Design Solutions for Securing SRAM Cell Against Power Analysis

Vladimir Rožić*, Wim Dehaene† and Ingrid Verbauwhede*
* Katholieke Universiteit Leuven, ESAT/SCD/COSIC and IBBT
† Katholieke Universiteit Leuven, ESAT/MICAS and IMEC
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
E-mail: {Vladimir.Rozic, Wim.Dehaene, Ingrid.Verbauwhede}@esat.kuleuven.be

***Abstract*—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 power-analysis resistant SRAM. We compare these solutions in terms of data stability, delay and side-channel resistance.**

***Index Terms*—SRAM, differential power analysis, security**

I. Introduction

In recent years, the issue of secure hardware implementations has gained considerable attention. As research on side channel attacks (SCA) progresses, new attacks which circumvent security provided by mathematically secure algorithms, are being developed [1]–[3]. Power analysis attacks make use of the intrinsic, physical correlation between device's power consumption and the values of internal variables in order to obtain the secret data. In parallel with the research on SCA, considerable effort has been made to develop efficient countermeasures. One solution is to use power flattening techniques which apply dual-rail precharge principle in order to equalize the amount of energy consumed in every clock cycle. Logic styles developed for this purpose, Wave Dynamic Differential Logic (WDDL) [4] and Sense Amplifier Based Logic (SABL) [5] are based on this principle. Placement and routing rules that balance dual signals have to be incorporated into the design flow.

While considerable research has been done on development of secure logic-styles, less attention has been paid to designing secure SRAM. This is somewhat surprising, taking into account the benefits of embedded memory arrays for compact hardware implementations. The area of a single memory cell is up to 10 times smaller than the area of a flip-flop available in standard libraries for digital design. We believe that this issue is of growing importance since embedded SRAM may provide the solution for compact, side-channel resistant implementations of public-key cryptography, which is difficult to achieve by using only flip-flop based storage. Power-analysis resistant SRAM cell [6] with two power-cut PMOS transistors uses the same principles as SABL and WDDL. Due to it's symmetric cell structure and regular layout, SRAM cell is suitable for dual-rail operation with balanced capacitive loads.

The topic of this paper is the side-channel resistant SRAM cell. As the first contribution, we explore the influence of the proposed countermeasure on noise margins, energy consumption and delay. Then, we propose a solution to reduce the area overhead by sharing power-cut PMOS transistors between different cells. In addition, we propose a second strategy which relies on cutting the feedback inside the cell during the precharge phase. A cell design which utilizes this technique is presented. All three solutions are evaluated for data stability, delay and side-channel security. The focus of this paper is on data secrecy, which means that processed data should not leak through the power trace. At this point, we are not concerned whether the attacker can guess the memory address or the type of operation.

This paper is organized as follows. Section II contains the background information and defines the terms that will be used throughout the paper. In this section basics of SRAM design are explained and sources of side-channel leakage are discussed. Description of the power-analysis resistant SRAM cell is presented in Section III. This section also contains the main contribution of this paper, which is the two novel circuit-level techniques for obtaining SRAM security, namely shared-PMOS structure and the feedback-cut cell. In section IV, we investigate noise margins, speed and layout of these cells and make a comparison with a standard 6T SRAM cell. Section V contains the security analysis. Conclusion is formed in Section VI.

II. Background

A. SRAM design

Standard SRAM cell (6T cell) consists of 6 transistors, as shown in figure 1 a). Two inverters form a latch and two NMOS are used to access bit lines. Cells are arranged in a matrix with bit lines (BL and $\overline{BL}$) running vertically and word lines (WL) running horizontally. In some designs fully-subdivided word line architecture is used, where each word line connects only to the cells of the same word. This

978-1-4673-2340-6/12/$31.00

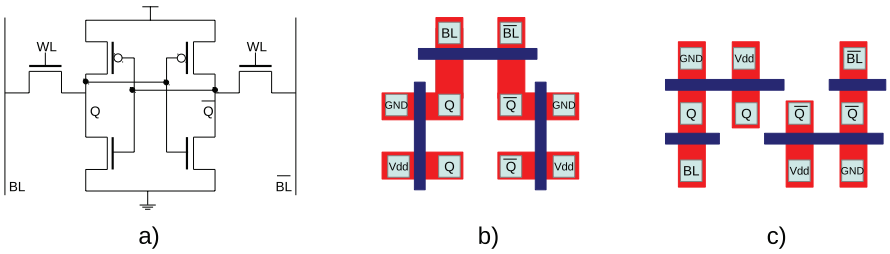

Fig. 1. Standard 6T SRAM cell. a) Circuit schematic. b) Stick diagram of a traditional cell layout. c) Stick diagram of a "thin cell" layout.

method requires for the last stage of the address decoder to be distributed inside the memory matrix.

Figures 1 b) and 1 c) show two most commonly used layout strategies for 6T SRAM cell design. In both of these strategies, power, ground and bit-line contacts are shared between the neighboring cells which reduces the area of the memory matrix. Figure 1 b) shows the traditional layout strategy which has been a standard in older technologies. However, this strategy is not suitable for technology nodes below $90nm$ due to transistor mismatch and signal integrity problems. In figure 1 c), a so-called "thin cell" layout strategy is shown [7]. This strategy has advantage over the traditional layout due to the fact that poly-silicon and diffusion lines are printed in only one direction, which reduces the mismatch of transistors. Due to the cell's aspect ratio, bit lines are placed further apart which improves the signal integrity issues. For these reasons "thin cell" layout has become the standard in newer technology nodes.

B. Power-analysis security of SRAM

Due to their symmetric and regular structure, SRAM arrays seem suitable for applying dual-rail precharge principle in order to achieve side-channel security. Since data signals are already dual-coded, this countermeasure should come without high area overhead. Furthermore, since SRAM matrices have very regular layout, no additional effort is needed for balancing capacitive loads of interconnect wires.

Data transfer in SRAM memories is performed using I/O circuits, sense-amplifiers, bit-line drivers, bit-lines and SRAM cells. In order to achieve power-analysis resistance, dual-rail precharge principle has to be applied in all of these components. The focus of this paper is on the SRAM cell.

During the write cycle, higher amount of energy is needed to change the state of the SRAM cell than to write the same value that is already stored. For this reason, the energy consumed during the write access is proportional to the number of cells that flip state. The rest of this paper is focused on improving the SRAM cell structure in order to remove this correlation.

III. Power-analysis resistant SRAM cells

In this section we analyze different possibilities for securing an SRAM cell against the power-analysis. Unfortunately, simply introducing the precharge phase into the write cycle would lead to high short-circuit currents. Therefore, the presented solutions rely on either cutting off the power supply or cutting the feedback inside the cell during precharge. First we give an overview of the power analysis resistant SRAM cell introduced in [6] which we will refer to as the "power-cut cell". We propose an improvement of this strategy, by sharing the PMOS power-cut switch between multiple cells. Finally, we propose a "feedback-cut cell" which relies on cutting the connections between inverters in order to avoid short-circuit current during precharge phase.

A. Power-cut cell

In order to perform writing to memory in a side channel secure manner, a power-cut SRAM cell has been proposed. This cell consists of 8 transistors as shown in figure 2. Two additional PMOS transistors per cell are added to enable power cut during the precharge phase. A precharge phase is introduced during the write access in order to write logic zeros in the internal nodes before the actual data is written. The value zero is chosen because NMOS transistors which connect internal nodes to bit-lines are better at passing logic zeros than logic ones. Gates of the power-cut PMOS transistors are connected to a word line, routed horizontally, and a $\overline{float}$ signal which is routed vertically. Power is cut only for the cells at the intersection of these two signals. The authors of [6] estimate the area overhead of this solution to 70%, but layout strategy or the dimensions of the memory matrix have not been reported.

B. Shared PMOS

An improvement in area consumption of the power-cut cell can be achieved by sharing the PMOS transistors between multiple cells as shown in figure 3. Two PMOS transistors

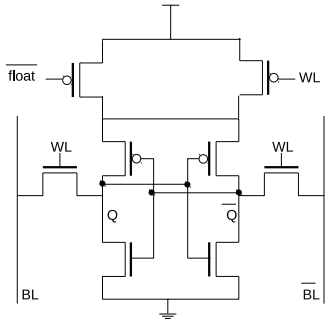

Fig. 2. Power-cut cell schematic.

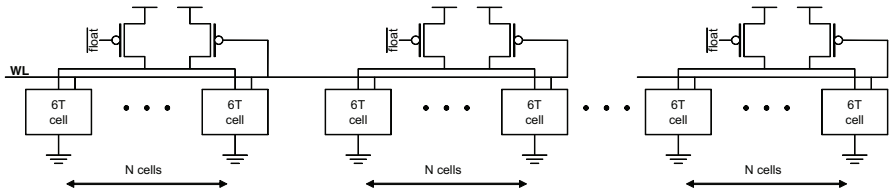

Fig. 3. Power-analysis secure cells with shared power-cut transistors.

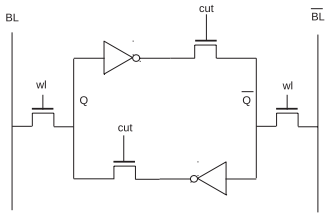

Fig. 4. Feedback-cut SRAM cell.

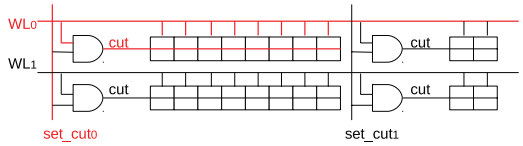

Fig. 5. Distribution of the *cut* signal in a design using feedback-cut cells.

form a power-cut switch. The number of cells which share one switch (N) is limited by the maximal current density. A current flowing through the metal line connecting the power contacts of 6T cells with the cut-off transistors has peak value during the write cycle. If this current is too high or if the metal line is too narrow, electromigration effect may damage the wire. Maximal current density in metal lines is specified by the foundry, and N should be chosen such that this restriction is not violated. This problem usually doesn't appear in standard SRAM design since power and ground lines are routed vertically.

In order to achieve the same performance as the power-cut cell, channel widths of the power-cut PMOS transistors have to be increased by the factor of N. However, area reduction is still obtained because of the reduced number of diffusion-to-metal contacts in layout. Additional improvement is in the dynamic power reduction since the number of $\overline{float}$ signal wires is reduced N times. This is a significant reduction since the length of these wires equals the height of the memory matrix which results in high capacitance that has to be fully discharged in every write cycle.

C. Feedback-cut cell

Somewhat different approach was taken in designing the feedback-cut cell (figure 4). Instead of cutting-off the power supply to prevent the short-circuit current, the feedback loop inside the SRAM cell is cut during the write access. Two NMOS transistors are added between inverter outputs and the data nodes. When the cell is not accessed and during the read access, signal cut is asserted to high logic value and the feedback loop is closed so that the stored data doesn't get lost. During the precharge phase of the write cycle cut signal is asserted low, feedback is cut and internal nodes are precharged to logic zero through the bit-lines. In order to avoid losing data in the non-accessed cells, cut signal wire connects only to the cells of the same word. This signal has to be routed in the same manner as fully-subdivided word lines, with control circuits inserted in the memory matrix as shown in figure 5.

IV. Cell properties

In this section we present circuit-level analysis of the secure SRAM cells. Results for the standard 6T SRAM cell are used for comparison. All results are obtained by HSPICE and SPECTRE simulations using TSMC 65nm device models. Channel dimensions of all transistors used in the SRAM cells are $L = 60nm$, $W = 150nm$. The dimensions of the power-cut PMOS in the shared PMOS configuration are $L_{PMOS} = 60nm$ and $W_{PMOS} = 1.2\mu m$. The configuration where $N = 8$ cells are shared between the power-cut switch is used.

A. Data stability

Maximal square method [8] is used to determine the cell stability. Static noise margin (SNM) is estimated as the side of the maximal square that fits the butterfly curve. Static noise margin of the non-accessed cell (SNM_{hold}) is used as a measure of the cell's stability while it is not being accessed. Noise margin during the read access (SNM_{read}) corresponds to the capability of the cell to retain it's data in the read operation mode. SNM_{read} is lower than SNM_{hold}.

Figure 6 shows the butterfly curve of the power-cut cell. The curve of the standard SRAM cell is shown in the same graph with a dashed line. It can be seen from the figure that static noise margin is higher for the power-cut cell. Butterfly curves of the shared PMOS structure are not visibly different from the ones of the 6T cell. Figure 7 shows the butterfly curve of the feedback-cut cell. The main drawback of this cell is the fact that data nodes Q and $\overline{Q}$ are never charged to the maximal value. Since there is pass-transistor between the inverter output and the data node which stores logic one, this node is charged to the value $V_{dd} - V_{T_{nmos}}$, which results in lower noise margins. This is visible in figure 7. This effect may cause scalability problems when moving to advanced technology nodes.

TABLE I
NOISE MARGINS FOR PROCESS CORNERS

	$SNM_{hold}[mV]$					$SNM_{read}[mV]$				
Corner	TT	SS	SF	FS	FF	TT	SS	SF	FS	FF
6T cell	392	416	391	354	351	154	181	206	99	110
Power-cut cell	408	429	424	359	367	152	181	204	97	103
Shared PMOS	391	418	396	349	345	153	182	205	98	107
Feedback-cut	376	338	282	354	351	133	138	174	63	79

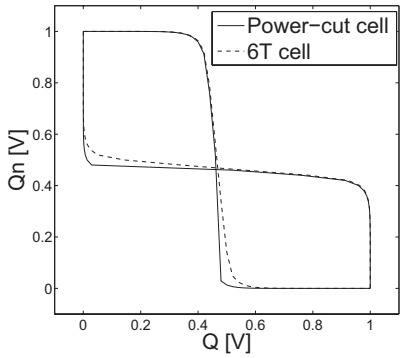

Fig. 6. Butterfly curve of the power-cut cell (full line) and the 6T cell (dashed line).

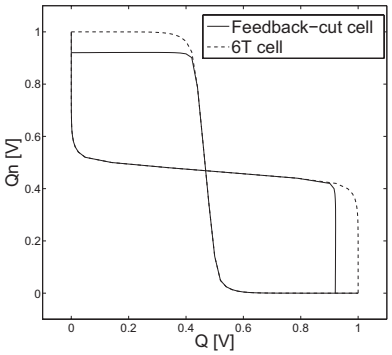

Fig. 7. Butterfly curve of the feedback-cut cell (full line) and the 6T cell (dashed line).

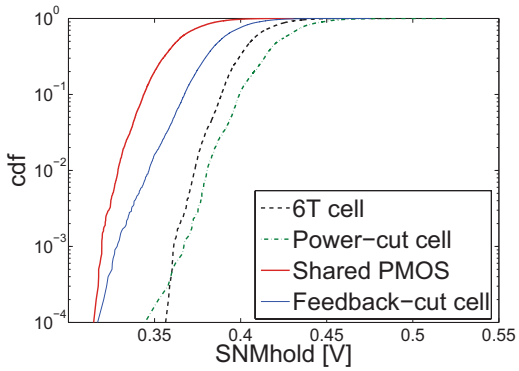

Fig. 8. Static noise margin when the cell is not accessed.

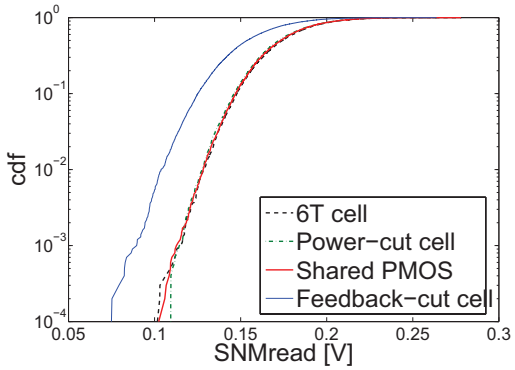

Fig. 9. Static noise margin during the read access.

Static noise margins of the presented cells for different process corners are summarized in table I. The only value significantly below $100mV$ is the read noise margin of the feedback-cut cell for the worst-case corner. This value, however is still above $50mV$, so read upset problems are not expected.

In order to evaluate the distribution of noise margins under process variations, Monte Carlo simulations were performed using 10000 iterations. Graphs showing a comparison of cumulative distribution functions for different cell types are shown in figures 8 and 9. SNM_{hold} is way above $100mV$ for most cells of all types. Therefore, data retention problems are not expected. It can be seen that probability distributions for SNM_{read} are almost identical for the standard cell, power-cut cell and the shared PMOS structure. As expected, feedback-cut cell will have lower margins in more cases, which implies the lowest yield for this type of cell.

B. Read delay

Before the read access, bit line pair is precharged to a logic high value. After the word line is activated, one of the bit-lines is discharged through the SRAM cell until a sufficient voltage swing is developed to activate sense amplifiers. Read delay depends on the bit-line capacitance, current through the SRAM cell and the minimal voltage swing required by the sense amplifiers.

In order to compare read currents of the proposed cells we used a simple simulation setup shown in figure 10. BL capacitance was estimated by designing a layout of a small memory matrix in which each BL pair connects to 128 cells. Parasitic capacitance extracted from the layout was approximately $50fF$, so this value was used in simulations. Read

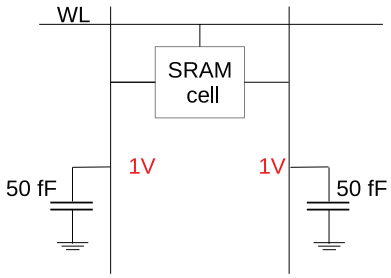

Fig. 10. Simulation setup for comparing read delay time.

TABLE II
READ DELAY.

Cell type	Read delay [ps]
6T cell	345
Power-cut cell	344
Shared PMOS	343
Feedback-cut cell	517

delay is defined as the time interval from the activation of the WL until the voltage swing of $200mV$ develops on the bit-lines. Results are summarized in table II. Feedback-cut cell is slower than the others due to the additional NMOS in the pull-down path.

C. Layout strategy

Feedback-cut cell layout strategy is presented in figure 11. In this layout polysilicon and diffusion lines are printed in only one direction which should reduce transistor mismatch and provide good scalability. This is the preferred technique for small technology nodes. This type of layout is unfortunately not applicable to shared PMOS structure since in this structure it is not allowed to share power-contacts between the cells connected to the same bit-line pair. For this reason, traditional cell layout as shown in 1 b) should be used. Major disadvantage of this strategy is the fact that poly and diffusion lines are printed in both directions which is not suitable for lower technology nodes and will probably result in area overhead. From the side-channel security point of view, disadvantage of the traditional layout strategy is the systematic mismatch between the pull-down and the access transistors. Introduced

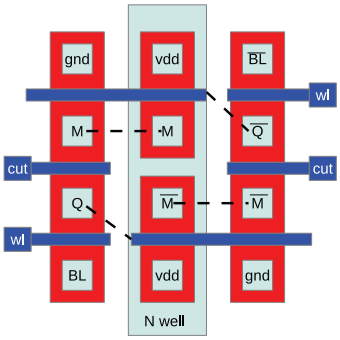

Fig. 11. Stick diagram of the feedback-cut cell.

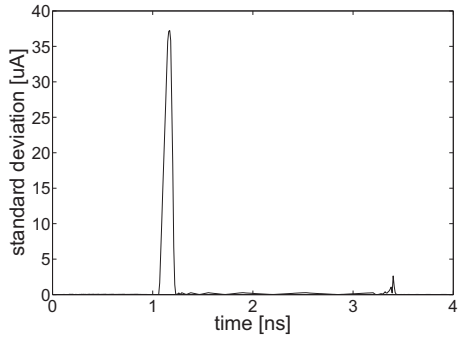

Fig. 12. Standard deviation over the inputs for different time samples for the standard 6T cell during the write cycle.

asymmetry will make the cell more vulnerable to side-channel attacks.

V. SECURITY ANALYSIS

Simulation of the write cycle of the 8-bit word for each cell type was performed for the purpose of estimating the resistance against power analysis. Simulations were performed using Hspice simulator and TSMC 65nm transistor models. Simulated power-traces correspond to 256 writes of all possible values when the previously stored value is 0. After the power traces were produced and aligned, standard deviation was computed over the inputs for each point in time. Standard deviation curves, obtained this way are shown in figures 12, 13, 14 and 15. These curves provide insight into which parts of the power trace carry the most information about the processed data since higher maximal deviation indicates higher information leakage. This methodology is known to give results which differ from the actual measurement data, but it is still good for estimating the order of magnitude of the information leakage [9]. In case that the deviations of the power supply are smaller than the noise in the circuit or the quantization step of the measurement setup, the attacker will not be able to carry out a successful attack.

Maximal deviation for the standard SRAM cell is above $35\mu A$. For secure SRAM cells this value is lower by four

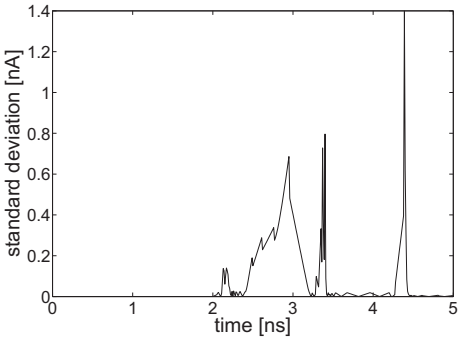

Fig. 13. Standard deviation over the inputs for different time samples for the power-cut cell during the write cycle.

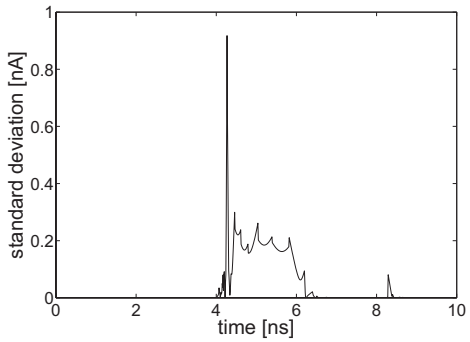

Fig. 14. Standard deviation over the inputs for different time samples for the shared PMOS structure during the write cycle.

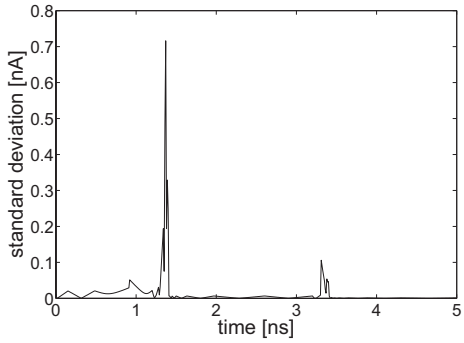

Fig. 15. Standard deviation over the inputs for different time samples for the feedback-cut cell during the write cycle.

orders of magnitude. It is noticed that standard deviation curves depend on the slope of the input signals, as well as the time step of the simulation. However. based on this initial analysis, it can already be concluded that all three secure cell types cause less information leakage compared to the standard SRAM cell. Further investigation, including the chip-fabrication and the measurement results, is needed in order to compare side-channel security of these three cell types.

VI. Conclusions and future work

This paper shows that the dual-rail precharge principle which is often applied in secure logic styles, can also be used to design SRAM cells with improved side-channel security. In order to apply this principle without causing high short-circuit currents one of the two methods can be used: cutting the power supply or cutting the feedback loop. Power-cut cell, and the newly introduced shared-PMOS structure and feedback-cut cell, all demonstrate significantly lower variations of supply current compared to the standard SRAM design, which implies better resistance against power-analysis.

From the data stability point of view, power-cut and shared PMOS are superior to feedback-cut cell due to the higher noise margins, and do not differ significantly from the standard memory cell. One of the drawbacks of the power-cut cell is the requirement of one additional vertically routed wire per column which is activated in every write cycle and operates in full-swing mode. This will typically lead to high dynamic power consumption. Shared PMOS structure partially avoids this problem due to the decreased number of vertically routed signal wires. The biggest drawback of this structure is the fact that the thin-cell layout cannot be used. However, in $90nm$ and older process technologies this should not be a problem. The biggest advantage of the feedback-cut cell is the simple compact layout strategy with polysilicon and diffusion lines printed in only one direction. We were not able to find such strategy for the other two cell types without causing significant area overhead.

Future work on this topic includes exploring different memory architectures for each type of cell and comparing them in terms of area and dynamic power consumption. Side-channel secure design of other memory components such as sense-amplifiers and data latches is also a topic to look into. The effect of process variations on side-channel security should be considered for each cell type. Finally, once the optimal solution is found, chip fabrication and measurement results are needed to prove the improved security features.

Acknowledgment

This work was supported in part by the Research Council K.U.Leuven: GOA TENSE (GOA/11/007), by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy) and by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II. In addition, this work was supported by the Flemish Government, FWO G.0550.12N and by the European Commission through the ICT programme under contract FP7-ICT-2011-284833 PUFFIN and FP7-ICT-2007-238811 UNIQUE.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology CRYPTO 99*, ser. LNCS, M. Wiener, Ed. Springer Berlin / Heidelberg, 1999, vol. 1666, pp. 789–789.

[2] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *CHES 2004*, ser. LNCS. Springer Berlin / Heidelberg, 2004, vol. 3156, pp. 135–152.

[3] S. Chari, J. Rao, and P. Rohatgi, "Template attacks," in *CHES 2002*, ser. LNCS. Springer Berlin / Heidelberg, 2003, vol. 2523, pp. 51–62.

[4] K. Tiri and I. Verbauwhede, "A digital design flow for secure integrated circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, no. 7, pp. 1197–1208, 2006.

[5] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Solid-State Circuits Conference, 2002. ESSCIRC 2002. Proceedings of the 28th European*, 2002, pp. 403 – 406.

[6] E. Konur, Y. Ozelci, E. Arikan, and U. Eksi, "Power Analysis Resistant SRAM," in *Automation Congress, 2006. WAC '06. World*, july 2006, pp. 1 –6.

[7] M. Ishida, T. Kawakami, A. Tsuji, N. Kawamoto, M. Motoyoshi, and N. Ouchi, "A novel 6T-SRAM cell technology designed with rectangular patterns scalable beyond 0.18 mu;m generation and desirable for ultra high speed operation," in *Electron Devices Meeting, 1998. IEDM '98 Technical Digest., International*, dec 1998, pp. 201 –204.

[8] E. Seevinck, F. List, and J. Lohstroh, "Static-noise margin analysis of mos sram cells," *Solid-State Circuits, IEEE Journal of*, vol. 22, no. 5, pp. 748 – 754, oct 1987.

[9] M. Renauld, D. Kamel, F.-X. Standaert, and D. Flandre, "Information Theoretic and Security Analysis of a 65-Nanometer DDSLL AES S-Box," in *CHES*, 2011, pp. 223–239.