

A 7T Security Oriented SRAM Bitcell

Robert Giterman*, Osnat Keren*, and Alexander Fish*

Abstract—Power analysis (PA) attacks have become a serious threat to security systems by enabling secret data extraction through the analysis of the current consumed by the power supply of the system. Embedded memories, often implemented with six-transistor (6T) static random access memory (SRAM) cells, serve as a key component in many of these systems. However, conventional SRAM cells are prone to side-channel power analysis attacks due to the correlation between their current characteristics and written data. To provide resiliency to these types of attacks, we propose a security-oriented 7T SRAM cell, which incorporates an additional transistor to the original 6T SRAM implementation and a two-phase write operation, which significantly reduces the correlation between the stored data and the power consumption during write operations. The proposed 7T SRAM cell was implemented in a 28nm technology and demonstrates over $1000\times$ lower write energy standard deviation between write ‘1’ and ‘0’ operations compared to a conventional 6T SRAM. In addition, the proposed cell has a 39%–53% write energy reduction and a 19%–38% reduced write delay compared to other power analysis resistant SRAM cells.

Index Terms—Static random access memory (SRAM), Side-channel attacks (SCA), Differential power analysis (DPA).

I. INTRODUCTION

The use of cryptographic devices storing sensitive information has grown considerably during the last few decades and has become a crucial part of many applications, such as smart cards, and mobile devices. [1], [2]. Side channel analysis (SCA) is a powerful threat to these devices because it exploits the information related to the physical behavior of these devices to extract sensitive data [3], [4]. PA attacks are considered to be one of the most powerful types of SCA methods since they require relatively simple equipment and setups [3], [5]–[10]. PA attacks exploit the correlation between the instantaneous current consumed by the power supply of the device and its processed and stored data, to extract secret data or sensitive information.

Embedded memories dominate the area and power consumption of many VLSI system-on-chips (SoCs) [11], and are key components of many cryptographic systems, such as smart cards [12] and wireless networks employing cryptography algorithms [13], where they are used to store instruction code and data. Therefore, the analysis and design of secured memories is of utmost importance. Embedded memories are mostly implemented with the 6T SRAM macrocell, which provides high density, robust operation, and high performance. However, 6T SRAM arrays are traditionally designed and optimized for high density and performance, while their security properties are often overlooked, resulting in a high susceptibility to PA attacks.

Previous works have proposed modified SRAM bitcells to reduce the correlation between the dynamic power dissipation and the stored data of a conventional 6T SRAM array [14], [15]. Both of these solutions are based on a two-stage write

operation. During the first stage, the internal nodes of the SRAM cell (Q and QB) are pre-charged to a constant voltage to eliminate the correlation between the previously stored data, and the write operation that follows. In [14] the authors suggested performing the pre-charge operation by using two additional PMOS transistors beyond the original 6T SRAM in order to power-cut the supply during the additional pre-charge phase. In [15] the authors proposed a feedback-cut SRAM cell, composed of two additional NMOS devices which are used to cut off the feedback of the SRAM cell in order to avoid short-circuit power dissipation. While these solutions effectively reduce the correlation between the power consumption and stored data of the SRAM array, they result in significant delay and power overheads, as well as reduced static noise margins (SNMs).

In general, we assume that a side-channel attacker has access to the power supply lines of the system, and that he has knowledge of the chip architecture, including the memory organization, array peripherals and internal timing paths. In addition, it is assumed that the attacker can assign input vectors to the system, which can result in memory write operations to selected rows. Finally, it is common to assume that the overall current consumed by the memory macro peripherals and other chip components can be treated as algorithmic noise, which can be filtered out using enough current traces [3], [4], especially when the memory array is operated under a separate supply voltage [16], [17].

In this paper, we describe a novel security-oriented 7T SRAM cell design, which incorporates a two-phased write operation, and significantly reduces the correlation between the written and stored data in the memory and its power dissipation, thus providing a PA resilient memory. The proposed 7T cell includes an additional transistor to the original 6T SRAM implementation and a single power gate transistor per memory word, which are used to equalize the Q and QB voltages during the first phase of the write operation. Compared to other PA resistant memory solutions, the proposed cell provides 39%–53% lower energy dissipation, 19%–38% lower write delay, and the highest read and hold SNMs compared to other PA resilient memory solutions.

Outline: The rest of this paper is organized as follows. Section II provides a cell-level PA of a conventional 6T SRAM, demonstrating the correlation between its data and write energy consumption. Section III introduces the proposed 7T SRAM cell, analyses its properties and discusses its security at both a cell and array level PA. Section IV compares the proposed 7T SRAM cell to a conventional 6T SRAM and other PA resilient memory options, and Section V concludes the paper.

II. POWER ANALYSIS OF A 6T SRAM

In this section, to simplify the discussion, we start with a correlation analysis between the current consumed by the power supply of a 6T SRAM cell and the data that it stores. This discussion is extended to a more practical case where

R. Giterman, O. Keren, and A. Fish are with the Emerging Nanoscaled Integrated Circuits and Systems (EnICS) Labs, Faculty of Engineering, Bar-Ilan University, Ramat Gan, Israel (e-mail: robert.giterman@biu.ac.il)

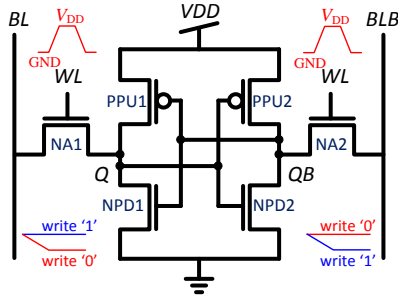


Fig. 1: Schematic representation of a 6T SRAM cell with illustrative write signal waveforms.

multiple cells are connected to the same power supply in section III.

A conventional 6T SRAM is shown in Fig. 1 with its signal waveforms during a write operation. To enable write access to the cell, the word line (WL) is asserted and the voltages on the bit-line pair (BL and BLB) are transferred to the internal storage nodes, Q and QB, respectively. When the written level differs from the value stored in the cell prior to the write event, the cell dissipates dynamic energy to charge the internal cell capacitances. In addition, the cell dissipates short circuit power since the access transistors (NA1 and NA2) must overcome the internal feedback of the cell (formed by transistors NPD1, PPU1, NPD2, and PPU2) to change its stored value. On the other hand, when the written value is similar to the stored data, no dynamic energy is dissipated by the cell and the total power consumption is dominated by its leakage currents. Fig. 2(a) depicts the current consumption during write '1' and '0' operations to a cell which previously stored a '0'. The current waveforms present a significant difference, with a peak current almost four orders of magnitude lower during the write '0' ($0.14 \mu\text{A}$) operation than the write '1' operation ($100 \mu\text{A}$), due to the changed state of the cell which previously stored a '0'. The energy distributions obtained from a full write cycle are shown in Fig. 2(b), as extracted from 1000 Monte-Carlo (MC) simulations including device mismatch and process variations in 28 nm CMOS technology. As expected, the write energy dissipated during the write '0' operation was over two orders of magnitude lower than the energy dissipated during a write '1' operation. The mean energy dissipations for write '1' and '0' were 1.475 fJ and 0.016 fJ , respectively. The significant difference between the energy dissipations obtained from the different write operations to the cell indicate that the power consumption of the 6T SRAM is highly dependent on the written data to the cell, making it highly susceptible to PA attacks.

III. POWER ANALYSIS RESISTANT 7T SRAM

To overcome the information leakage of the 6T SRAM cell during write operations, we propose a modified 7T SRAM cell employing a two-phase write operation consisting of an equalization and write phases, and resulting in a significantly lower correlation between its current dissipation and the stored data in the cell.

A. Basic Operation

The schematic representation of the proposed 7T SRAM cell is shown in Fig. 3. A power gate PMOS transistor (PG) is

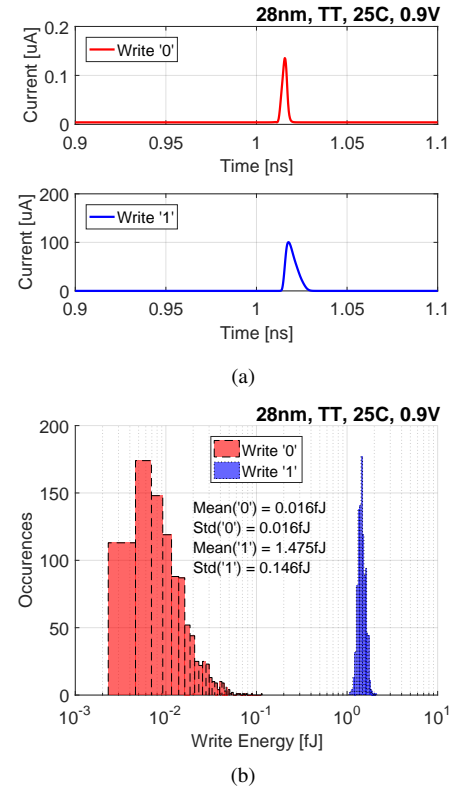


Fig. 2: (a) Current consumed during write '1' and '0' operations to a 6T SRAM. (b) Write energy distribution of a 6T SRAM during write operations under process variations.

used to disable the voltage supply of an entire memory word (VVDD) to avoid short-circuit power dissipation during the equalization phase of the write operation. Transistor PPC is added to the original 6T SRAM implementation to short Q and QB during the equalization phase. A PC signal is used to disable PG and enable PPC to perform voltage equalization between Q and QB using charge-sharing, hence avoiding additional power consumption from the supply. During the second phase of the write operation, PC is discharged to charge VVDD and cut off PPC, and charged to enable the NMOS access transistors (NA1 and NA2) allowing them to pass the data from BL and BLB to Q and QB, respectively, to complete the write operation

A waveform demonstration of the two-phased write operation is depicted in Fig. 4, showing how a write '1' operation is made to a cell which previously stored a '0'. The internal Q and QB voltages of a conventional 6T SRAM cell are shown for comparison. First, the PC voltage is asserted to cut off the supply voltage of all the cells in a single word. As a result, VVDD is decreased and the internal Q-7T and QB-7T voltages are equalized using charge-sharing. Then, the PC signal is de-asserted to resume the VVDD supply, and the WL is asserted to enable write access to the cell. BL and BLB, already set to V_{DD} and GND , respectively, are then transferred to Q-7T and QB-7T to complete the write '1' operation. For comparison, the internal voltages of a conventional 6T cell (Q-6T and QB-6T) are only changed when the WL has been asserted, resulting in a significant energy difference between write '1' and '0' operations.

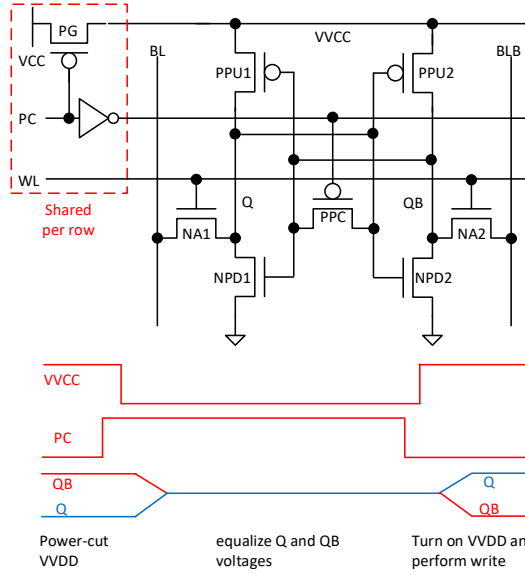


Fig. 3: Proposed 7T SRAM cell and basic operation.

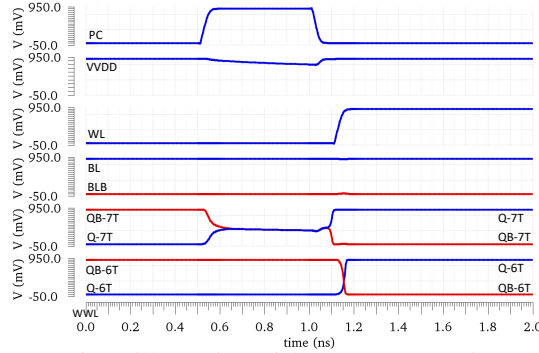


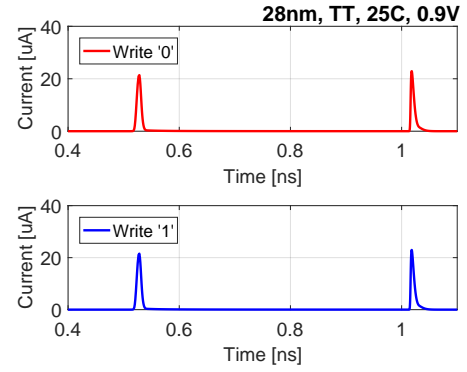
Fig. 4: Waveform illustration of the 7T SRAM write operation.

B. Power Analysis

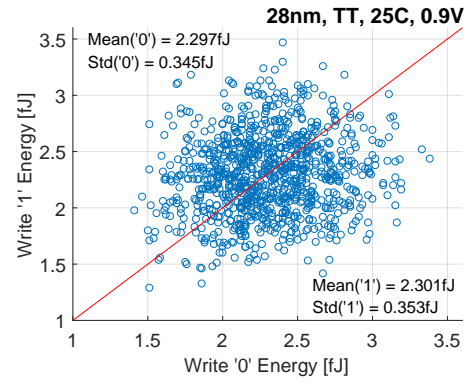
Due to the symmetric structure of the 7T cell, the current consumed during the equalization phase is independent of the data previously stored in the cell. Moreover, the cell does not consume additional energy during this phase since VDD is cut off and the voltages on Q and QB are equalized through charge sharing; hence, the power consumption prior to the WL assertion is identical when either '1' or '0' were previously stored in the cell.

The currents dissipated by the 7T SRAM cell during the write '1' and '0' operations to a cell previously storing a '0' are shown in Fig. 5(a), resulting in almost identical waveforms due to the two-phase write operation, thus demonstrating the lack of current information leakage. The corresponding write energy scatter plot of the 7T SRAM cell is shown in Fig. 5(b), as extracted from 1000 MC simulations including device mismatch and process variations. As expected, the mean energy dissipations for the write '0' and '1' operations are 2.297 fJ and 2.301 fJ with a standard deviation of 0.0345 fJ and 0.353 fJ, respectively, thus resulting in a much smaller difference than similar distributions obtained for the 6T SRAM cell.

The correlation between the write energy dissipation and the stored data can be generalized to obtain the overall energy consumption of an m -bit word stored in a memory row. For



(a)



(b)

Fig. 5: (a) Current consumed during write '1' and '0' operations to the 7T cell. (b) Write energy distribution of the proposed 7T SRAM during a write operation under process variations.

an m -bit word stored in array, the total energy dissipation depends linearly on the Hamming weight of the stored data, given by

$$E_{word} = H_w \cdot E_C + (m - H_w) \cdot E_{NC} \quad (1)$$

where m is the word length, E_C and E_{NC} are the write energy dissipations when the data stored in the cell is changed or unchanged, respectively, and H_w is the Hamming weight of the word, which equals the Hamming distance between the word value and the BL voltages, given by

$$H_w = HD(BL, Q) = \sum_i (BL_i \neq Q_i) \quad (2)$$

To evaluate the security of a 32bit memory word, write simulations of the 32 different H_w values were applied to the 7T and 6T SRAM cells, and the standard deviations between the current traces were computed. This methodology is commonly used to estimate the magnitude of the information leakage [15], [18]¹. The obtained standard deviation curves are depicted in Fig. 6. The maximal deviation for the 7T SRAM cell was 1.1 μ A, which is almost three orders of magnitude lower than that found for the 6T SRAM cell at 875 μ A. The same analysis was repeated for the power-cut [14] and

¹Information leakage enables the reduction of the entropy of the memory word, which is defined as the base-2 logarithm of all possible 32-bit data combinations.

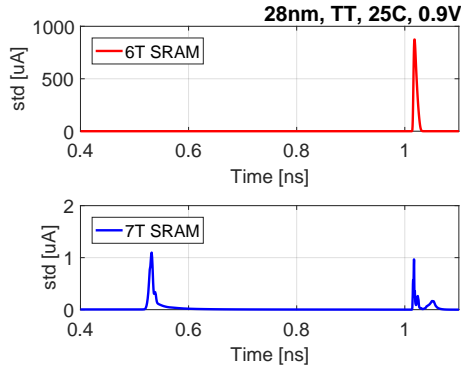


Fig. 6: Standard deviation of the current consumption of the 6T and 7T SRAM cells during a write cycle for different H_w values.

feedback-cut [15] bitcells, resulting in similar maximal deviations compared to the 7T cell, at 2.1 μ A and 0.99 μ A, respectively.

IV. CELL PROPERTIES AND COMPARISON

Table I compares the key features of the proposed 7T cell and other SRAM cells, including a conventional 6T, a power-cut 8T [14], and a feedback-cut 8T [15], which are the only power-analysis resistant SRAM cells published in literature, to the best of our knowledge. The simulations were made on 128×32 memory arrays of the considered bitcells, including the parasitic capacitances of the array control lines, as extracted from the layout of the cells. All simulations were conducted using 28 nm CMOS technology models under a 900 mV supply voltage at room temperature.

A. Area Analysis

The layouts of the proposed 7T and the conventional 6T SRAM cells are shown in Fig. 7. The additional PPC transistor is placed between the pull-up devices to preserve its symmetric structure, albeit extending the vertical pitch of the cell compared to the 6T SRAM. The WL, PC, and VVCC signals are routed horizontally using M2, while GND, BL, and BLB are routed vertically using M3. Note that the PC poly layer must cut the diffusions of Q and QB in order to avoid an additional poly-to-poly spacing requirement, resulting in the creation of parasitic MOS capacitors between PC and Q/QB. The 7T cell was measured at $1.1 \mu\text{m} \times 0.52 \mu\text{m}$, which is 78% larger than the 6T SRAM cell. The areas of the power-cut and feedback-cut 8T SRAM cells are 81% and 40% larger than the 6T SRAM area, respectively.

B. Security Analysis

In order to evaluate the security improvement of the considered cells over a conventional 6T SRAM, the mean energy difference (MED) between the energies consumed during write '1' and write '0' operations, as extracted from 1000 MC simulations, was evaluated. Fig. 2(b) illustrates that the MED of the 6T SRAM is 1.46 fJ, while, according to Fig. 5(b), the MED of the proposed 7T SRAM is only 0.004 fJ. A similar analysis was performed on the power-cut and feedback-cut 8T SRAM cells, achieving an MED of 0.0051 fJ and 0.0043 fJ, respectively.

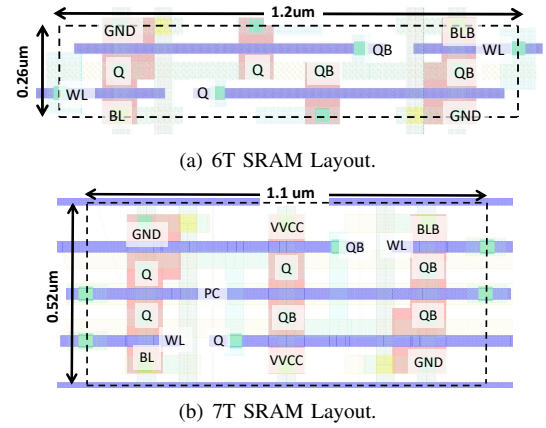


Fig. 7: Cell layouts in 28 nm CMOS technology.

C. Energy Analysis

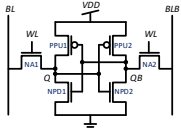
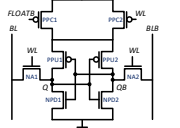
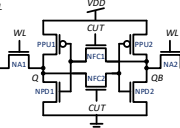
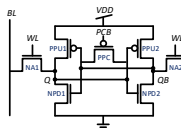
The write energy consumption of the power-cut and feedback-cut 8T SRAM cells is mainly dominated by the switching activity on the highly capacitive BL and BLB, which are used to pre-charge Q and QB during the first phase of the write operation, in order to drive Q and QB to the required voltages during the second phase. In addition, the FLOATB and CUT signals must be toggled to cut off the power supply and feedback of the power-cut and feedback-cut 8T cells, respectively. Due to the larger dimensions of the power-cut cell it dissipates more energy than the feedback-cut cell: 7.15 pJ compared to 5.52 pJ. For the proposed 7T cell, the write energy consumption is composed of charging the PC signal during the first phase of the write operation to cut off the supply of the cell and equalize Q and QB voltages using charge-sharing, hence avoiding the charging of BL and BLB during this phase, and resulting in a reduced energy consumption compared to the power-cut and feedback-cut cells. For the second write phase, the PC signal is discharged and WL is enabled, passing the voltages of BL and BLB to Q and QB, respectively. The write energy dissipation of the 7T cell was 3.49 pJ, which is 39%–53% lower than the write energies of the other PA resilient cells, and 57% higher than the conventional 6T SRAM.

During standby, the feedback-cut cell exhibits the highest leakage power dissipation due to the V_T drop across NFC1\NFC2, which is over 80% higher than the proposed 7T cell.

D. Delay Analysis

The write delay of the considered memory options was defined as the minimum required time to perform the two-phased write operation. As with the energy comparison, the requirement of the power-cut and feedback-cut cells to charge the highly capacitive BL and BLB signals to perform the pre-charge phase resulted in increased write delays compared to the 7T cell, which only requires toggling the row-wise PC and WL signals. As a result, the 7T cell achieved a 19%–38% reduced write delay compared to the power-cut and feedback-cut cells. On the other hand, the additional equalization phase and increased cell dimensions resulted in a 56% longer write delay compared to the conventional 6T cell.

TABLE I: Comparison of SRAM cells

Cell type	Conventional 6T SRAM	Power-cut 8T SRAM [14]	Feedback-cut 8T SRAM [15]	Proposed 7T SRAM
Cell structure				
Cell size	0.32 μm^2	0.58 μm^2	0.45 μm^2	0.57 μm^2
PA resiliency (MED)	1.46 fJ	0.0051 fJ	0.0043 fJ	0.004 fJ
Write energy	2.09 pJ	7.56 pJ	5.86 pJ	3.6 pJ
Write delay	333 ps	904 ps	701 ps	569 ps
Read SNM	287 mV	121 mV	252 mV	281 mV
Hold SNM	392 mV	385 mV	376 mV	387 mV
Leakage power	5.6 nW	5.8 nW	12.9 nW	7.1 nW

All the results are in 28 nm technology.
The energy and delay simulations are based on 128×32 array structures.

E. Stability Analysis

The read and hold SNMs of the SRAM cells were extracted by finding the maximal square that resides inside the “butterfly curves”, a metric introduced by Seevinck in [19]. The proposed 7T cell achieved 67% and 11% higher read SNM than the power-cut and feedback-cut SRAM cells, respectively. The low read SNM of the power-cut cell is due to the power gate devices which are integrated inside the bitcell and limit the supply current used to retain the data in the cell. The read SNM of the feedback-cut cell is limited because Q and QB cannot be charged to their maximal value as a result of the V_T drop across the feedback-cut NMOS transistors. As expected, the hold SNM of all the considered bitcells was higher than their read SNM, with the proposed 7T SRAM achieving the highest hold SNM among the security oriented bitcells.

V. CONCLUSIONS

Embedded memories, implemented with 6T SRAM macros, occupy a large portion of cryptographic systems and may hold secret data; these require special design precautions to provide resiliency to PA attacks. In this paper, we proposed a novel 7T SRAM cell composed of an additional PMOS transistor added to the original 6T SRAM implementation, and employing a two-phase write operation to significantly reduce the correlation between the consumed energy and the written data. The proposed 7T SRAM cell achieves over $1000\times$ decreased energy correlation compared to the conventional 6T SRAM. In addition, using a voltage equalization mechanism during the pre-charge phase of the write operation, the proposed 7T SRAM cell achieves 39%–53% lower energy dissipation and 19%–38% lower write delay than other PA resilient SRAM bitcells.

REFERENCES

- [1] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, “Extracting secret keys from integrated circuits,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.
- [2] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom, “Ecdsa key extraction from mobile devices via nonintrusive physical side channels,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 1626–1638.
- [3] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, “Introduction to differential power analysis,” *Journal of Cryptographic Engineering*, vol. 1, no. 1, pp. 5–27, 2011.
- [4] S. Mangard and A. Y. Poschmann, *Constructive Side-Channel Analysis and Secure Design*. Springer, 2015.
- [5] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, “Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 2, pp. 355–367, 2010.
- [6] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Trifiletti, “Effectiveness of leakage power analysis attacks on dpa-resistant logic styles under process variations,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 2, pp. 429–442, 2014.
- [7] I. Levi, O. Keren, and A. Fish, “Data-dependent delays as a barrier against power attacks,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 8, pp. 2069–2078, 2015.
- [8] M. Avital, I. Levi, O. Keren, and A. Fish, “Cmos based gates for blurring power information,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 7, pp. 1033–1042, 2016.
- [9] M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish, “Dpa-secured quasi-adiabatic logic (sqal) for low-power passive rfid tags employing s-boxes,” *IEEE Trans. on Circuits and Systems*, vol. 62, no. 1, pp. 149–156, 2015.
- [10] R. Gitterman, M. Vicentowski, I. Levi, Y. Weizman, O. Keren, and A. Fish, “Leakage power attack-resilient symmetrical 8t sram cell,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, no. 99, pp. 1–5, 2018.
- [11] ITRS, “International Technology Roadmap for Semiconductors - 2015 Edition,” 2015. [Online]. Available: <http://www.itrs2.net>
- [12] M. Neve, E. Peeters, D. Samyde, and J.-J. Quisquater, “Memories: a survey of their secure uses in smart cards,” in *Security in Storage Workshop, 2003. SISW'03. Proceedings of the Second IEEE International*. IEEE, 2003, pp. 62–62.
- [13] W. Liu, R. Luo, and H. Yang, “Cryptography overhead evaluation and analysis for wireless sensor networks,” in *Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on*, vol. 3. IEEE, 2009, pp. 496–501.
- [14] E. Konur et al., “Power analysis resistant sram,” in *2006 World Automation Congress*. IEEE, 2006, pp. 1–6.
- [15] V. Rožić et al., “Design solutions for securing sram cell against power analysis,” in *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*. IEEE, 2012, pp. 122–127.
- [16] B. Zimmer, S. O. Toh, H. Vo, Y. Lee, O. Thomas, K. Asanovic, and B. Nikolic, “Sram assist techniques for operation in a wide voltage range in 28-nm cmos,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 59, no. 12, pp. 853–857, 2012.
- [17] M.-H. Chang, Y.-T. Chiu, and W. Hwang, “Design and iso-area vmin analysis of 9t subthreshold sram with bit-interleaving scheme in 65-nm cmos,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 59, no. 7, pp. 429–433, 2012.
- [18] M. Renauld, D. Kamel, F.-X. Standaert, and D. Flandre, “Information theoretic and security analysis of a 65-nanometer ddsll aes s-box,” in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2011, pp. 223–239.
- [19] E. Seevinck et al., “Static-noise margin analysis of mos sram cells,” *Solid-State Circuits, IEEE Journal of*, vol. 22, no. 5, pp. 748–754, 1987.