PERMUTATION GROUP METHODS FOR BLOCK CIPHER SECURITY

Riccardo Aragona

Università degli Studi dell'Aquila

In 1949 Shannon gave the first formal definition of block cipher as a set of transformations on a message space. In 1975, Coppersmith and Grossman studied the group generated by a set of bijective transformations defining a cipher and the relationship of some properties of this group with the security of the corresponding cipher. From this work a new research sector in algebraic cryptography arises, that of the study of the properties of the group generated by the encryption functions of a cipher that can reveal weaknesses in the cipher itself. In the first part of the talk, after presenting the algebraic background describing the structure of block ciphers and some security notions, we will explain the relationship between permutation groups and security of block ciphers. In the second part of the talk we will present some new results that characterize the properties of the components of a block cipher and of the corresponding permutation group which guarantee security against known algebraic attacks.