A New Power Analysis Resistant SRAM Cell

Ebru Arıkan[1], Atilla Ataman[2]

[1]TÜBİTAK – UEKAE, Anibal Street Gebze Kocaeli, TURKEY
ebru@uekae.tubitak.gov.tr
[2]Yıldız Technical University, Yıldız İstanbul, TURKEY
ataman@yildiz.edu.tr

Abstract

The power consumption of a standard SRAM during read/write operations is dependent on the address applied, the data accessed, and the type of access (read/write). The power analysis resistant SRAM structure [1] developed during the Project "SCARD" (Side Channel Analysis Resistant Design Flow) of the European Community 6. Framework Program reduces the dependency of power consumption on data and address compared to standard SRAM at the expense of higher power and silicon area consumption. In this work a new SRAM primitive cell structure is proposed to reduce the power consumption and its dependency to data to be written.

1. Introduction

Side-channel attacks which extract secret data running on the cryptographic device were introduced in 1999 [2]. And since then many research has been doing on side channel attacks and countermeasures against them. Side channel attacks use information leaked by the hardware to reveal the secret key. Power analysis which is one of the several side channel analysis methods is based on the fact that the consumed power by the cryptographic device is depended on the processed data. To make the cryptographic device resistant against power attacks several countermeasures on hardware [4 - 16] and algorithmic level have been proposed.

The memories may store critical information in cryptographic hardwares. Depending on the application, the data bus or address bus, or both of them may contain critical information. The power analysis of memory blocks reveals that conventional CMOS memories are vulnerable to side-channel analysis since their power consumption shows dependencies on the data read from or written into the memory and the address applied. In order to be called "secure" against power analysis, the memory must not reflect any information about both the data and address on the consumed power.

During the Project "SCARD" (Side Channel Analysis Resistant Design Flow) of the European Community 6. Framework Program, power attacks resistant SRAM structure has been proposed and implemented in ASIC [1]. In this work a new secure primitive memory cell is proposed to reach less power consumption and better resistance against power attacks. The rest of the paper is organized as follows: In the second section the power consumption of the conventional SRAM is analyzed. In the third section the secure SRAM primitive cell developed during the SCARD Project is introduced and a new primitive cell is proposed. The fourth section concludes the paper.

2. Conventional SRAM Cell

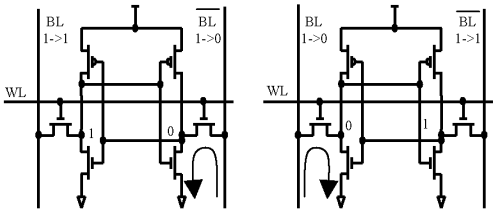

Fig. 1 The current flow directions in a standard memory cell during the read operation

The current flow directions in a conventional primitive memory cell during the read operation are shown in Fig. 1. The complementary bitlines BL and $\overline{BL}$ are both precharged to logic level '1' during the precharge phase and let be floating during the evaluation phase. The complementary outputs of the memory cell are connected to floating bitlines during evaluation phase through the pass transistors controlled by WL (word line) signal. While always one bitline discharges to ground the other one preserves its high level state. If the bitlines capacitances match each other the same amount of charge transfer takes place during read operation at all times, which makes read process independent from the data. Precharge and differential logic style of conventional SRAM is an advantageous from security point of view. The current flow directions during write operation are shown in Fig. 2.

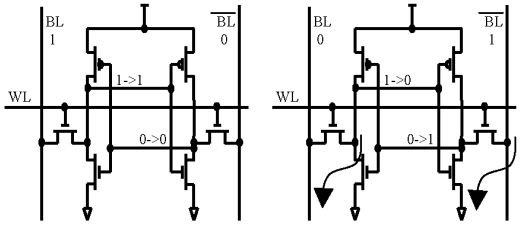

Fig. 2 The current flow directions in a standard memory cell during the write operation

The complementary bitlines BL and $\overline{BL}$ are precharged to logic level '1' during the precharge phase. The data to be written is applied complementarily to these lines during the evaluation phase and the memory cell is forced to store the data. If the data being written is the same as the value already stored in the addressed cell no charge transfer takes place. On the other hand, if the data being written is different from the previously stored data charge is transferred in order to toggle the state of the internal nodes in the SRAM cell. It concludes that the current consumption during write process depends on the value being

already stored and the data being written into the addressed SRAM cell. The write operation of the standard SRAM is vulnerable to power analysis.

3. Secure SRAM Cell

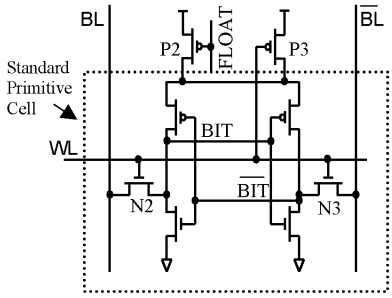

Fig. 3 Secure SRAM primitive cell

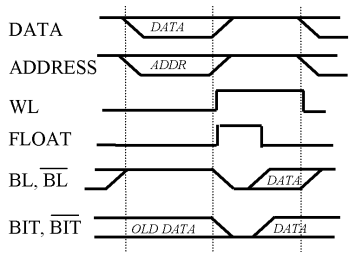

Fig. 4 Secure SRAM write operation

The secure SRAM primitive cell and timing diagram of modified write operation are shown in Fig. 3 and Fig. 4 If the internal nodes BIT and $\overline{BIT}$ of the addressed cell would be brought to the same logic level (precondition) before forcing data to be written, one node will always toggle and the other will remain unchanged after the write process is completed regardless of the data. Because NMOS transistor can pass logic level low better then logic level high, the preconditioning of internal nodes is accomplished through discharging the bitlines (BL and $\overline{BL}$) connected to the addressed cell trough N2 and N3 transistors at the beginning of the evaluation phase. To prevent the resistance of the cross coupled inverters to preconditioning the cell is isolated from the supply. This fact results in the addition of an extra series PMOS device (P2). The control signal FLOAT of P2 is common to all the cells on the same column for minimal routing overhead. Therefore in order to isolate only the addressed cell in a column, a PMOS device P3 parallel to P2 is also introduced to the cell which is controlled by the WL signal. FLOAT signal should be de-activated when the internal nodes are discharged. So the actual write process can take place. In order to detect whether both of the internal nodes are discharged an extra row of cells is placed in the SRAM array that imitates the behavior of the addressed cell. The internal nodes of the extra SRAM cell are used to create the control signal FLOAT.
One can refer to the paper [1] to see the detailed simulations and how the resistance of the address decoding to power attacks is improved. According to the simulations the data dependency of power consumption is reduced 10 times but the power consumption is doubled. The secure SRAM has been manufactured within the SCARD project. The measurement results match with the simulations.
It is possible to avoid the second PMOS transistor P3. In this case, all the cells at the selected column will be isolated from the power supply during preconditioning. While the internal nodes of the addressed cell will be discharged through bitlines, the others cells at the same column will preserve their states dynamically and then will return to their static states when connection to supply is established.

In this work the new proposed SRAM primitive cell is compared to this SRAM primitive cell having one extra PMOS transistor which is called cell-1 during the rest of the paper.

3.2. The New Proposed Secure SRAM Cell

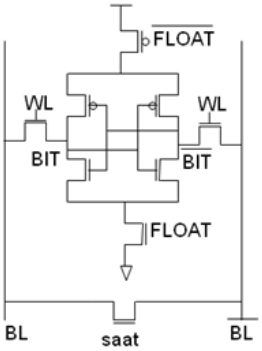

Fig. 5 The new SRAM primitive cell

The new proposed SRAM primitive cell called cell-2 is shown in Fig. 5. In the precharge phase the complementary bitlines are neither precharged to supply level nor discharged to ground. Instead the floating bitlines are shortened via the NMOS transistor. The bitlines reach to the same voltage level VDD/2 because the bitlines have the same capacitive load in order to prevent the leakage. This is the basic constraint for complementary signals in all dual-rail precharge logic styles which are used in cryptographic devices as a countermeasure on hardware level against power attacks. At the beginning of the evaluation phase the conditioning of the internal nodes to the same voltage level before write operation is achieved by isolating the addressed cell from both supply and ground and connecting to the bitlines. The conditioning voltage level is VDD/2. At the rest of the evaluation phase the isolation from ground and supply is removed and the actual complementary data is forced to the bitlines. Always one bitline discharges from VDD/2 to ground and the other charges to VDD from VDD/2 independent from the data to be written, which means resistance against power attacks. The important improvement of the cell-2 over cell-1 and even over standard cell is the power consumption reduction. The energy required during precharge phase and conditioning of the internal nodes is obtained from the initial stored charges on bitlines instead of supply. The simulation results of the cell-2 is shown in the Fig. 6. As test vector data and inverted data are applied sequentially to cell-2. As in [3], the energy per cycle E is used as merit to measure the resistance against power analysis attacks. The smaller are the normalized energy deviation (NED) and the normalized standard deviation (NSD) values the better is the resistance against power attacks. E_{max}, E_{min}, $\mu(E)$ *and* $\sigma(E)$ are maximum, minumum, mean and standard deviation of E respectively.

$$E = \int_0^T I_{VDD}(t)dt \quad (1)$$

$$NED = (\mathrm{E_{max}} - \mathrm{E_{min}})/\mathrm{E_{max}} \quad (2)$$

$$\mathrm{NSD} = \sigma(\mathrm{E})/\mu(\mathrm{E}) \quad (3)$$

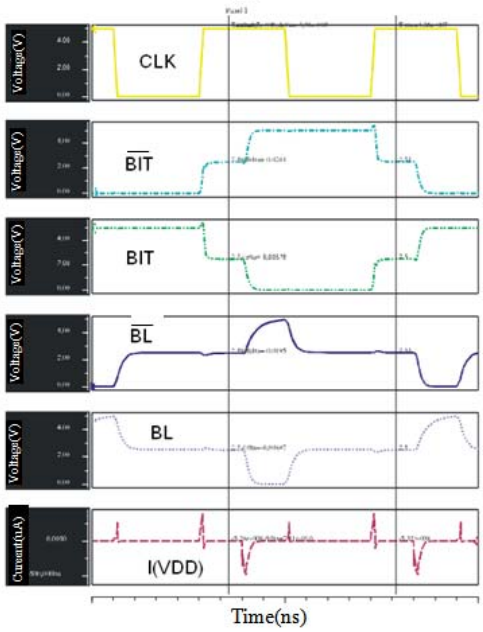

Fig. 6 The simulation of the primitive cell

The NSD and NED values for standard cell, cell-1 and cell-2 for the same simulation setup in schematic level are given in Table 1. VDD is 5V. The resistance of cell-2 is better than the one of cell-1. The power consumption of cell-2 is even less then the power consumption of the standard cell.

	Standard	**Cell-1**	**Cell-2**
E_{max}(mJ)	0.1679	0.1840	0.0154
E_{min}(mJ)	0.1597	0.1766	0.0153
NED	0.0489	0.0406	0.0033
σ*1e-4	0.0379	0.0341	0.0003
μ(mJ)	0.1640	0.1803	0.0154
NSD	0.0231	0.0289	0.0018

Table 1 NSD and NED values of different SRAM primitive cell structures.

4. Conclusions

The new proposed primitive cell is a strong candidate in term of reduced power consumption and increased resistance against power attacks over the cell-1. The disadvantegous of the new proposed cell is the one extra NMOS transistor in the cell compared to the cell-1. The simulation results mentioned in the third section should be verified with different simulation setups. And all of these simulations should be repeated on layout level for SRAM blocks having standard, cell-1 and cell-2 primitive cells. As final step, these SRAM blocks will be produced with 0.7μm CMOS technology of YİTAL (Semiconductor Technologies Research Labrotory) in UEKAE (Natioanal Electronics and Cryptology Research Institute) in Turkey.

5. References

[1] E. Konur, Y. Özelçi, E. Arıkan, U. Ekşi, "Power Analysis Resistant SRAM", World Automation Congress (WAC) 2006, July 24-26, Budapest, Hungary.

[2] P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis", Proc. Of Advances in Cryptology, Lecture Notes in Computer Science, 1999, pp.388-397.

[3] K. Tiri, M. Akmal, I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards", European solid-state circuits conference, Florence, Sept. 2002, pp. 403-406.

[4] A. Bystrov, D. Sokolov, A. Yakovlev, A. Koelmans J. Murphy, "Design and Analysis of Dual-Rail Circuits for Security Applications", IEEE Trans. on Computers, vol. 54, no. 4, April 2005.

[5] J. S. Lee, J. W. Lee, Y. H. Kim, "Symmetric Discharge Logic against Differential Power Analysis", IEICE Trans. Fundamentals, vol.E90–A, no.1 January 2007.

[6] O. Mirmotahari, Y. Berg, "Proposal for a Ultra Low Voltage NAND gate to withstand Power Analysis Attacks", Proceedıngs of World Academy Of Science, Engineering and Technology vol. 25 November 2007 ISSN 1307-6884

[7] Mac´e, F., Standaert, F.-X., Hassoune, I., Legat, J.-D., Quisquater, J.-J. "A Dynamic Current Mode Logic to Counteract Power Analysis Attacks" In: The Proceedings DCIS 2004, Bordeaux France, pp. 186–191 (November 2004)

[8] Hassoune, I., Mac´e, F., Flandre, D., Legat, J.-D. "Low-swing current mode logic (LSCML): a new logic style for secure smart cards against power analysis attacks.", Microelectronics Journal 37(9), 997–1006 (2006).

[9] S. Mangard, K. Schramm, "Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations", CHES 2006, LNCS 4249, pp. 76–90, 2006

[10] A. Moradi, M. Taghi, M. Shalmani, M. Salmasizadeh, "Dual-rail transition logic: A logic style for counteracting power analysis attacks", Comput. Electr. Eng. (2008), doi:10.1016/j.compeleceng.2008.06.004.

[11] M. Aigner, S. Mangard, R. Menicocci, M. Olivieri, G. Scotti, A. Trifiletti, "A Novel CMOS Logic Style with Data Independent Power Consumption", ISCAS 2005, Kobe, Japan May 23-26.

[12] Marco Bucci, Luca Giancane,Raimondo Luzzi and Alessandro Tri.letti, "Three-Phase Dual-Rail Pre-charge Logic", CHES 2006,Yokohama, Japan, October 10-13.

[13] Zhimin Chen and Yujie Zhou, "Dual-rail Random Switching Logic A Countermeasure to Reduce Side Channel Leakage", CHES 2006 Yokohama, Japan, October 10-13.

[14] Wieland Fischer and Berndt M. Gammel, "Masking at Gate Level in the Presence of Glitches", CHES 2005, Edinburgh, UK, August 29-September 1

[15] F. Gürkaynak, S. Oetiker, H. Kaeslin, N. Felber, W. Fichtner, "Improving DPA Security by Using Globally-Asynchronous Locally Synchronous Systems", ESSCIRC 2005, Grenoble, France, September 12-16

[16] S. Mangard, T. Pop, B. M. Gammel, "Side-Channel Leakage of Masked CMOS Gates*?"*, CT-RSA 2005, San Francisco, CA, USA, February 14-18.

[17] Kris Tiri and Ingrid Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", DATE 2004, Paris, France, 20 February.