International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 08 | August - 2022 Impact Factor: 7.185 ISSN: 2582-3930

A 7T SECURITY ORIENTED SRAM BITCELL

C.Durga Tejaswi, M.Nithesh kumar[2],N.Vineeth[2], V.Srinivasulu Reddy[2],V.Ananth Babu[2].

[1]Assistant Professor, Department of ECE, Narayana Engineering College, Gudur, AP, 524101.
[2]UG Student, Department of ECE, Narayana Engineering College, Gudur, AP,524101.

[1]drpr1197@gmail.com, [2]vineethrisk8500@gmail.com

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.

***Key Words*:** Power Analysis, SRAM Design, 6T SRAM, 7T SRAM, Power Dissipation

Software Tools:

- Tanner eda Tool

1.INTRODUCTION

A major part of the chip is SRAM, which is expected to be used extensively in high-performance servers and handheld computers. In order to achieve better efficiency and longer battery life for mobile applications, low power SRAM plays a major role . Main power is absorbed in the SRAM by data lines, bit lines and peripherals. The active energy use of these products . Almost 50 percent of the power is dissipated by bit lines during a write process of the overall complex power consumption . Application strategies for low-power SRAM are primarily dependent on lowering energy consumption. The largest capacitive components of the memory are data lines, bit lines, and word lines. In several implementations the use of computers for the storage of classified and confidential details has expanded . Critical knowledge extortion by side channel attacks (SCAs) is an important danger to these devices . Power testing refers to the kinds of side channel attacks that use the information processed which leaks during system power dissipation. In the energy study, the association between system power use and stored data is used. Because it has become a grave threat to the safety of cryptographic systems for PA technology to extract valuable information using system power dynamic properties, several papers have revealed the effectiveness of the leakage power analysis on Structures based and more deeply scaled technologies[8]. power analysis attacks on logic circuits as well as the construction of protected logic, the design of stable memory structures and review of power attacks on embedded memories is emphasized. In several cases, embedded storages are introduced with a 6-transistor (6T) SRAM array that occupies the region and strength of many VLSI system-on chips. In several cryptographic systems including smart cards and network devices with cryptographic algorithms , the 6T SRAM array serves as a main component. SRAM arrays for storing instruction code and data are used in these programmers. The study and development of secured experiences must also be carried out with the greatest possible consideration.

SRAM continues to be an important building block of system-on-a-chips (SoCs). The low-power feature for on-chip SRAMs is becoming more important, especially for battery-operated portable applications. It is, however, also one of the most significant challenges of high-speed VLSI circuits whose

primary target is not low power but high performance. As systems become more complex toward higher performance, on-chip SRAMs tend to have a large number of bit width such as 16 to 256 or even greater. In this type of SRAM, the active power of the SRAM is dissipated mainly by charging and discharging of the highly capacitive bit/data lines, as shown in Fig. 1.2(a), due to their full swing nature in write cycles.The size of transistors is a vital part of ensuring stability in query processing and we have used 25nm technology in this paper to incorporate cells..

2.AIM AND OBJECTIVE

In this work will describe a novel security oriented 7T SRAM cell design, which incorporates a two-phased write operations and significantlyTo design a 7T SRAM bit cell in 22nm CMOS technology with single bit and 8-bit level operations with compared to existing 6T SRAM bit cell in terms of area, delay and power leakage.

3.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.

4.EXISTING METHOD

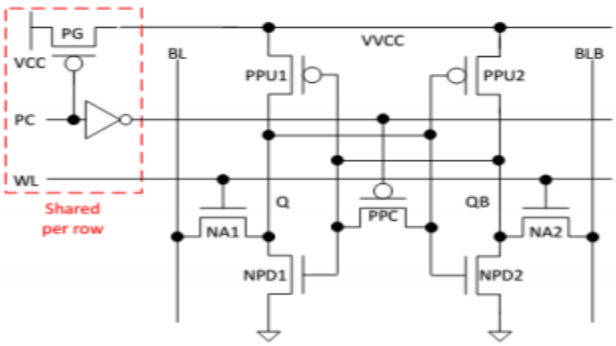
The use of cryptographic devices storing sensitive information has grown considerably during the last few decades and has become a crucial part of many applications, such as smart cards, and mobile devices. Side channel analysis (SCA) is a powerful threat to these devices because it exploits the information 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.

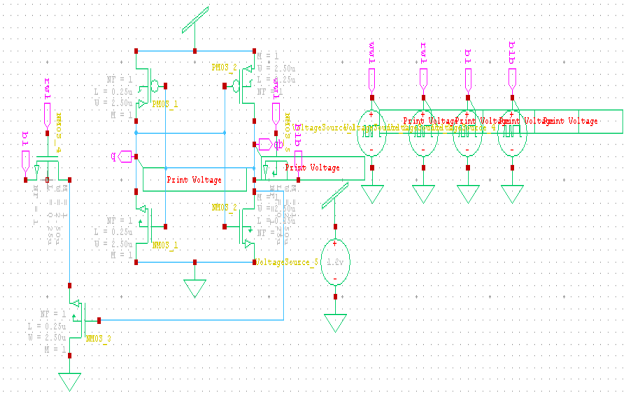
5.PROPOSED METHOD

Power has been a major issue in system-on-chip (SoC) designs with the contemporary submicron technologies. It has thus become very important to control the power and address the power dissipation throughout the design cycle right from the architectural level. However, for 65nm and below technologies, leakage is the main factor which dominates over the dynamic power and contributes to almost 40-50% of total power dissipation. In many new high performance designs, the leakage component of power consumption is comparable to the dynamic/switching component. According to some authenticated reports, 40% or more of the total power consumption is due to the leakage of transistors.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, themean 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.

Schematic Diagram:





6.SIMULATION &RESULTS

Tanner EdaTool : Tanner tool is a Spice Computer Analysis Programmed for Integrated Circuits. Tanner tool consists of the following Engine Machines:

1. S-EDIT (Schematic Edit)
2. T-EDIT (Simulation Edit)
3. W-EDIT (Waveforms Edit)
4. L-EDIT (Layout Edit)

Using these engine tools, spice program provides facility to the use to design & simulate new ideas in Analogue Integrated Circuits before going to the time consuming & costly process of chip fabrication.

SCHEMATIC EDIT TOOL (S-EDIT):

S-Edit is hierarchy of files, modules & pages. It introduces symbol & schematic modes. S-Edit provides the facility of:

1. Beginning a design.
2. Viewing, drawing & editing of objects.
3. Design connectivity.
4. Properties, net lists & simulation.
5. Instance & browse schematic & symbol mode.

Beginning a design: It explains the design process in detail in terms of file module operation and module.

Browser: Effective schematic design requires a working knowledge of the S-Edit design hierarchy of files & modules. S-Edit design files consist of modules. A module is a functional unit of design such as a transistor, a gate and an amplifier.

Modules contain two components:

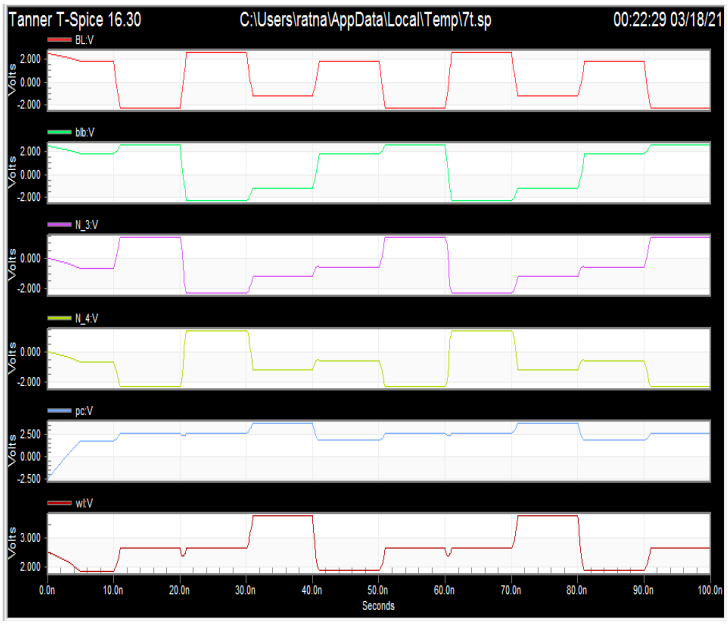
1) **Primitives:** Geometrical objects created with drawing tools.

2) **Instances**: References to other modules in file. The instanced module is the original.

S-Edit has two viewing modes:

1. **Schematic Mode:** to create or view a schematic, we operate in schematic mode.
2. **Symbol Mode:** it represents symbol of a larger functional unit such as operational amplifier.

Output WaveForm



7. 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_ 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 bit.

FUTURE SCOPE

The future research activities may include integration of the proposed DFF in complex digital systems, combining sequential and combinatorial logic. The future research activities may include integration of the proposed DFF in complex digital systems, combining sequential and combinatorial logic. The future research activities may include integration of the proposed DFF in complex digital systems, combining sequential and combinatorial logic. In the future, we can integrate this proposed SRAM in different applications like EMBEDED SYSTEMS, CPU which are power hungry to reduce the power consumption. Also when integrate this sram cell into an array, the overall power consumption of the array will be decreased which is very useful for all portable applications. The future research activities may include integration of the proposed DFF in complex digital systems, combining sequential and combinatorial logic.

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. 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] P.Rajasekar,V. Lakshmi Sravani, G. Anjani Priya, V. Thrushitha, P. Bhavana,(2020),Efficient Combinational Logic Circuit Design Using Quantum- Dot Cellular Automata, Juni Khyat - ISSN 2278-4632VOL-10 ISSUE-5 NO. 1 MAY 2020

[15] E. Konur et al., “Power analysis resistant sram,” in 2006 World Automation Congress. IEEE, 2006, pp. 1–6.

[16] T Prathyusha, P Madhuri, D Pavan Kalyan, R Abhishek, & P Rajasekar(2021), “ Implementation Of Efficient Code Convertors Using Reversible Logic Gates” Dogo Rangsang Research Journal, ISSN : 2347-7180