Abstract

Vectorial Boolean functions are crucial building-blocks in symmetric ciphers. Different known attacks on block ciphers have resulted in diverse cryptographic criteria for vectorial Boolean functions,such as differential uniformity and nonlinearity. Very recently, Bar-On et al. Introduced at Eurocrypt'19 a new tool, called the differential-linear connectivity table (DLCT), which allows for taking into account the dependency between the two subciphers E_0 and E_1 involved in differential-linear attacks. This new notion leads to significant improvements of differential-linear attacks on several ciphers.

In this talk we present a theoretical characterization of the DLCT of vectorial Boolean functions and also investigates this new criterion for some families of functions with specific forms. More precisely, we firstly reveal the connection between the DLCT and the autocorrelation of vectorial Boolean functions, we characterize properties of the DLCT by means of the Walsh transform of the function and of its differential distribution table, and we present generic bounds on the highest magnitude occurring in the DLCT of vectorial Boolean functions, which coincides with the well-established notion of absolute indicator.

Next, we investigate the invariance property of the DLCT of vectorial Boolean functions under the affine, extended-affine, and Carlet-Charpin-Zinoviev (CCZ) equivalence and exhaust the DLCT spectra of optimal 4-bit S-boxes under affine equivalence. Furthermore, we study the DLCT of APN, plateaued and AB functions and establish its connection with other cryptographic criteria. Finally, we investigate the DLCT and the absolute indicator of some specific polynomials with optimal or low differential uniformity, including monomials, cubic functions, quadratic functions and inverses of quadratic permutations.

This is joint work of Anne Canteaut, Lukas Kölsch, Chao Li, Chunlei Li, Kangquan Li and Friedrich Wiemer