JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IMPLEMENTATION OF 7T SRAM FOR LOW POWER DATA PROCESSING APPLICATIONS IN A SECURITY SYSTEM

[1]V.Mahesh,[2]R.Rama Mohan,[3]K.Dhanumjaya

[1]PG Scholar,[2]Assistant Professor, [3]Professor,Dept. of E.C.E

[1,2,3]Audisankara College of Engineering and Technology(Autonomous), Gudur, SPSR Nellore(dt.) A.P

ABSTRACT:

Power analysis (PA) assaults have turned into a genuine danger to security frameworks by empowering secret data extraction through the analysis of the current consumed by the power supply of the framework. Implanted recollections, frequently executed with six-semiconductor(transistor) (6T) static random access memory (SRAM) cells, fill in as a critical part in a significant number of these frameworks. 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.

I.INTRODUCTION:

The utilization of cryptographic devices putting away delicate information has developed considerably during the most recent couple of many years and has turned into a urgent piece of numerous applications, like shrewd cards, and cell phones. Side channel examination (SCA) is a strong danger to these devices since it takes advantage of the information connected with the actual way of behaving of these devices to remove touchy information . Dad assaults are considered to be one of the most impressive sorts of SCA strategies since they require generally straightforward gear and arrangements. Dad assaults exploit the correlation between the quick current consumed by the power supply of the gadget and its handled and put away information, to remove restricted information or delicate information.

Implanted recollections rule the region and power consumption of numerous VLSI system-on-chips (SoCs) and are key components of numerous cryptographic systems, for example, shrewd cards and remote organizations utilizing cryptography calculations , where they are utilized to store instruction code and information. Subsequently, the examination and plan of gotten recollections is of most extreme significance. Inserted recollections are for the most part carried out with the 6T SRAM macrocell, which gives high thickness, vigorous operation, and superior

execution. Notwithstanding, 6T SRAM exhibits are traditionally planned and streamlined for high thickness and execution, while their security properties are frequently disregarded, bringing about a high weakness to PA assaults.

Past works have proposed changed SRAM bitcells to lessen the correlation between the unique power dissipation and the put away information of a conventional 6T SRAM cluster. Both of these solutions depend on a two-stage writeoperation. During the principal stage, the inner hubs of the SRAM cell (Q and QB) are pre-charged to a constant voltage to wipe out the correlation between the recently put away information, and the compose operation that follows. In the creators proposed playing out the pre-charge operation by utilizing two additional PMOS semiconductors beyond the first 6T SRAM to drive cut the supply during the additional pre-charge stage. In the creators proposed an input cut SRAM cell, made out of two additional NMOS devices which are utilized to remove the criticism of the SRAM cell to stay away from hamper dissipation. While these solutions really lessen the correlation between the power consumption and put away information of the SRAM cluster, they bring about huge deferral and power overheads, as well as decreased static clamor edges (SNMs).

By and large, we expect that a side-channel aggressor approaches the power supply lines of the system, and that he knows about the chip engineering, including the memory organization, cluster peripherals and inward timing ways. In addition, it is accepted that the aggressor can relegate input vectors to the system, which can bring about memory compose operations to chose columns. At long last, it is common to expect that the general current consumed by the memory large scale peripherals and other chip components can be treated as algorithmic commotion, which can be sifted through utilizing an adequate number of current follows, particularly when the memory exhibit is worked under a different 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.

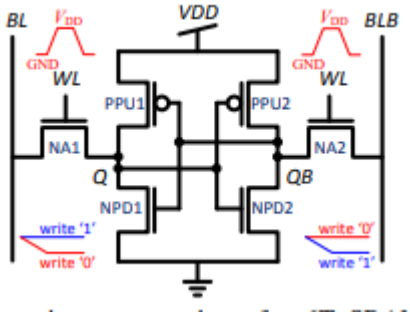

Fig. 1: Schematic representation of a 6T SRAM cell with illustrative write signal waveforms

A conventional 6T SRAM is displayed in Fig. 1 with its sign waveforms during a compose operation. To empower compose admittance to the cell, the word line (WL) is attested and the voltages on the piece line pair (BL and BLB) are moved to the inward stockpiling hubs, Q and QB, individually. At the point when the composed level varies from the worth put away in the cell before the compose occasion, the cell scatters dynamic energy to charge the interior cell capacitances. In addition, the cell disperses hamper since the entrance semiconductors (NA1 and NA2) should beat the inner criticism of the cell (shaped by semiconductors NPD1, PPU1, NPD2, and PPU2) to change its put away worth. On the other hand, when the composed worth is like the put away information, no unique energy is scattered by the cell and the complete power consumption is overwhelmed by its leakage currents.

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.

Disadvantages:

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

II.PROPOSED SYSTEM:

In ongoing strategy for Cryptographic application based devices which have more touchy information with more vital piece of putting away and recovering the information. In this way it's effect with power examination and side channel investigation its adventure correlation between the prompt current consumed power supply devices with information leakages. In this work will portray an original security situated 7T SRAM cell plan, which consolidates a two-staged compose operations and fundamentally decreases the correlation between the composed and put away information in the memory and its power dissipation, subsequently its giving a power examination strong memory. This proposed 7T cell incorporates an additional transistor to the current 6T SRAM implementation with single power gate transistor per memory. Here, this proposed work will plan a 7T SRAM digit cell in 22nm CMOS innovation in TANNER EDA Software with single cycle and 8-bit level operations with contrasted with existing 6T SRAM bit cell regarding region, postponement and power leakage.

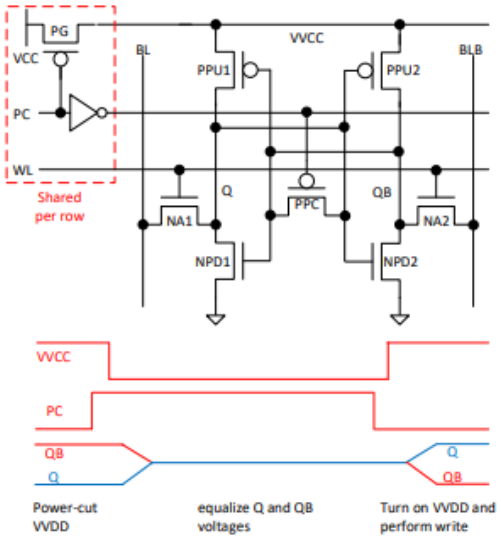

Fig. 2: Proposed 7T SRAM cell and basic operation

The schematic representation of the proposed 7T SRAM cell is shown in Fig. 2. A power gate PMOS transistor (PG) isused 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.

Advantages:

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

TABLE I: Comparison of SRAM cells

PARAMETERS	6T SRAM	7 T SRAM	7T SRAM WITH SUBTHRESHOLD USING LOW SWING LOGIC
MOSFETS	6	10	7
DELAY (SEC)	1.01	0.96	0.97
POWER	$4.102^{*}e^{-003}$	2.76^{+e-003}	1.12e-003
AREA (NO.OF.NODES)	7	11	11
INPUT VOLTAGE	5V	3V	
TECHNOLOGY	25nm	25nm	18nm

III.RESULTS:

The average power consumption for this circuit was **1.12e-003** watts.

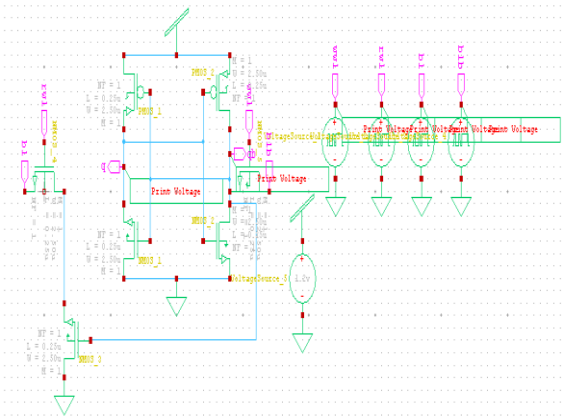

Fig.3 Schematic of Sub Threshold 7T SRAM Cell schematic circuit implemented using adiabatic logic in Tanner EDA tool to analyze and compare with the existing design.

In SRAM, To convert from BL to VDD, simply input a "1 into the cell", which begins loading and

changing "Q" to "0". Sometimes one is better than many. By connecting the "QB" to the "1" input, the M1 can let the node be run. To write the data to the 0 state, use the M5 to access the bit line. the Q node starts discharging At this stage, this node, the flow shifts to M3. When the QB has fired, the M2 will energise the zero generation, after which a justification will be produced from the zero node. Read the cell activity 0: A0 is the cell to be read: Until data in the bit line are loaded, they have been applied to VDD. The current value of the bit line is not being changed until after it has been pre-loaded with a value before being shifted out of phase.

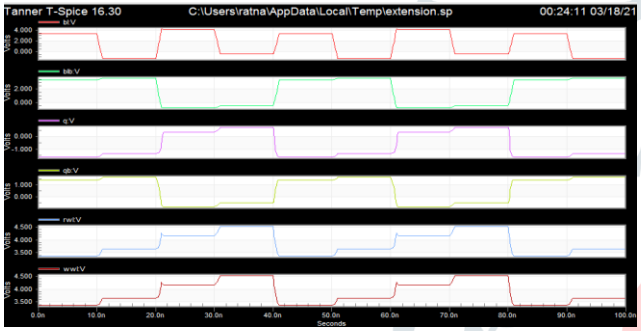

Fig.4: Output Analysis of Sub Threshold 7T SRAM Cell

VI. 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 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. 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. Rozi˘ 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.