International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Leakage Power Attack Resiliency in Novel-7T SRAM

C.Padmini[1], B. Anjan kumar[2], V. Prem kumar[3]

[1]*Assistant Professor, Dept. of E.C.E, Vardhaman College of Engineering, Hyderabad, India*
[2,3]*B. Tech Final Year student, E.C.E, Vardhaman College of Engineering, Hyderabad, India*

Abstract - *Power analysis (PA) attacks have become a serious damage to security systems by enabling secret data extortion 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 major component in many of these systems. However, conventional SRAM cells are prone to side-channel attacks due to the correlation between their current characteristics and written data. For reducing these types of attacks, we propose a security based design of 7T SRAM cell, which consists of an additional transistor to the conventional 6T SRAM cell and a two-phase write operation, which reduces the correlation between the stored data and the power consumption during read and write operations. The proposed 7T SRAM cell was implemented in a 45 nm technology and has a lower write energy standard deviation between write '1' and '0' operations compared to a conventional 6T SRAM. The proposed cell has a 38%–52% write power reduction and a 18%–37% reduction in write delay compared to other power analysis resistant SRAM cells.*

***Key Words*: Power analysis, SRAM design, Static noise margin.**

1. INTRODUCTION

A large portion of the chip is represented by SRAM, and it is predicted to be widely used in high-performance processors and portable devices. Low-power SRAM plays a major role in achieving higher reliability and longer battery life for portable application [3]. Major part of the power in SRAM is consumed by data lines, bit lines and periphery circuits. These represent the active power consumption [5] [6]. During a write operation out of total dynamic power consumption, nearly 50% of the power is dissipated in bit lines [7]. Low-power SRAM design techniques are mainly based on reducing the power consumption level. Data lines, bit lines, and word lines are the largest capacitive parts in the memory.

The usage of devices to store sensitive and confidential information has increased and become essential in many applications [2]. A significant threat to those devices is extortion of sensitive information by side-channel attacks (SCAs) [9]. Power analysis is on the type of side channel attacks that uses the processed information that leaks during power dissipation of device [1]. The correlation between the power consumption of device and stored information is used in power analysis.

As PA techniques can be used in extracting valuable information by the usage of dynamic power characteristics of a system, this has become a serious threat to the security of cryptographic systems [4], several works have shown the effectiveness of leakage power analysis on FPGA devices and more deeply scaled technologies [9]. The design of secured memory structures and the analysis of power attacks on embedded memories are highlighted during the study on power analysis attacks on logic circuits and the development of secured logic [9] [10]. Mostly, embedded memories are implemented using a 6-transistor (6T) SRAM array, which dominates the area and power of several VLSI system-on-chips, 6T SRAM array acts as a key component in many cryptographic systems like smart cards and wireless networks employing cryptography algorithms [11]. In these systems, SRAM arrays are used to store instruction code and data. Hence, the analysis and design of secured memories has to be performed with utmost care.

1.1 DESIGN OF CONVENTIONAL 6T SRAM CELL

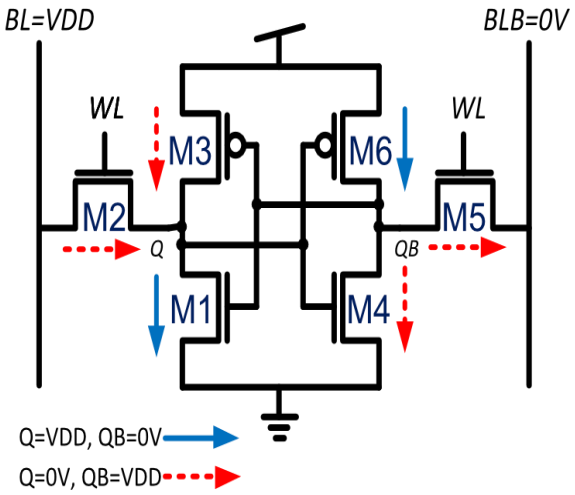

Fig: 1 Circuit diagram of 6T SRAM cell

A conventional 6T SRAM cell is shown in Fig. 1, consists of two nMOS pass transistors which are used to access the cell for read or write operations and two inverters are connected back-to-back. For a stable write operation, one of the bit lines has to be set to '0' and the other to '1'. Transistors size plays an important role to ensure a stable read and write operations and here, in this paper we have used 45nm technology of Cadence Virtuoso tool for implementing the cells.

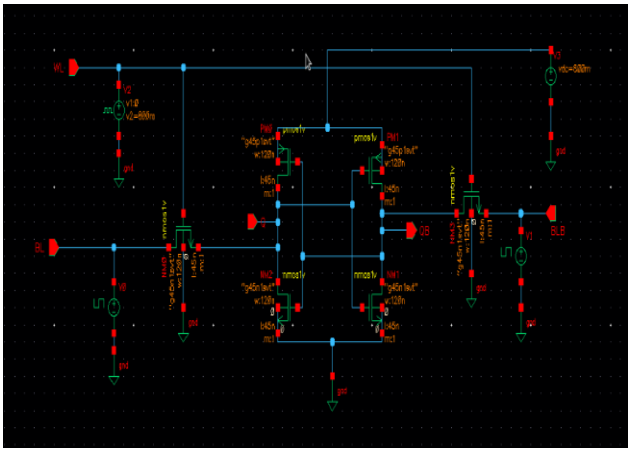

Fig. 1. Schematic of 6T SRAM cell

During the hold state the bit line (BL) and the bit line bar(BLB) are connected to VDD and GND respectively and also the main leakage components are connected as shown in the above Fig. 1. When a write '1' operation is made to a cell, the signal voltages can be generated for a cell storing a '1' or '0' in a unselected row corresponding to the same column. The signal voltages for each operating mode of the memory structure is shown in the Fig. 1. Due to the leakage paths present in the 6T SRAM cell, it exhibits an asymmetrical leakage mechanism depending upon the stored data of the cell [1]. If the cell holds '1' i.e., Q=VDD and QB=0 V respectively, then it consists of two leakage paths through M1 and M6 transistors. On the other hand, if the cell holds '0' i.e., Q = 0 V and QB = VDD, then it consists of four leakage current paths through M2, M3, M4, and M5 transistors. These leakage currents are capable of providing the information present in the steady state. These leakage current paths are found to be caused due to subthreshold conduction.

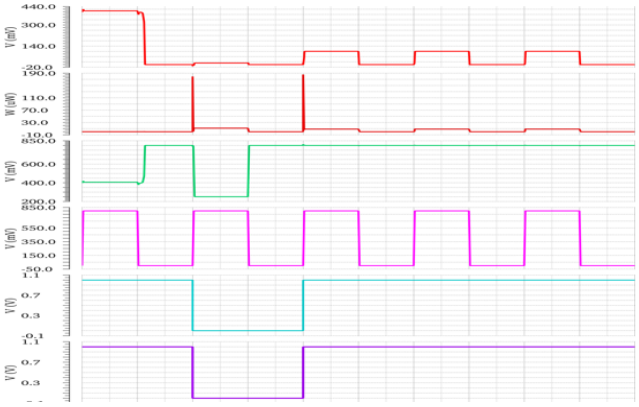

Fig: 1(a) Power analysis of 6T SRAM cell

The above scenario represents the power analysis of 6T SRAM cell implemented and simulated in Cadence virtuoso tool at GPDK 45nm technology under a nominal supply voltage of 0.5 V. An LPA attack are capable of extracting a secret word in a 6T memory array.

1) In general, the attacker has knowledge on structure of the memory macro and particularly system architecture, internal timing paths, memory peripherals including the array organization.

2) Also, The attacker has the ability to provide inputs to the system, which may result in memory read and write operations to any row in the array.

3) The attacker can figure out noise included with total power consumption of other chip components. Hence, the signal to noise margin is assumed to be very low.

To know the stability of the 6T SRAM cell the signal to noise margin (SNM) distributions for read, write and hold states were evaluated and simulated using Cadence virtuoso tool at GPDK 45nm technology are provided as shown in the fig.1 (b) and Fig.1(c).

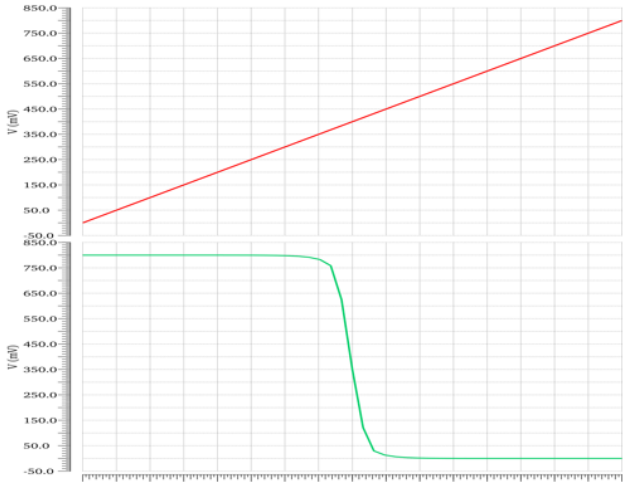

Fig.1 (b) SNM for 6T SRAM cell

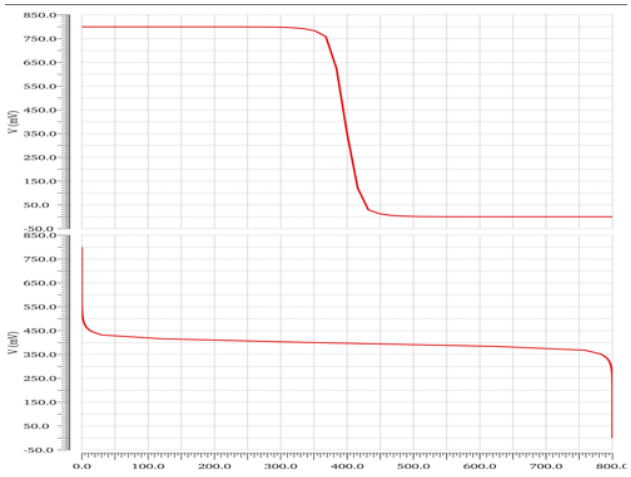

Fig.1(c) SNM for 6T SRAM cell

2. DESIGN OF 8T SRAM CELL

The 8T SRAM cell is based on a conventional 6T SRAM cell along with two more additional nMOS transistors 'M7' and 'M8'. These also act as access transistors similar to transistors 'M2' and 'M5' and these transistors are connected between the bit line 'BL' and 'QB', and 'BLB' and 'Q', respectively.

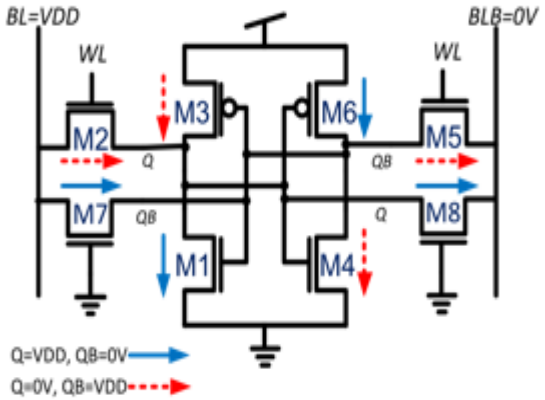

Fig.2 Circuit diagram of 8T SRAM cell

The gate terminals of the transistors 'M7' and 'M8' are connected to GND, to keep them in cutoff throughout all the memory operating modes. Nonetheless, during the hold state,

Two additional leakage current paths are formed due to these transistors in the case where the voltages in 'Q' and 'BL' are equal.

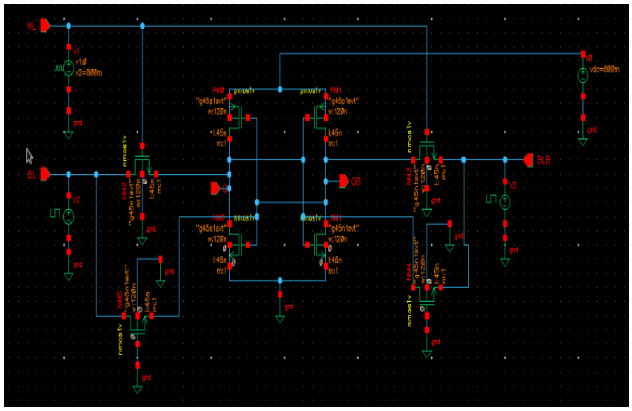

Fig.2 (a) Schematic of 8T SRAM cell

Due to the symmetry, the number of leakage current paths occurred are equal under any BL/BLB condition for the data levels stored in the cell [8]. Thus showing the leakage current paths for both cases, where the cell stores '1' and '0'.

And the leakage currents of cells storing '0' and '1' with the bit line 'BL' driven to 'VDD' and bit line bar 'BLB' discharged to GND. There is a smaller mean difference between the leakage current distributions in both the data levels than a similar distribution fora 6T SRAM cell.

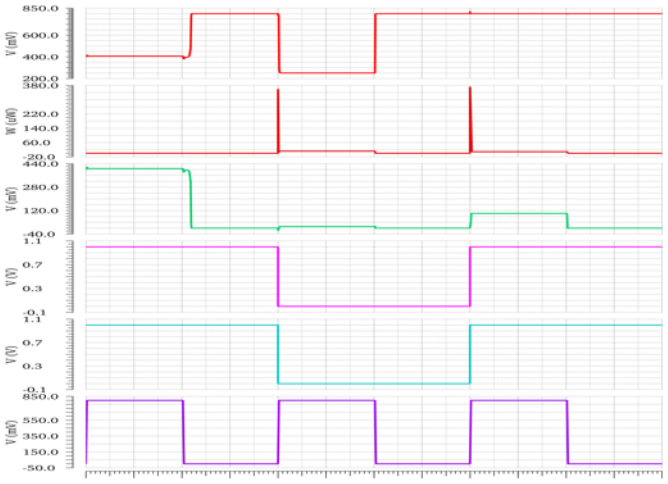

Fig.2 (b) Power analysis of 8T SRAM cell

To know the stability of the 8T SRAM cell the signal to noise margin (SNM) distributions for read, write and hold states were evaluated and simulated using Cadence virtuoso tool at GPDK 45nm technology are provided as shown in the fig.2 (c) and Fig.2 (d).

Fig.2 (c) SNM of 8T SRAM cell

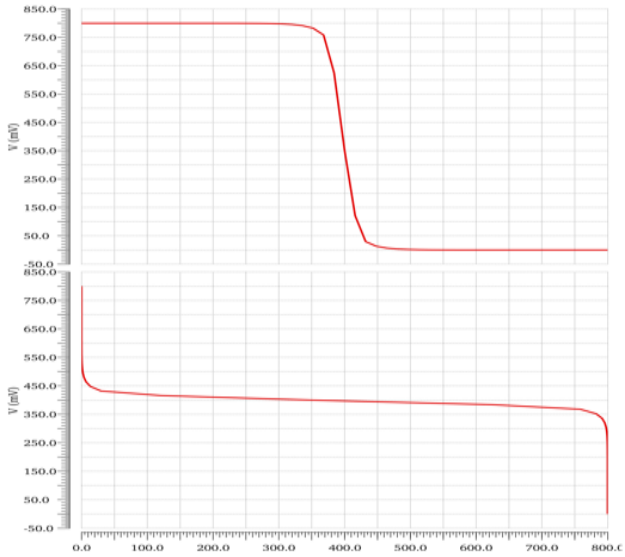

Fig.2 (d) SNM of 8T SRAM cell

The 8T SRAM cell operations for read and write are similar to that of the conventional 6T SRAM cell, and therefore, the 8T SRAM cell can be directly integrated into the conventional memory architectures without making any changes to the memory peripherals.

3. DESIGN OF NOVEL-7T SRAM CELL

The schematic of 7T SRAM cell is as shown in Fig. 4 is similar to the 6T SRAM cell, but the only difference is, it is having an extra transistor 'M7' has been connected in series with the 'M1' transistor. This transistor 'M7' prevents the leakage of voltage passing to ground by making itself to OFF state during the read operation. It contains an extra word line bar 'WLB' which is complement to the main word line 'WL'.

During the write operation the word line 'WL' is turned ON and 'WLB' is kept low.

The simulated Input and output waveforms along with power dissipated during transient analysis for 7T SRAM memory cell is as shown in the Fig.3.

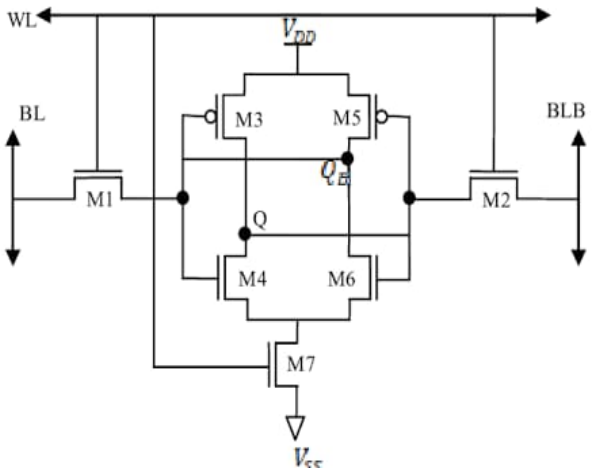

Fig.3 circuit diagram of 7T SRAM cell

The simulations are performed using Cadence virtuoso tool at GPDK 45nm technology. The schematic of 7T SRAM cell and transient response are shown in Fig.3 (a) and Fig.3 (b).

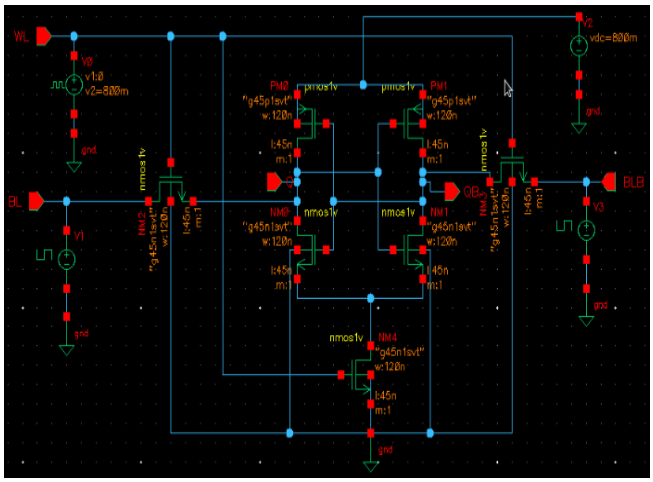

Fig.3 (a) Schematic of 7T SRAM cell

When word line is '0' as data hold state will be activated no data flows into the memory. When WL is '1' the read and write operations will be activated. During write operation bit line BL and bit line bar BLB are inputs and Q and QB are outputs and data can be easily write into the memory. In read operation Q and QB are inputs and bit line BL and bit line bar BLB are outputs and data can be read from the memory. Because of the presence of the extra accessing transistor the data read speed can be increased compared with the conventional 6T SRAM cell and also the leakage current is constant and the extra transistor are connected and no inputs to it's of the gate terminal. Bit lines acts as the input output nodes during the read and write operation in the SRAM cells.

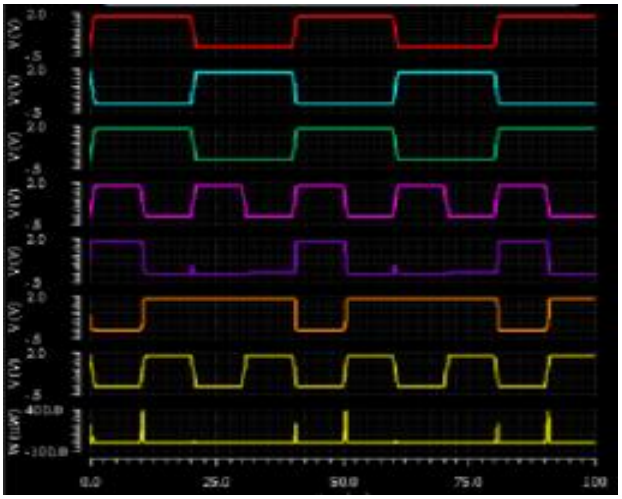

Fig.3 (b) Power analysis of 7T SRAM cell

The stability of 7T SRAM cell is mainly depend on signal to noise margin (SNM). The signal to noise margin (SNM) distributions for read, write and hold states were evaluated and simulated using Cadence virtuoso tool at GPDK 45nm technology are provided as shown in the fig.3 (c) and Fig.3 (d).

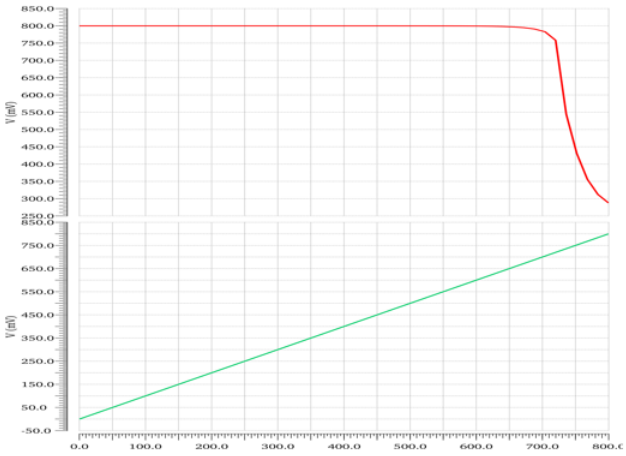

Fig.3(c) SNM of 7T SRAM cell

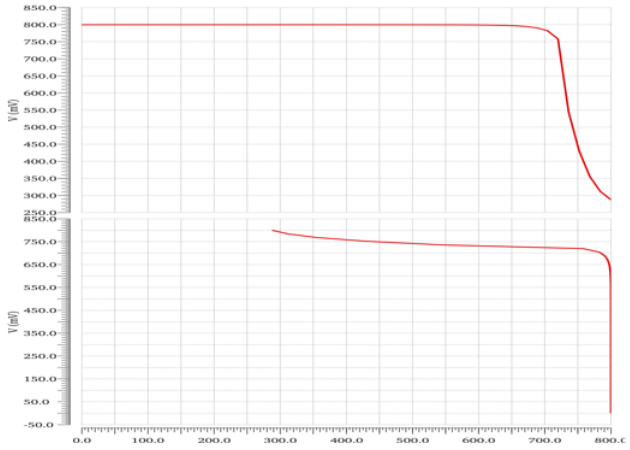

Fig.3 (d) SNM of 7T SRAM cell

4. RESULTS

The corresponding power and delay values of the 6T SRAM cell, 8T SRAM cell and 7T SRAM cell are evaluated and simulated using cadence virtuoso tool at GPDK 45nm technology and provided the power delay products of the corresponding SRAM cells are tabulated as shown.

SRAM	POWER	DELAY	PDP
6T	3.738E-6	-4.5E-11	-1.68E-16
8T	3.756E-6	-4E-11	-1.5E-16
7T	2.771E-6	-5.11E-11	-1.41E-16

5. CONCLUSION

It is observes that due to the presence of extra access transistors in the SRAM cell the accessing speed of the cell has been increased by decreasing delay in read operation and the power consumption has been reduced 42% compared with the conventional 6T SRAM cell. Hence it is observed that the power delay product also decreased after comparing the results evaluated obtained from the simulations in cadence virtuoso tool.

REFERENCES

[1] R. Giterman, M. Vicentowski, I. Levi, Y. Weizman, O. Keren and A. Fish, "Leakage Power Attack-Resilient Symmetrical 8T SRAM Cell," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 26, no. 10, pp. 2180-2184, Oct. 2018.

[2] M. Alioto, L. Giancane, G. Scotti and A. Trifiletti, "Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 57, no. 2, pp. 355-367, Feb. 2010.

[3] 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," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 61, no. 2, pp. 429-442, Feb. 2014.

[4] M. Neve, E. Peeters, D. Samyde and J. -. Quisquater, "Memories: A Survey of Their Secure Uses in Smart Cards," Second IEEE International Security in Storage Workshop, Washington, DC, USA, 2003, pp. 62-62.

[5] D. Samyde, S. Skorobogatov, R. Anderson and J. -. Quisquater, "On a new way to read data from memory," First International IEEE Security in Storage Workshop, 2002. Proceedings. Greenbelt, MD, USA, 2002, pp. 65-69.

[6] W. Liu, R. Luo and H. Yang, "Cryptography Overhead Evaluation and Analysis for Wireless Sensor Networks," 2009 WRI International Conference on Communications and Mobile Computing, Yunnan, 2009, pp. 496-501.

[7] V. Rožić, W. Dehaene and I. Verbauwhede, "Design solutions for securing SRAM cell against power analysis," 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, San Francisco, CA, 2012, pp. 122-127.

[8] Hulfang Qin, Yu Cao, D. Markovic, A. Vladimirescu and J. Rabaey, "SRAM leakage suppression by minimizing standby supply voltage," International Symposium on Signals, Circuits and Systems. Proceedings, SCS 2003. (Cat. No.03EX720), San Jose, CA, USA, 2004, pp. 55-60.

[9] R. E. Aly and M. A. Bayoumi, "Low-Power Cache Design Using 7T SRAM Cell," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 54, no. 4, pp. 318-322, April 2007.

[10] R. Giterman, O. Keren and A. Fish, "A 7T Security Oriented SRAM Bitcell," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 66, no. 8, pp. 1396-1400, Aug. 2019.

[11] Daihyun Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "Extracting secret keys from integrated circuits," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 13, no. 10, pp. 1200-1205, Oct. 2005.