ANF Computation of Cryptographic Switching Functions using a Netlist Representation

David K. Houngninou
Dept. of Computer Science and Engineering
Texas A&M University
College Station, Texas, USA
DavidKebo@TAMU.edu

D. Michael Miller
Dept. of Computer Science
University of Victoria
Victoria, BC, Canada
MMiller@UVic.ca

Mitchell A. Thornton
Darwin Deason Institute for Cyber Security
Southern Methodist University
Dallas, Texas, USA
Mitch@SMU.edu

***Abstract*—Cryptographic primitives may be composed of, or modeled as collections of switching functions. We show that Algebraic Normal Form (ANF) coefficients can be recovered through traversals of a structural netlist. This method avoids the computationally prohibitive step of first extracting an alternative switching function representation to enable computation of the ANF. This method is particularly useful when the cryptographic primitive of interest is natively in the form of a combinational logic structural netlist. We present a technique whereby ANF coefficients can be extracted through traversals of a netlist of N gates or operators with a computational complexity of $O(N)$. The netlist representing the switching function of interest does not require any modification or pre-processing. We also provide a method for constructing a complete or partial netlist from a captured black box primitive. This technique is a highly advantageous alternative to other modern methods for computing the ANF, given that many modern cryptographic primitives can be too large to allow for practical computational processing runtimes or memory requirements.**

***Index Terms*—Cryptography, Security, Algebraic Normal Form (ANF), Switching Functions**

References

[1] Knudsen, L. R., “Truncated and Higher Order Differentials,” in proc. *Second International Workshop of Fast Software Encryption*, Lecture Notes in Computer Science 1008, Springer-Verlag pub., pp. 196–211, 1995.

[2] Khoo, K., Gong, G., and D. Stinson, “A New Characterization of Semi-bent and Bent Functions on Finite Fields,” in proc. *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 279–295, 2006.

[3] Meier, W. and Staffelbach, O., “Fast Correlation Attacks on Stream Ciphers,” in proc. *Advances in Cryptology*, EUROCRYPT’88, Lecture Notes in Computer Science 330, pp. 301–314, 1988.

[4] Dinur, I. and Shamir, A., “Cube Attacks on Tweakable Black Box Polynomials,” in *Cryptology*, ePrint Archive, Report 385, 2008.

[5] Blum, M., Luby, M., and Rubinfeld R., “Self-testing/correcting with Applications to Numerical Problems,” *Journal of Computer and System Sciences*, vol. 47, no. 3, pp. 549–595, 1993.

[6] Kaufman, T., and Sudan, M., “Algebraic Property Testing: The Role of Invariance,” in proc. *Ann. ACM Symp. on Theory of Computing*, pp. 403–412, May 17-20, 2008.

[7] Filiol, E., “A New Statistical Testing for Symmetric Ciphers and Hash Functions,” in proc. *4th International Conference on Information and Communications Security*, (ICICS ’02), Deng, R. H., Qing, S., Bao, F., and Zhou, J. (Eds.). Springer-Verlag Pub., London, UK, UK, pp. 342–353, 2002.

[8] McCarthy, P. J., **Introduction to Arithmetical Functions**, Springer-Verlag, New York, 1985, ISBN 0-367-96262-X.

[9] Thornton, M. A. and Miller, D. M., “On the Computation of Reed-Muller Spectra for Cryptography and Switching Theory Applications,” in proc. *Proceedings of the Workshop on Applications of the Reed-Muller Expansion in Circuit Design*, 2017.

[10] Drechsler, R., and Thornton, M. A., “Computation of Spectral Information from Logic Netlists,” in proc. *IEEE Int. Symp. on Multiple-Valued Logic*, pp. 53–58, 2000.

[11] Krenz, R., Dubrova, E., and Kuehlmann, A., “Fast Algorithm for Computing Spectral Transforms of Boolean and Multiple-Valued Functions on Circuit Representation,” in proc. *IEEE Int. Symp. on Multiple-Valued Logic*, pp. 334–339, 2003.

[12] Thornton, M. A., Drechsler, R., and Miller, D. M., **Spectral Techniques in VLSI CAD**, Kluwer Academic Publishers, Boston, Massachusetts, July 2001, ISBN 0-7923-7433-9.

[13] Thornton, M. A., **Modeling Digital Switching Circuits with Linear Algebra**, Morgan & Claypool Pub., San Rafael, California, April 2014, ISBN 9781627052337.

[14] Thornton, M. A., “Simulation and Implication using a Transfer Function Model for Switching Logic,” *IEEE Transactions on Computers*, vol. 64, no. 12, pp. 3580–3590, December 2015.

[15] Bakoev, V. P., “A Method for Fast Computing the Algebraic Degree of Boolean Functions,” in proc. *International Conference on Computer Systems and Technologies*, pp. 141-147, July 2020.

[16] Shannon, C. E., “The Synthesis of Two-Terminal Switching Circuits,” *Bell System Technical Journal*, vol. 28, no. 1, January 1949, pp. 59-98.

[17] Houngninou, D. K., “Implementation of Switching Circuit Models as Vector Space Transformations,” *Ph.D. dissertation, Dept. of Comp. Sci. and Engineering*, Southern Methodist University, December 16, 2017.

[18] McElvain, K., “ACM/SIGDA Benchmarks Electronic Newsletter DAC’93 Edition,” `https://people.engr.ncsu.edu/brglez/CBL/benchmarks/1993-Newsl-Brglez.txt` (accessed April 30, 2021), June 1993.

[19] Bryan, D., “The ISCAS’85 Benchmark Circuits and Netlist Format,” North Carolina State University, `https://www.davidkebo.com/documents/iscas85.pdf` (last accessed April 30, 2021), 1985.

[20] Brglez, F. and Fujiwara, H., “A Neutral Netlist of 10 Combinational Benchmark Circuits and a Target Translator in FORTRAN,” in proc. *IEEE Int. Symp. Circuits and Systems, Special Session on ATPG and Fault Simulation*, magnetic tape distribution, June 5-7, 1985.

[21] Houngninou, D. K. and Thornton M. A., “Implementation of Switching Circuit Models as Transfer Functions,” in proc. *IEEE Int. Symp. on Circuits and Systems*, May 22-25, 2016, pp. 2167-2170.

[22] Houngninou, D. K. and Thornton M. A., “Simulation of Switching Circuits using Transfer Functions,” in proc. *IEEE Midwest Symp. on Circuits and Systems*, August 6-9, 2017, pp. 511-514.