On round functions of permutation

Joan Daemen

Radboud University, The Netherlands

Permutation-based cryptography was successful the NIST SHA-3 competition and more recently also in the NIST lighweight cryptography competition. Building an efficient permutation is similar to building a good block cipher, but not quite. In this talk we take a closer look at the structure and components of round functions of successful permutations with a focus on symmetry properties.