Boolean Functions with Multiplicative Complexity 3 and 4

Çağdaş Çalık, Meltem Sönmez Turan, and René Peralta

National Institute of Standards and Technology

Classification of Boolean functions with respect to affine equivalence relation is important in cryptography and logic synthesis. It is helpful when studying cryptographic properties of Boolean functions, since (*i*) most of the relevant properties (such as nonlinearity, distribution of absolute values in Walsh spectrum and auto-correlation spectrum) are invariant under affine transformations, and (*ii*) for any number of variables n, the number of equivalence classes is significantly less than the number of Boolean functions. For logic synthesis applications, classification is useful, since having a combinatorial logic circuit to implement a function allows constructing circuits for all functions from the same equivalence class, by simply modifying the linear inputs of the circuit based on the affine equivalence relation.

Due to the recent developments in secure multi-party computation, fully-homomorphic encryption, and zero-knowledge proofs, circuits with fewer number of nonlinear gates has become more desirable. This promoted the design of symmetric primitives (e.g., Rasta [1], LowMC [2]), which inherently uses small number of `AND` gates. *Multiplicative complexity* (MC) of a Boolean function is defined to be the minimum number of `AND` gates necessary and sufficient to implement it with a circuit over the basis {`XOR`, `AND`, `NOT`}, and it is computationally hard to calculate even for small number of variables. In 2019, Çalık et al. [4] found the MC of all 6-variable Boolean functions. In 2017, Find et al. [3] studied Boolean functions with MC 1 and 2 by using the affine invariance property of MC and showed that Boolean functions with MC 1 are affine equivalent to x_1x_2, and Boolean functions with MC 2 are affine equivalent to one of the following functions: $x_1x_2x_3$, $x_1x_2x_3 + x_1x_4$ and $x_1x_2 + x_3x_4$.

In this work, we focus on Boolean functions with MC 3 and 4. For an n-variable Boolean function f, we define the dimension $dim(f)$ to be $n - l$, where l is the linearity dimension of f (i.e., the dimension of the set of its linear structures). Based on this, we show that a function with MC k can have dimension at most $2k$, and the MC of a function is at least $dim(f)/2$. We also present a new algorithm for finding the affine transformation between two functions if they are affine equivalent. Finally, we show that there are 24 equivalence classes with MC 3, and 1277 equivalence classes with MC 4.

References

[1] C. Dobraunig, M. Eichlseder, L.o Grassi, V. Lallemand, G. Leander, E. List, F. Mendel, C. Rechberger: Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit. CRYPTO 2018: 662-692

[2] M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, M. Zohner: Ciphers for MPC and FHE. EUROCRYPT 2015: 430-454

[3] M. G. Find, D. Smith-Tone, M. Sönmez Turan: The number of boolean functions with multiplicative complexity 2. IJICoT 4(4) 2017: 222-236

[4] Ç. Çalık, M. Sönmez Turan, R. Peralta: The multiplicative complexity of 6-variable Boolean functions. Cryptography and Communications 11(1) 2019: 93-107