NIKOLAY KALEYSKI, University of Bergen, Norway
Bounding the Hamming distance between APN functions

Almost perfect nonlinear (APN) functions are defined as those functions that provide the best possible resistance to differential cryptanalysis. Their significance reaches far beyond the practical needs of cryptography: APN functions have a natural combinatorial definition, and thus correspond to optimal objects in many diverse areas of study (design theory, coding theory, sequence design, algebra, affine geometry, etc.) APN functions have very little structure by design and are difficult to study. We show how a lower bound on the distance between APN functions can be derived, and explore some of its practical and theoretical applications.