Low-weight correlation-immune Boolean functions for counter-measures to side channel attacks

Claude Carlet
LAGA, University of Paris 8
University of Bergen
(work in common with Xi Chen)

Correlation-immune (CI) Boolean functions are defined as keeping the same output distribution when some number (called the correlation immunity order of the function) of input variables are fixed. CI functions have been widely used as combiners in stream ciphers to allow resistance to the Siegenthaler correlation attack. Since such functions need to be balanced, it is more resilient functions (i.e. CI balanced functions) which were actively studied. The supports of CI functions are orthogonal arrays and these functions play then also a role in combinatorics.

The Siegenthaler bound on the algebraic degree of CI functions makes high order CI functions weak against fast algebraic attacks and their study has then been less active during the last ten years.

Recently, a new use of CI functions has appeared in the framework of side channel attacks (SCA) [1]. To reduce the cost overhead of counter-measures to SCA, CI functions need to have low Hamming weights. This poses new challenges (the known constructions, based on properties of the Walsh transform, do not allow to build unbalanced CI functions).

We shall propose constructions from [2] of low-weight CI functions based on the Fourier-Hadamard transform, while the known constructions of resilient functions are based on the Walsh transform. These two transforms are closely related but the resulting constructions are very different.

References

[1] C. Carlet and S. Guilley. Side-channel indistinguishability. *HASP '13*, pp. 9:1-9:8. Tel Aviv, Israel. ACM, New York, 2013.

[2] C. Carlet and X. Chen. Constructing low-weight dth-order correlation-immune Boolean functions through the Fourier-Hadamard transform. IEEE Transactions on Information Theory 64(4), pp. 2969-2978, 2018.