Classification of Balanced Quadratic Functions

Lauren De Meyer, Begül Bilgin

imec - COSIC, ESAT, KU Leuven, Leuven, Belgium

S-boxes, typically the only nonlinear part of a block cipher, are the heart of symmetric cryptographic primitives. They have a significant impact on both the implementation characteristics and the cryptographic strength of an algorithm. Our work focuses on quadratic vectorial Boolean functions, since they tend to have low area requirements in hardware, especially for masked implementations or multi-party computation. New cryptographic algorithms should be designed with resistance against SCA in mind and we see this trend in recent proposals such as Keccak, LowMC, Ascon, ..., which all use quadratic functions as S-boxes. Also low-depth compositions of quadratic functions (such as the Prince and Present S-boxes) are popular in this context.

Many properties of a function stay invariant under affine equivalence. With gradually growing knowledge on Boolean functions and computational power, the Boolean functions with up to 6-bit inputs have all been classified between the fifties and 2003 [7, 1, 6]. For vectorial Boolean functions, only n-bit permutations for $n \leq 4$ have been completely classified so far [2, 5, 8]. Most of these classifications use the affine equivalence (AE) tool of Biryukov *et al.* [3]. Since the methods used in these works are unpractical for larger dimensions ($n > 4$), no classification of the complete space of 5-bit permutations exists. The quadratic ones alone have been classified by Bozilov *et al.* [4]. Their approach requires a runtime of a couple of hours, using 16 threads. Again, extending this approach to higher dimensions is not feasible.

In this work, we explore the extension of Biryukov's AE algorithm to non-bijective $n \times m$ functions with $m < n$ and analyse its performance. We propose a highly efficient algorithm that does not only classify all n-bit permutations, but also all balanced $n \times m$-bit functions for $m \leq n$. Our complexity is significantly lower than that of previous algorithms known to date. This allows us to generate all quadratic vectorial Boolean functions with five inputs in merely six minutes[1] and enables for the first time a complete classification of balanced 6-bit quadratic functions. These functions can be valuable for new cryptographic algorithm designs with efficient multi-party computation or side-channel analysis resistance as goal.

We also introduce a tool for finding length-two quadratic decompositions of permutations of higher degree and we use it to decompose the 5-bit AB and APN permutations. Furthermore, we find a set of high quality 5-bit permutations of degree 4 with small decomposition length that can be efficiently implemented.

When it comes to choosing S-boxes, designers can use our classification to pick quadratic components and use our (de)composition tool to create cryptographically strong low-depth S-boxes with efficient masked implementations. After the classifications of 4- and 5-bit permutations in previous works, this work expands the knowledge base on both classification and decomposition, bringing us one step closer to classifying 8-bit functions and decomposing the AES S-box using permutations instead of tower field or square-and-multiply approaches.

[1] E. Berlekamp and L. Welch. Weight distributions of the cosets of the (32, 6) Reed-Muller code. *IEEE Transactions on Information Theory*, 18(1):203–207, 1972.
[2] B. Bilgin, V. Nikov, S. Nikova, V. Rijmen, N. Tokareva, and V. Vitkup. Threshold Implementations of Small S-boxes. *Cryptography and Communications*, 7(1):3–33, 2015.
[3] A. Biryukov, C. De Canniere, A. Braeken, and B. Preneel. A toolbox for cryptanalysis: Linear and affine equivalence algorithms. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 33–50. Springer, 2003.
[4] D. Bozilov, B. Bilgin, and H. A. Sahin. A Note on 5-bit Quadratic Permutations' Classification. *IACR Transactions on Symmetric Cryptology*, 2(1):398–404, 2017.
[5] C. D. Cannière. *Analysis and Design of Symmetric Encryption Algorithms*. PhD thesis, Katholieke Universiteit Leuven, 2007.
[6] J. E. Fuller. *Analysis of affine equivalent boolean functions for cryptography*. PhD thesis, Queensland University of Technology, 2003. URL `http://eprints.qut.edu.au/15828/`.
[7] S. Golomb. On the classification of Boolean functions. *IRE transactions on circuit theory*, 6(5):176–186, 1959.
[8] M.-J. O. Saarinen. Cryptographic analysis of all 4× 4-bit S-boxes. In *International Workshop on Selected Areas in Cryptography*, pages 118–133. Springer, 2011.

[1] using a single thread on a 3.2 GHz Intel Core i5-6500 machine.