Power-Gated MOS Current Mode Logic (PG-MCML): a Power Aware DPA-Resistant Standard Cell Library

Alessandro Cevrero[1,2], Francesco Regazzoni[3,4], Micheal Schwander[1]
Stephane Badel[1], Paolo Ienne[2], and Yusuf Leblebici[1]

[1]School of Engineering - EPFL, Lausanne, Switzerland. {first_name.last_name}@epfl.ch
[2]School of Computer and Communication Sciences - EPFL, Lausanne, Switzerland. paolo.ienne@epfl.ch
[3]ALaRI - University of Lugano, Lugano, Switzerland. regazzoni@alari.ch
[4]UCL Crypto Group, Université catholique de Louvain, Louvain-la-Neuve, Belgium.

ABSTRACT

MOS Current Mode Logic (MCML) is one of the most promising logic style to counteract power analysis attacks. Unfortunately, the static power consumption of MCML standard cells is significantly higher compared to equivalent functions implemented using static CMOS logic. As a result, the use of such a logic style is very limited in portable devices. Paradoxically, these devices are the most sensitive to physical attacks, thus the ones which would benefit more from the adoption of MCML.

We propose to overcome this limitation by reducing drastically the static power consumption of MCML-based cryptographic circuits. To this end, we designed Power Gated MCML (PG-MCML), a standard cell library featuring a sleep transistor in every cell. The effects of the sleep transistor on performance as well as on area are negligible. Moreover, the proposed differential library is supported by conventional EDA tools.

We evaluated our standard cell library using Advanced Encryption Standard (AES) as benchmark and we compared the power consumption, the area, and the DPA-resistance figures with the ones of static CMOS and conventional MCML. Our results show that our PG-MCML library can achieve a power consumption comparable with the one of static CMOS, thus proving that PG-MCML cells can suit the strict power budget of battery operated devices.

Categories and Subject Descriptors

B.7.1 [**Integrated Circuits**]: Types and Design Styles — *Algorithms implemented in hardware, Standard cells.*

General Terms

Security, Design.

Keywords

Security, DPA, Current Mode Logic, Side Channel Attacks.

1. INTRODUCTION

The static CMOS design style is adopted in almost all digital applications. Such a wide spread diffusion is mainly due to its robustness and the negligible static power consumption (as long as the leakage dissipation is not dominant). Nevertheless, there are specific requirements which cannot be fulfilled by static CMOS.

The most relevant application for which CMOS does not represent the best solution is embedded system security. In fact, devices such as smart cards or wearable systems are characterized by a limited power budget, but they also need to be robust against power analysis attacks. Such attacks, first demonstrated in 1999 [8], exploit the correlation between the power consumed by the device and the data being processed to recover the secret key.

It is widely accepted that robustness against side channel attacks can not be achieved using static CMOS: its data-dependent power consumption is the key enabler for the attack. On the contrary, MCML would be an appealing candidate, since its power consumption is almost independent from the specific input patterns or fan-out conditions. Yet, the area overhead, the lack of tool support, and the large static power consumption, have limited the diffusion of such design option. Recently, the CAD tool problem was mitigated by the work of Badel et al. [2], which proposes a standard cell MCML library and discusses the problem of integrating such library into place and route tools. Yet, to date, the high power consumption was not addressed.

In this paper we solve this problem by applying a power gating technique to MCML standard cells. The current-based operation of the MCML logic style allows us to add power gating to each cell with a negligible cost. We thus implement a fine grain power gating technique suitable for MCML cells and we built a MCML standard cell library to support it. Our approach leads to a drastic reduction of the power consumed by MCML, paving the way to a widespread use of MCML as protected logic style in embedded systems. To the best of our knowledge, this work represents the first successful attempt to realize a library robust against power analysis attacks which meets the low power constraints of small and medium size modern embedded systems.

2. RELATED WORK

MCML has been introduced by Yamashina et al. in 1992 [17] as a new logic style targeting, at least initially, high-speed and mixed signal applications. To this end, MCML offers reduced voltage swing and differential operation, two key elements needed to reduce the generation of switching noise. In addition, power consumption is independent of the operating frequency.

Due to these advantageous characteristics, MCML circuits have been implemented in various demanding applications such as high-speed ring oscillators, frequency dividers, and multi-channel data multiplexing [13, 4, 5, 7]. Since the power consumption depends less strongly on the particular switching activity or the operating frequency, when used in multi-GHz applications, MCML circuits typically consume less power than conventional design styles.

Recently, with the advent of power analysis attacks [8] and the differential power analysis (DPA) in particular, another application for MCML has appeared. DPA-resistant logic gates, in fact, should not exhibit a significant input pattern-dependence with respect to current drawn from the power supply [16]. Indeed, MCML outperforms other DPA-resistant logic styles [15, 11] considering the current fluctuations produced during switching events. On the negative side, the power consumed when the device is not switching limits MCML utilization in medium or low frequency applications.

One of the first attempts of reducing the power consumed by current mode logic styles was presented by Allam et al. [1]. In their work, the authors proposed Dynamic Current Mode Logic (DyCML), which combines the advantages of conventional MCML with the ones of dynamic logic. Unlike CML circuits, DyCML gates employ a dynamic current pulse. As a consequence, the power dissipation is only due to the gates which are processing data. However, the complexity associated with the dynamic current source generation limits the applications of DyCML in advanced nodes. Moreover, it is not possible to use conventional EDA tools to design circuits based on DyCML. Thus, the use of DyCML is considered unpractical.

More recently, Badel et al. [2] proposed a standard cell design methodology suitable for differential circuit style. Their work reports a successful design of a MCML based standard cell library supported by conventional EDA tools. However, the library used by Badel et al. was not designed targeting embedded applications.

To minimize the area and the cost overhead due to MCML gates, researchers considered to use them only for critical cryptographic operations and to realize the rest of the design with static CMOS libraries [12]. This approach mitigates the area overhead of secured cryptographic circuits. However, a large scale utilization of conventional MCML was never considered since the power consumption is usually prohibitive for embedded applications.

To this end, the power gated MCML library presented in this paper is the first attempt toward widespread diffusion of this technology in secure embedded systems. In fact, the proposed sleep transistor insertion is much simpler compared to the one of DyCML and it is easier to be implemented. Moreover, our library is fully supported by commodity EDA tools.

3. MCML OPERATING PRINCIPLE

MCML is a fully differential logic style with reduced voltage swing. Every MCML gate consists of three main blocks, namely the current source, the NMOS network and the load resistors. The current source provides a constant bias current I_{SS}. The NMOS network realizes the Boolean function and steers the current to one of the output load resistors resulting in a voltage drop at one of the output terminal. The other output will be at the same potential of the supply voltage V_{dd} since no current is flowing through the resistor. The

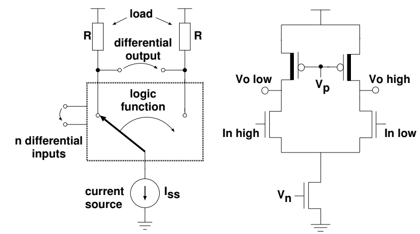


Figure 1: MCML operating principle (left) and schematic of a buffer/inverter (right).

resulting voltage swing is defined as the difference between the output levels and it is given by Eq. 1.

$$V_{SW} = V_{DD} - I_{SS} \cdot R \qquad (1)$$

The current source is implemented using a NMOS transistor operated in the saturation region. The logic function is realized by a NMOS network that implements the corresponding binary decision diagram (BDD). The load resistors can be implemented either as passive or active devices. Passive resistors occupy large silicon area and are highly sensitive to process variations. There is typically a tolerance of 20 to 30% of the nominal value. Active load devices can be implemented with PMOS devices which are biased in linear region to produce a tunable load resistance.

Fig. 1 shows the basic principle of a MCML cell and the transistor arrangement of a MCML buffer/inverter. As the logic is fully differential, the inverted logic function is obtained by exchanging the positive and the negative output nodes. Depending on the complexity of the logic function, several levels of stacked differential pairs may be needed. The bias voltage V_p defines the resistivity of the active load, while V_n determines the tail current. V_p, V_n, and sizing are the design parameters which determine the performances of MCML circuits. Power dissipation is a function of V_n and it is defined by $V_{dd} \times I_{ss}$.

4. PG-MCML CELLS DESIGN

Power gating [6] is a technique which reduces the static power consumption of a digital circuit by inserting power switches (sometimes referred as sleep transistors) in the supply path. To implement this technique, two solutions have been proposed in the past: *coarse-grain power gating*, in which complete blocks are disconnected from the power supply and the ground through a common power switch, and *fine-grain power gating*, in which every standard cell contains a sleep transistor internally.

In conventional static CMOS circuits, the use of fine grain power gating causes a significant area overhead and negatively affects performance. For this reason, coarse grain power gating is the preferred approach for static CMOS.

On the contrary, the insertion of a sleep transistor in each MCML cell introduces negligible power overhead. Also, the switching speed is not directly affected by the sleep transistor since it is located outside the signal path. Therefore, in our library, we implemented fine grain power gating, which suits better the needs of MCML cells.

Moreover, a fine grain power gating allows to selectively switch off each standard cells depending on the circuit topology: this step can be easily automated during the synthesis process, using an approach similar to automatic clock gating.

Table 1: Area comparison between conventional MCML and PG-MCML standard cells in 90 nm CMOS technology.

Cell	MCML [μm^2]	PG-MCML [μm^2]
BUFX1	7.056	7.448
MUX4X1	19.7568	20.8544
AND4X1	16.9344	17.8752
DLX1	8.4672	8.9376

However, it should be taken into account that many of the existing synthesis tools currently do not offer the capabilities of fine grain power gating. This issue will be detailed in Section 5.

Different power gating topologies for MCML standard cells are depicted in Fig. 2. The solutions (a) and (b) use a transistor to pull down the bias voltage V_n to ground during the sleep mode. Solution (c) applies just a ON signal to the gate of the current source and connects the bulk voltage to the bias voltage V_n. Option (d) consists of an additional sleep transistor in series with the current source.

Indeed, solution (a) was discarded since it requires the use of a large bandwidth source follower amplifier to settle the output voltage to V_n within a single clock cycle.

Option (b) slightly improves option (a). However, this solution was discarded too, since it requires the insertion of two transistors per cell. Solution (c) relies on the body-biasing principle and modulates the bias current adjusting the threshold voltage. However, to ensure a correct functionality in all the process corners, the voltage V_n needs to range from -500 mV to 1 V. Such voltage is difficult to obtain in practice. In addition, the current source is sitting in a separate well. This solution leads to a significant area overhead. For all the above reasons, we selected solution (d). It can be seen from the Fig. 2 that the sleep transistor is located on top of the current source. Thanks to this choice, the sleep transistor has a negative V_{GS} voltage during power down, decreasing the leakage current.

Table 1 shows the silicon area of MCML gates with and without sleep transistor. On average, the cells with sleep transistor are approximately 6% larger than conventional MCML gates.

5. LIBRARY AND DESIGN FLOW

The PG-MCML library proposed in this work is based on the standard cell design methodology proposed by Badel et al. [2]. To demonstrate the benefit of power gating on a real circuit we designed a relatively small library, including 16 cells. Nevertheless, it is worth to mention that an increased number of cells would positively affects our results because of the higher flexibility offered during synthesis, placement and routing. The internally developed PG-MCML library is specifically optimized for area and power, and the switching speed of the PG-MCML cells is similar to the one of their CMOS counterparts implemented on the same technology. As previously mentioned, the main target application is security, with particular emphasis on battery operated embedded systems which need to be robust against power analysis attacks.

The main difference between a MCML standard cell which includes a sleep transistor and its conventional counterpart is that, in the former, the minimal supply voltage and the current source are slightly increased. Finally, to minimize the layout area, we designed the sleep transistor and the current source with the same channel width to share the same diffusion region.

Table 2: Area and delay characteristic of the PG-MCML library.

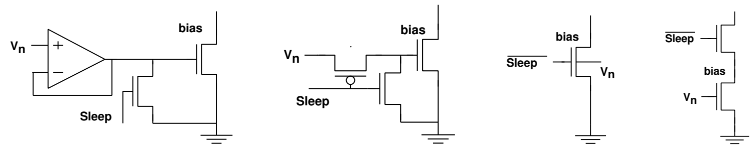
Cell	Area [μm^2]	Delay [ps]	MCML area/ CMOS area
Buffer	7.448	23.97	2.4
Diff2Single	8.9376	80.41	
AND2	8.9376	41.34	1.9
AND3	13.40641	68.74	2.1
AND4	17.8752	99.96	2.8
MUX2	8.9376	43.58	1.2
MUX4	20.8544	87.11	1.2
MAJ32	17.8752	82.32	
XOR2	8.9376	44.26	1.1
XOR3	17.8752	84.37	1.1
XOR4	20.8544	109.68	1.1
D-Latch	8.9376	36.32	1.3
DFF	17.8752	53.4	1.3
DFFR	26.8128	69.33	1.8
EDFF	23.8336	63.53	
FA	35.7504	84.49	1.4

The PG-MCML library is designed using a 90 nm CMOS process. To improve timing, area, and power we implemented each cell using a combination of low-V_t and high-V_t transistors. Indeed, high-V_t devices can reduce the leakage current during sleep mode without affecting the cell delay, thus we selected them for the NMOS Boolean network, the current source and the sleep transistor. We used low-V_t devices for the PMOS load, since this approach leads to the smallest silicon area. Furthermore, smaller active loads have less parasitic and thus they lead to higher speed. To determine the optimal bias current I_{ss}, we explored how the cell delay and the power consumption vary in function of the tail current. Fig. 3 (a) depicts the delay for a MCML buffer/inverter driving FO1 and FO4 loads. Interestingly, increasing the bias current above 250 μA provides a limited speed improvement with a large penalty in cell area. Fig. 3 (b) depicts the power delay product under different bias conditions. The simulation based evaluation revealed a minimum area delay product at 50 μA.

Table 2 shows area and delay for the cells belonging to the PG-MCML library. An area comparison between equivalent cells in a commercial 90 nm standard cell library is also provided. PG-MCML cells are 1.6 times larger in average. To the best of our knowledge, this is the smallest area overhead measured for a power analysis resistant library so far. Fig. 4 depicts the schematic and the layout view of a buffer cell belonging to the PG-MCML library. Both driving strengths one and four are shown.

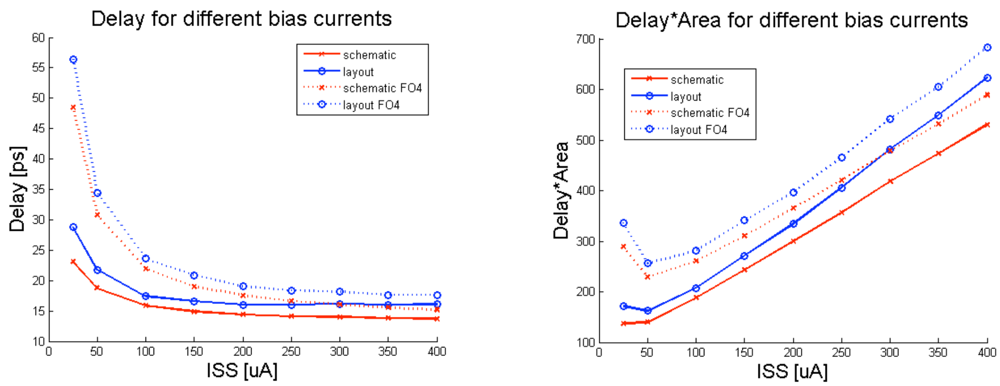
Our cells are designed to support fine grain power gating. Theoretically, in a design, there are several power gating opportunities which could be detected automatically and exploited during synthesis. However, since modern synthesis tools are specifically designed for conventional CMOS libraries, they do not support fine grain power gating. Due to this limitation, we were forced to manually connect the sleep transistor. For fine-grained power gating applications, each individual sleep input of all cells in a cluster can be driven collectively, provided that the signal is sufficiently buffered.

The design flow used for PG-MCML is based on commod-



(a) (b) (c) (d)

Figure 2: Different power gating techniques for MCML circuits.



(a) (b)

Figure 3: Delay and Area delay trade-off for a MCML inverter driving FO1 and FO4 loads .

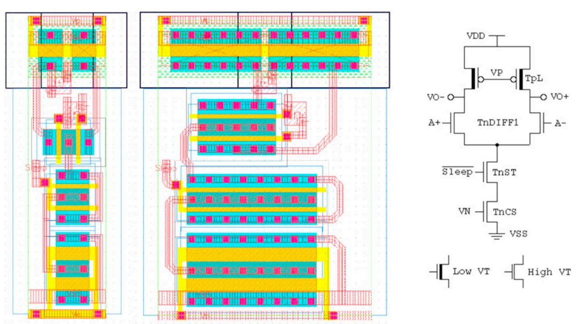


Figure 4: Schematic and layout views of a PG-MCML buffer with drive strength X1 and X4. The bias transistor is laid out close to the ground rail while PMOS load transistors are placed below the power rail. The sleep transistor is located next to the bias transistor for minimal silicon area. Intra-cell routing is limited to Metal-1 to facilitate inter cell routing using upper metal layers.

ity EDA tools for synthesis, placement and routing. We used *Synopsys Design Compiler* for synthesis and *Cadence Encounter Digital Implementation* for placement and routing. The last step exploits the fat-wire approach [2], which ensures that both wires of a differential signal are routed side by side (to have the same delay and load). In order to switch off and on the controlled logic in a fraction of the clock cycle (in the order of few ns), the sleep signal, managing the power gating, should be buffered.

In practice, to control skew and propagation delay from the root to the individual sleep input of all cells in a cluster, the sleep signal is routed and buffered as a balanced tree. Also, single ended clock buffers are used to route it with a controllable insertion delay. To integrate such cells with the PG-MCML library, we designed and characterized static CMOS buffer/inverters with the same height as the PG-MCML cells. The *clock tree synthesis (CTS)* engine available in the place and route tool is used to synthesize the buffer tree and route the sleep signal. In this way, we could exploit capabilities already existing in digital design tools.

6. DPA RESISTANT PROCESSOR

As previously discussed, the main target applications of the proposed PG-MCML library are embedded systems which have to be robust against power analysis attacks. For these devices, the most critical aspect is security. However, since they are very often battery operated, minimizing the power cost of the security features is an important goal.

Interestingly, very often, cryptographic functions included in embedded devices are inactive over a long period of time, thus our PG-MCML library is suitable for implementing these blocks. An appealing target for PG-MCML is represented by the DPA-resistant instruction set extension (ISE) recently proposed in literature [14, 12]. In these works, the authors proposed to augment a processor, realized with conventional standard cell libraries, with additional functional units (in the form of custom instructions) implemented in a logic style robust against power analysis attacks. Considering the relevance of such an example, we used the same approach to evaluate the power consumption of PG-MCML.

We started from a software implementation of the AES algorithm [10] and we augmented the OpenRISC 1000 [9] 32-bit embedded processor with a custom functional unit, sitting in the processor's pipeline, consisting of four identical S-boxes (each S-box is implemented in the form of 8 × 8 look-up-table) to match the processor's word size. The new custom instruction is labeled S-box ISE. Both the processor and the custom instruction are available as RTL code. We synthesized, placed and routed three different versions of the considered core. In all cases, the processor was realized using the reference static CMOS technology, a 90 nm commercial standard cell library, while the protected instruction was implemented using the same conventional CMOS technology, the conventional MCML and the PG-MCML respectively.

The custom functional unit implemented with differential cells was connected to the processor by means of converters and it appears in the processor's layout as a macro block. The full design was synthesized, placed and routed setting 400 MHz as operating frequency (to meet the speed requirement of modern embedded systems) and a software implementing the AES cipher was repeatedly executed 5000 times using a random plain-text. The full AES algorithm was simulated with a logic simulator (*Mentor Graphics Modelsim*) using the post place and route netlist and the delay back annotation (in SDF format) as input.

For such a benchmark, the S-box ISE under evaluation was active 0.01% of the whole execution time. The signal triggering the custom instruction's execution controls also the sleep signal, so that the protected logic is turned on only during the custom instruction execution. The sleep signal is shared among all the cells that compose the custom instruction and its insertion delay is approximately 1 ns. This allows us to turn on the custom instruction in a small fraction of the clock period and to process the data within the same cycle. The circuit's functionality has been verified in simulation.

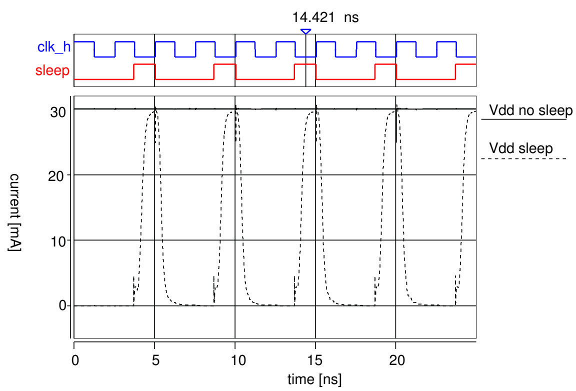


Figure 5: Current waveform for S-box ISE with and without power gating implemented. The sleep signal waveform for the power gated implementation is also plotted.

The custom instruction's inputs, stored in VCD format, are then used to run transistor level simulations (using *Synopsys Nanosim* as fast SPICE simulator) to monitor the custom instruction's current consumption. Fig. 5 depicts the current waveform of the S-box ISE realized with conventional MCML (dashed line) and the one realized with our PG-MCML (solid line). The clock and sleep signals are also depicted. It can be seen how our power gating allows to significantly decrease the power consumption: the current drawn by the conventional MCML circuit is always flat (around 30 mA), while the current absorption of the power gated S-box ISE is almost negligible when encryption is not performed (sleep signal low).

	CMOS	MCML	PG-MCML
Cells	3865	2911	3076
Area [μm^2]	30'547.52	77'378.97	78'355.21
Delay [ns]	0.630	0.698	0.717
Avg Power [W]	207.72u	490.56m	47.77u

Table 3: Area, delay, and power consumption on the S-box ISE implemented in different logic styles.

The overall results are summarized in Table 3, which reports the area, the gate occupation, the delay, and the power consumption for the considered S-box instruction set extension implemented in three different logic styles. The average power consumption of PG-MCML is significantly lower compared to the one of conventional MCML (reduced by a factor or 10^4). Also, it can be noticed that PG-MCML consumes four times less power than CMOS. This data should not suggest that PG-MCML is less power hungry than static CMOS logic, since when power gating techniques are applied to CMOS, the power consumption of this technology is significantly reduced. Finally, it can be seen that the area overhead necessary to support the sleep signal is negligible (the PG-MCML is roughly 1000 μm^2 larger compared to conventional MCML).

Considering the specific application field, we also carefully evaluated the robustness against power analysis attacks of the PG-MCML library. To evaluate the security, we synthesized, placed and routed the commonly accepted reduced version of the AES algorithm composed by a key addition and a S-box look-up-table. Each implementation was realized using three different technologies: the reference static CMOS, the conventional MCML, and the PG-MCML. For all of them, we performed SPICE simulation to extract the instantaneous current of all possible plain-text secret key pairs, using very high resolution both for current (1 μA) and time (1 ps). Finally, we repeatedly attacked all the implementation using as power model the Hamming weight of the S-box output [3].

As expected, all the attacks on the CMOS implementations were successful, while none of the ones performed on conventional MCML as well as on PG-MCML were able to reveal the secret key. In fact, as it can be seen from Fig. 6, which reports an example of correlation power attack (CPA) on PG-MCML, the secret key, plotted in black, is not distinguishable from all the other key guesses plotted in light gray. Our experiments showed that the security level achievable using the proposed PG-MCML is comparable to the conventional MCML, thus the insertion of the sleep signal does not introduce a negative effect on robustness against power analysis attacks.

7. CONCLUSION

In this paper we have presented a fine grain power gating technique for MCML circuits. A standard cell library implementing the proposed strategy has been designed in 90 nm CMOS technology. The library can synthesize, place and route any circuit starting from its RTL description; therefore, it can be directly used by designers with a limited additional effort.

We have demonstrated that our power gating approach dramatically reduces DC power consumption typical of conventional MCML cells while maintaining the same level of

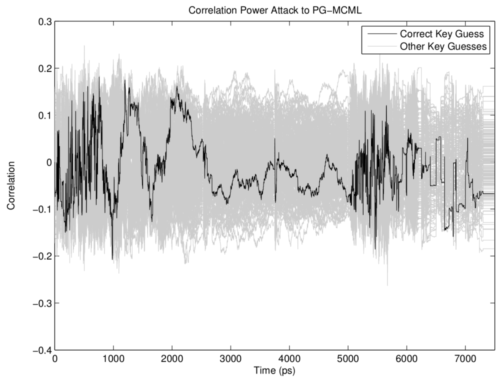


Figure 6: Correlation power attacks to PG-MCML: the black line, corresponding to the secret key, is not distinguishable.

security. Moreover, the insertion of the sleep transistor does not reduce the performances of the conventional MCML cells and we proved that the proposed library is a promising technology for implementing DPA resistant embedded systems. Automatic insertion of sleep signal during synthesis will be investigated in future work.

8. ACKNOWLEDGMENT

This research was partially supported by the Swiss Confederation Nanotera program, under the NTF "ULP-systems" and "SecWear" projects.

9. REFERENCES

[1] M. W. Allam and M. I. Elmasry. Dynamic current mode logic (DyCML): A new low-power high-performance logic style. *IEEE Journal of Solid-State Circuits*, 36(3):550–58, Mar. 2001.

[2] S. Badel, E. Guleyupoglu, O. Inac, A. P. Martinez, P. Vietti, F. K. Gürkaynak, and Y. Leblebici. A generic standard cell design methodology for differential circuit styles. In *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition*, pages 843–48, Munich, Mar. 2008.

[3] E. Brier, C. Clavier, and F. Olivier. Correlation power analysis with a leakage model. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems—CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29. Springer, Berlin, Sept. 2004.

[4] H. Bui and Y. Savaria. 10 GHz PLL using active shunt-peaked MCML gates and improved frequency acquisition XOR phase detector in 0.18 μm CMOS. In *4th IEEE International Workshop on System-on-Chip for Real-Time Applications, 2004. Proceedings*, pages 115–118, 2004.

[5] H. Bui and Y. Savaria. Shunt-peaking in MCML gates and its application in the design of a 20 Gb/s half-rate phase detector. In *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*, volume 4, 2004.

[6] S. Henzler. *Power management of digital circuits in deep sub-micron CMOS technologies*. Springer Verlag, 2006.

[7] M. Houlgate, D. Olszewski, K. Abdelhalim, and L. MacEachern. Adaptable MOS current mode logic for use in a multi-band RF prescaler. In *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*, volume 4, 2004.

[8] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology—CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412. Springer, Berlin, Aug. 1999.

[9] D. Lampret. *OpenRISC 1000 Architecture Manual*, Apr. 2006.

[10] NIST. Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, November 2001.

[11] T. Popp and S. Mangard. Masked dual-rail pre-charge logic: DPA-resistance without routing constraints. In J. R. Rao and B. Sunar, editors, *Cryptographic Hardware and Embedded Systems—CHES 2005*, volume 3659 of *Lecture Notes in Computer Science*, pages 172–86. Springer, Berlin, Aug. 2005.

[12] F. Regazzoni, A. Cevrero, F.-X. Standaert, S. Badel, T. Kluter, P. Brisk, Y. Leblebici, and P. Ienne. A design flow and evaluation framework for DPA-resistant instruction set extensions. In C. Clavier and K. Gaj, editors, *Cryptographic Hardware and Embedded Systems—CHES 2009*, Lausanne, Switzerland, Sept. 2009.

[13] A. Tanabe, M. Umetani, I. Fujiwara, T. Ogura, K. Kataoka, M. Okihara, H. Sakuraba, T. Endoh, and F. Masuoka. 0.18 μm CMOS 10 Gb/s multiplexer/demultiplexer ICs using current mode logic with tolerance to threshold voltage fluctuation. *IEEE Journal of Solid-State Circuits*, 36(6):988–996, 2001.

[14] S. Tillich and J. Großschädl. Power analysis resistant AES implementation with instruction set extensions. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems—CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 303–19. Springer, Berlin, Sept. 2007.

[15] 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 *Proceedings of the 28th European Solid-State Circuits Conference*, pages 403–6, Florence, Sept. 2002.

[16] K. Tiri and I. Verbauwhede. Securing encryption algorithms against DPA at the logic level: Next generation smart card technology. In C. D. Walter, Çetin Kaya Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems—CHES 2003*, volume 2779 of *Lecture Notes in Computer Science*, pages 125–136. Springer, Berlin, Sept. 2003.

[17] M. Yamashina and H. Yamada. An MOS current mode logic (MCML) circuit for low-power sub-GHz processors. *IEICE Transactions on Electronics*, 75(10):1181–1187, 1992.