talk we explore the connections between these objects.

Katholieke Universiteit Leuven, Dept. Elektrotechniek-ESAT/COSIC, Kasteelpark Arenberg 10, Bus 2446, B-3001 Leuven-Heverlee, Belgium
bart.preneel@esat.kuleuven.be