A 7T Security Oriented SRAM Bitcell

1.1 Base paper 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 28 nm technology and demonstrates over 1000× 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.

1.2 Enhancement of this project:

- To design a 7T SRAM bit cell in 22nm CMOS technology in TANNER EDA Software with single bit and 8-bit level operations with compared to existing 6T SRAM bit cell in terms of area, delay and power leakage.

1.3 Proposed title:

CMOS Implementation of Low Power and High Security Data Information using 7T SRAM Bit cell

1.4 Proposed Abstract:

In recent method of Cryptographic application based devices which have more sensitive information with more crucial part of storing and retrieving the data. Thus its affect with power analysis and side channel analysis its exploit correlation between the instantaneous current consumed power supply devices with information leakages. In this work will describe a novel security oriented 7T SRAM cell design, which incorporates a two-phased write operations and significantly reduces the correlation between the written and stored data in the memory and its power dissipation, thus its providing a power analysis resilient memory. This proposed 7T cell includes an additional transistor to the existing 6T SRAM implementation with single power gate transistor per memory. Here, this proposed work will design a 7T

SRAM bit cell in 22nm CMOS technology in TANNER EDA Software with single bit and 8-bit level operations with compared to existing 6T SRAM bit cell in terms of area, delay and power leakage.

1.5 **Existing system:**

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. 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 . PA attacks are considered to be one of the most powerful types of SCA methods since they require relatively simple equipment and setups. 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) and are key components of many cryptographic systems, such as smart cards and wireless networks employing cryptography algorithms , 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. Both of these solutions are based on a two-stage writeoperation. 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 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 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 shortcircuit 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, especially when the memory array is operated under a separate supply voltage.

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.

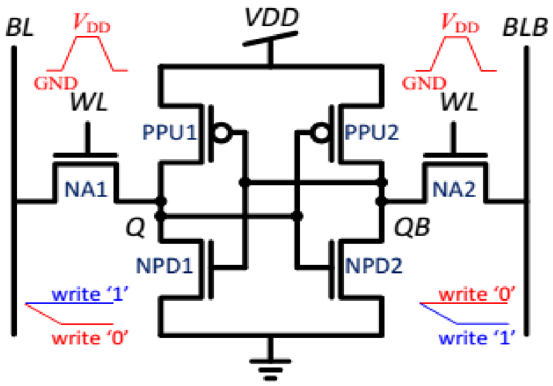

Figure 1: Schematic representation of 6T SRAM.

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.5 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 µA) operation than the write ‘1’ operation (100 µA), due to the changed state of the cell which previously stored a ‘0’.

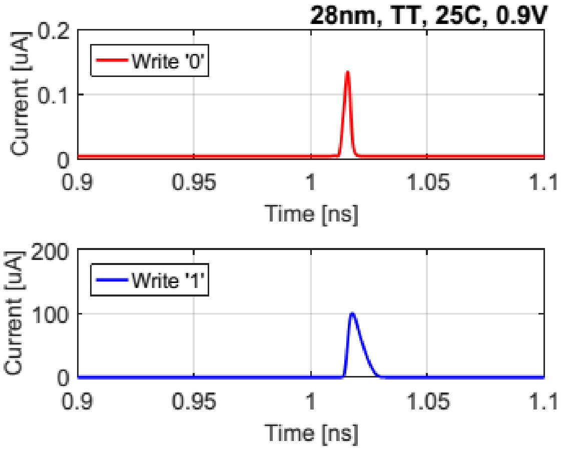

Figure 2: Current consumed during write ‘1’ and ‘0’ operations to a 6T SRAM.

The energy distributions obtained from a full write cycle are shown in Fig. 3, 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.

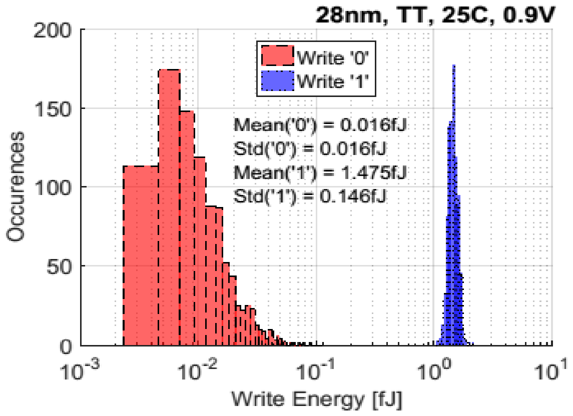

Figure 3: Write energy distribution of a 6T SRAM during write operations under process variations.

1.6 Disadvantage:

- High area occupied and more delay.
- Power analysis attack is high.
- High energy Dissipation.

1.7 Proposed System:

1.7.1 SRAM:

SRAM is semiconductor memory cell. It stores one bit of information. It is faster and consumes very less power as compared to other memory cells. Due to its robustness and stability, researchers are interested in further improvement of SRAM cell. SRAM is vital component in a chip or microprocessor IC. Designing a SRAM cell in nano scale regime has become a challenging task because of reduction in noise margins and increased sensitivity to threshold voltage variation . 10T SRAM cell performs better then 6T SRAM cell in terms of reliability and stability. 6T SRAM cell has less reliability at low supply voltage due to degradation in noise margins.

1.7.2 Power Analysis Based Side Channel Attack

Power analysis is a branch of side channel attacks where the side channel used is the power consumption. In electronic devices, the instantaneous power consumption is dependent on the data that is being processed in the device as well as the operation performed by that device . Therefore by analysing the power consumed by a device when it is doing encryption or decryption the key can be deduced. There are two types of power analysis: differential power analysis (DPA) and simple power analysis (SPA).

1.7.3 **SPA**

Simple power analysis is a method of side-channel attack that examines a chip's current consumption over a period of time. Since different operations will exhibit different power profiles, one can determine what type of function is being performed at a given time. For example, one can distinguish a multiplication function from an addition function, since multiplication consumes more current than addition. Also, when reading data from a memory, the ratio of 1's vs. 0's will be reflected in the power profile. SPA is useful when data-dependent features in the power traces are apparent. It may not be practical if there is significant noise in the system. In which case, DPA would be more advantageous.

1.7.4 **DPA**

Differential power analysis is a statistical method for analyzing power consumption to identify data-dependent correlations. This approach takes multiple traces of two sets of data, then computes the difference of the average of these traces. If the difference is close to zero, then the two sets are not correlated. If the sets are correlated, then the difference will be a non-zero number. Given enough traces, even tiny correlations can be seen, regardless of how much noise is in the system, since the noise will effectively cancel out during the averaging.

1.7.5 **Countermeasure**

Side-channel attacks, such as DPA and SPA, are dangerous because they allow hackers to circumvent conventional hardware and software security measures. DPA can accomplish in minutes or days what cryptoanalysis and other brute force methods cannot. Also, since they are non-invasive, they do not leave a trace, allowing for attackers to steal confidential information without being detected. Therefore, measures must be taken to prevent such attacks.

1.7.6 **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.

1.7.6.1 Basic Operation

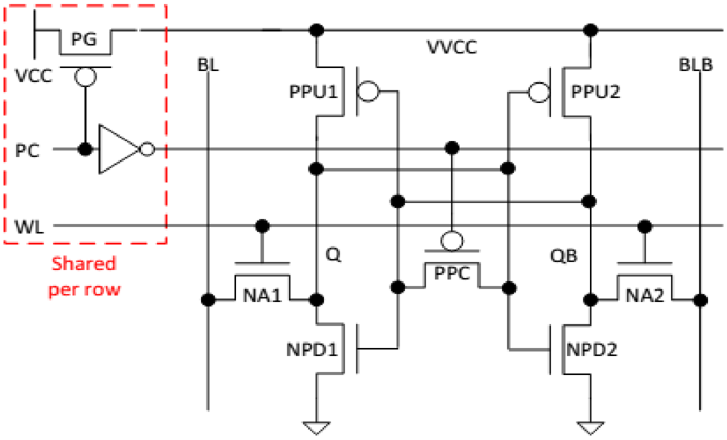

Figure 4: Proposed 7T SRAM.

The schematic representation of the proposed 7T SRAM cell is shown in Fig. 4. A power gate PMOS transistor (PG) is 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. 5, 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 deasserted to resume the VVDD supply, and the WL is asserted to enable write access to the cell. BL and BLB, already set to VDD 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.

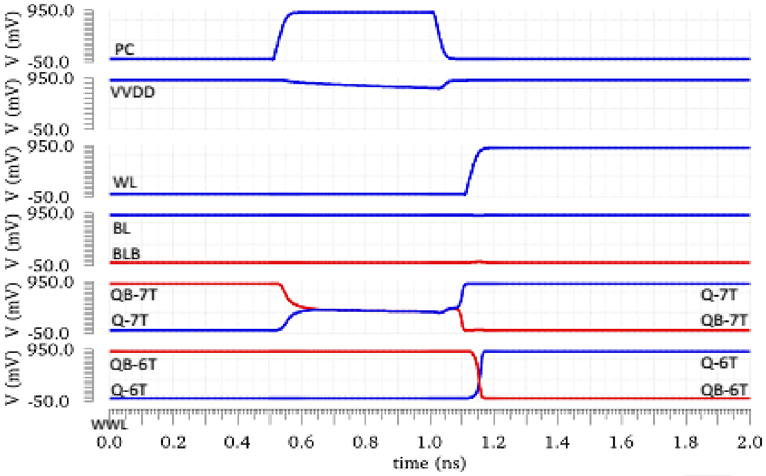

Figure 5:Waveform of 7T SRAM during Write operation.

1.7.7 **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 VVDD 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.

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. 6, 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. 7, 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.

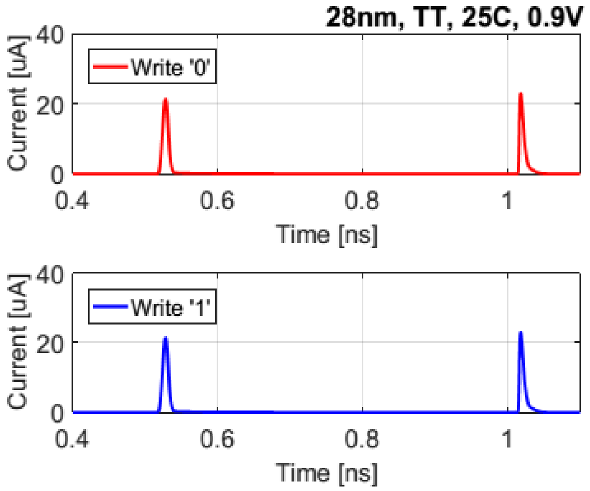

Figure 6: Current consumed during write '1' and '0' operations to the 7T cell.

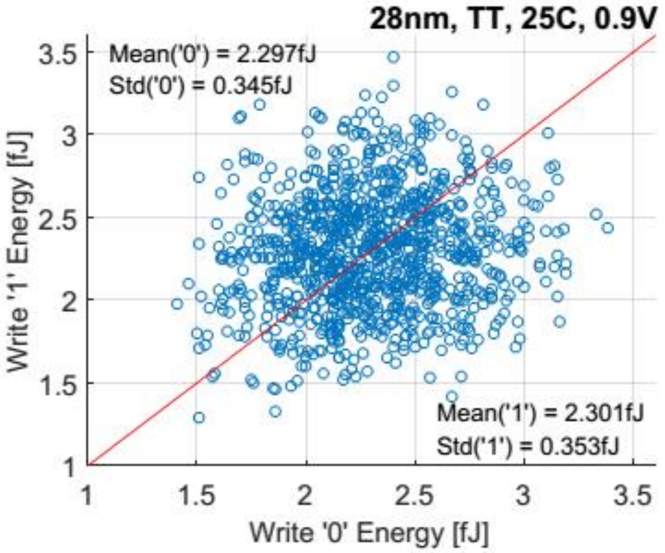

Figure 7 :Write energy distribution of the proposed 7T SRAM during a write operation under process variations.

1.8 **Advantage :**

- Low Area .
- Low energy Consumption.
- Reduction in power analysis attack.

Literature survey:

- A 7T Security Oriented SRAM Bit cell Robert Giterman , Osnat Keren , and Alexander Fish 1549-7747 2018 IEEE. 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 28 nm technology and demonstrates over 1000× 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.

- Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits Massimo Alioto, Senior Member, IEEE, Luca Giancane, Student Member, IEEE, Giuseppe Scotti, and Alessandro Trifiletti,1549-8328 2010 IEEE.In this paper, a novel class of power analysis attacks to cryptographic circuits is presented. These attacks aim at recovering the secret key of a cryptographic core from measurements of its static (leakage) power. These attacks exploit the dependence of the leakage current of CMOS integrated circuits on their inputs (including the secret key of the cryptographic algorithm that they implement), as opposite to traditional power analysis attacks that are focused on the dynamic power. For this reason, this novel class of attacks is named “Leakage Power Analysis” (LPA). Since the leakage power increases much faster than the dynamic power at each new technology generation, LPA attacks that is based on a solid theoretical background is presented. Advantages and measurement issues are also analyzed in comparison with traditional power analysis attacks based on dynamic power measurements. Examples are provided for various circuits, and an experimental attack to a register is performed for the first time. An analytical model of the LPA attack result is also provided to better understand the effectiveness of this technique. The impact of technology scaling is explicitly addressed by means of a simple analytical model and Monte Carlo simulations. Simulations on a 65- and 90-nm technology and experimental results are presented to justify the assumptions and validate the leakage power models that are adopted.

- Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations Massimo Alioto, Simone Bongiovanni, Milena Djukanovic, Giuseppe Scotti, and Alessandro Trifiletti 1549-8328 2013 IEEE.This paper extends the analysis of the effectiveness of Leakage Power Analysis (LPA) attacks to cryptographic VLSI circuits on which circuit level countermeasures against Differential Power Analysis (DPA) are adopted. Security metrics used for assessing the DPA-resistance of crypto core implementations, such as the minimum number to disclosure (MTD) and the asymptotic correlation coefficient, have been extended to the case of LPA. The LPA-resistance has been evaluated in terms of MTD as a function of the on chip noise. Noise variances up to 10000 times greater than the signal variance have been taken into account and LPA attacks have been successfully executed for all the logic styles under analysis using less than 100000 measurements. Moreover the role of process variations has been investigated through extensive Monte Carlo simulations in order to evaluate their impact on the leakage model for the logic styles under analysis. Results show that LPA attacks can be successfully carried out on the different anti-DPA logic styles even in presence of process variations. To the best of our knowledge, this work proves for the first time the effectiveness of LPA attacks in a real scenario where on chip noise and process variations are taken into account.

- Leakage Power Attack-Resilient Symmetrical 8T SRAM Cell Robert Giterman , Maoz Vicentowski, Itamar Levi , Yoav Weizman, Osnat Keren , and Alexander Fish 1063-8210 2018 IEEE. Power analysis attacks have become a serious threat to security systems by enabling secret data extraction using side-channel leakage information. Embedded memories, often implemented with 6T SRAM cells, serve as a key component in many of these systems. However, conventional SRAM cells are prone to side-channel leakage power attacks. To provide resiliency to these types of attacks, we propose a symmetric 8T SRAM cell which incorporates two more transistors than the conventional 6T cell to significantly reduce the correlation between the stored data and the leakage currents. To demonstrate the improved security of the suggested memory array, both cells were implemented in a 65-nm CMOS technology. Simulation results, including Monte Carlo analysis and signal-to-noise ratio comparison, illustrate the resiliency of the 8T cell to leakage power attacks.

- Design Solutions for Securing SRAM Cell Against Power Analysis Vladimir Roziˇ c´∗, Wim Dehaene† and Ingrid Verbauwhede 978-1-4673-2340-6/12/$31.00 c 2012 IEEE. Side channel attacks exploit physical imperfections of hardware to circumvent security features achieved by mathematically secure protocols and algorithms. This is achieved by monitoring physical quantities, usually power consumption or electromagnetic radiation, which contain information about the secret data. As a countermeasure, several circuit styles have been proposed for designing side-channel resistant logic gates and flip-flops. However, little effort has been made to develop secure memory arrays. An SRAM cell with 8 transistors has been proposed in order to obtain power analysis resistance by using a dual-rail precharge principle, the same technique used in various secure logic styles. In this paper we look into the practical aspects of this cell such as noise margins, layout strategy and read current. In addition, we propose alternative solutions for poweranalysis resistant SRAM. We compare these solutions in terms of data stability, delay and side-channel resistance.

- SRAM Assist Techniques for Operation in a Wide Voltage Range in 28-nm CMOS Brian Zimmer, Student Member, IEEE, Seng Oon Toh, Member, IEEE, Huy Vo, Yunsup Lee, Student Member, IEEE, Olivier Thomas, Krste Asanovic,´ Senior Member, IEEE, and Borivoje Nikolic,´ Senior Member, IEEE 1549-7747 2013 IEEE. Reducing static random-access memory (SRAM) operational voltage (Vmin) can greatly improve energy efficiency, yet SRAM Vmin does not scale with technology due to increased process variability. Assist techniques have been shown to improve the operation of SRAM, but previous investigations of assist techniques at design time have either relied on static metrics that do not account for important transient effects or make specific assumptions about failure distributions. This paper uses importance sampling of dynamic failure metrics to quantify and analyze the effect of different assist techniques, array organization, and timing on Vmin at design time. This approach demonstrates that the most effective technique for reducing SRAM Vmin is the negative bitline write assist, resulting in a Vmin of 600 mV for a 28-nm LP process in the typical corner.

- Design and Iso-Area Vmin Analysis of 9T Subthreshold SRAM With Bit-Interleaving Scheme in 65-nm CMOS Ming-Hung Chang, Student Member, IEEE, Yi-Te Chiu, and Wei Hwang, Fellow, IEEE 1549-7747 2012 IEEE. In this brief, a 9T bit cell is proposed to enhance write ability by cutting off the positive feedback loop of a static random-access memory (SRAM) cross-coupled inverter pair. In read mode, an access buffer is designed to isolate the storage node from the read path for better read robustness and leakage reduction. The bit-interleaving scheme is allowed by incorporating the proposed 9T SRAM bit cell with additional write wordlines (WWL/WWLb) for soft-error tolerance. A 1-kb 9T 4-to-1 bitinterleaved SRAM is implemented in 65-nm bulk CMOS technology. The experimental results demonstrate that the test chip minimum energy point occurs at 0.3-V supply voltage. It can achieve an operation frequency of 909 kHz with 3.51-μW active power consumption.

Reference:

[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. Giterman, 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. Roziˇ c´ 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.