The revised boomerang connectivity tables and their connection to the difference distribution table

Kirpa Garg*[1]

[1]université de rouen normandie – Université de Rouen Normandie – France

Résumé

It is well-known that functions over finite fields play a crucial role in designing substitution boxes (S-boxes) in modern block ciphers. To analyze the security of an S-box, recently, three new tables have been introduced: the Extended Boomerang Connectivity Table (EBCT), the Lower Boomerang Connectivity Table (LBCT), and the Upper Boomerang Connectivity Table (UBCT). These tables provide improved methods over the usual Boomerang Connectivity Table (BCT) for evaluating the resistance of S-boxes to boomerang-style attacks.
We put in context these new EBCT, LBCT, and UBCT concepts by connecting them to the well known Difference Distribution Table (DDT) for a differentially δ-uniform function. Moreover, we determine the entries of these tables for three families of differentially 4-uniform power permutations: Gold, Kasami, and Bracken-Leander. As by products of our approach, we obtain some previously published results quite easily. In addition, we study the invariance of the EBCT, LBCT and UBCT under CCZ, extended affine and affine-equivalence.
Collaboration with Sartaj Ul Hasan, Constanza Riera and Pantelimon Stanica

*Intervenant