Standard Cell Design For Data-Independent Static Power Under Illumination

Jan Bělohoubek, Petr Fišer and Jan Schmidt
Czech Technical University in Prague
Prague, Czech Republic

{jan.belohoubek, petr.fiser, jan.schmidt}@fit.cvut.cz

Keywords. Static Power, Subthreshold Leakage, Optical Beam Induced Current (OBIC), CMOS, Standard Cell, SPICE, AES SBOX

Abstract

Physical attacks, namely invasive, observation, and combined, represent a great challenge for today's digital design. Successful class of strategies adopted by industry, allowing hiding data dependency of the side channel emissions in CMOS is based on balancing. Although attacks on CMOS dynamic power represent a class of state-of-the-art attacks, vulnerabilities exploiting data dependency in CMOS static power [1, 2, 3, 4] and light-modulated static power were recently presented [5, 6, 7].

In this contribution are presented the structures and techniques developed to enhance and balance the power imprint of the traditional static CMOS bulk structures under invasive light attack. The idea behind the balancing is to mimic the behavior of balanced inverter chains (see Figure 1) in a more complex CMOS cell. The microarchitecture of the proposed cells is inspired by the connection approximating the *Constant Current Source*.

The standard cell design was confirmed by SPICE simulations using the validated SPICE models for CMOS under *Photoelectric Laser Stimulation* (PLS) [8, 9].

The novel standard cells designed according to the presented techniques in the TSMC180nm technology node were used to synthesize the dual-rail AES SBOX block. The behavior of the AES SBOX block composed of the novel cells is compared to classical approaches. Usage of novel cells enhances circuit security under invasive light attacks while preserving comparable circuit resistance against state-of-the-art power attacks.

The models and resources used for this research are available online [10].

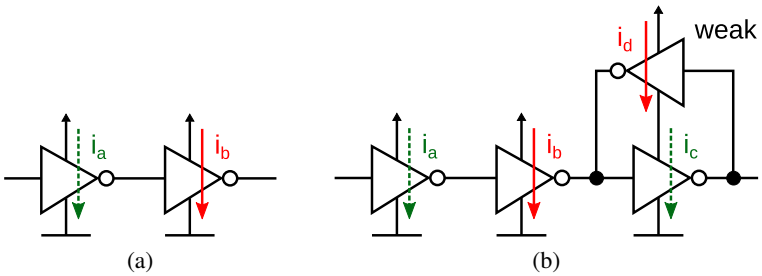

Figure 1: Two-inverter chain (a) uses complementary power consumption to obtain a constant power imprint: $i_a + i_b = const.$; three-inverter chain with feedback weak inverter (b) uses the same principle

Paper origin

This work has been accepted and presented at the 23rd International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS 2020), while the extended version of the original contribution is currently under review in the Microelectronics Reliability journal.

Acknowledgment

The authors acknowledge the support of the OP VVV MEYS funded project CZ.02.1.01/0.0/0.0/16_019/0000765 "Research Center for Informatics". Computational resources were supplied by the project "e-Infrastruktura CZ" (e-INFRA LM2018140) provided within the program Projects of Large Research, Development and Innovations Infrastructures. The novel structures presented in this paper are subject of the patent application.

References

[1] J. Giorgetti, G. Scotti, A. Simonetti, and A. Trifiletti, "Analysis of data dependence of leakage current in CMOS cryptographic hardware," in *Proceedings of the 17th ACM Great Lakes symposium on VLSI*. ACM, 2007, pp. 78–83.

[2] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage Power Analysis attacks: Well-defined procedure and first experimental results," in *2009 International Conference on Microelectronics - ICM*, Dec 2009, pp. 46–49.

[3] T. Moos, A. Moradi, and B. Richter, "Static Power Side-Channel Analysis – An Investigation of Measurement Factors," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2019.

[4] B. Fadaeinia, T. Moos, and A. Moradi, "BSPL: Balanced Static Power Logic." *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 558, 2020.

[5] J. Bělohoubek, P. Fišer, and J. Schmidt, "Using Voters May Lead to Secret Leakage," in *IEEE 22nd International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS 2019)*, April 2019, pp. 1–4.

[6] ——, "CMOS Illumination Discloses Processed Data," in *22nd Euromicro Conference on Digital System Design (DSD 2019)*, Aug 2019, pp. 381–388.

[7] ——, "Standard Cell Tuning Enables Data-Independent Static Power Consumption," in *23rd International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS 2020)*, Apr 2020.

[8] A. Sarafianos, R. Llido, O. Gagliano, V. Serradeil, M. Lisart *et al.*, "Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90nm technology," in *38th International Symposium for Testing and Failure Analysis, (ISTFA) 2012*, 2012, pp. 5B–5.

[9] A. Sarafianos, O. Gagliano, M. Lisart, V. Serradeil, J. Dutertre, and A. Tria, "Building the electrical model of the pulsed photoelectric laser stimulation of a PMOS transistor in 90nm technology," in *Proceedings of the 20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, July 2013, pp. 22–27.

[10] J. Bělohoubek. (2019 – 2021) Photoelectric Laser Stimulation of Combinational Logic. [Online]. Available: https://github.com/DDD-FIT-CTU/CMOS-PLS/