A Simulation-Based Methodology for Evaluating the DPA-Resistance of Cryptographic Functional Units with Application to CMOS and MCML Technologies

Francesco Regazzoni[1], Stéphane Badel[2], Thomas Eisenbarth[3], Johann Großschädl[4], Axel Poschmann[3], Zeynep Toprak[2], Marco Macchetti[5], Laura Pozzi[6], Christof Paar[3], Yusuf Leblebici[2], and Paolo Ienne[7]

[1] ALaRI - University of Lugano, Lugano, Switzerland. E-mail: regazzoni@alari.ch
[2] School of Engineering, EPFL, Lausanne, Switzerland. E-mail: {stephane.badel,zeynep.toprak,yusuf.leblebici}@epfl.ch
[3] Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany. E-mail: {eisenbarth,poschmann,paar}@crypto.rub.de
[4] Department of Computer Science, University of Bristol, United Kingdom. E-mail: johann.groszschaedl@cs.bris.ac.uk
[5] C.E. Consulting (Altran Group), Milan, Italy. E-mail: mmacchetti@ceconsulting.it
[6] Faculty of Informatics, University of Lugano, Lugano, Switzerland. E-mail: laura.pozzi@unisi.ch
[7] School of Computer and Communication Sciences, EPFL, Lausanne, Switzerland. E-mail: paolo.ienne@epfl.ch

***Abstract*— This paper explores the resistance of MOS Current Mode Logic (MCML) against Differential Power Analysis (DPA) attacks. Circuits implemented in MCML, in fact, have unique characteristics both in terms of power consumption and the dependency of the power profile from the input signal pattern. Therefore, MCML is suitable to protect cryptographic hardware from DPA and similar side-channel attacks.**

In order to demonstrate the effectiveness of different logic styles against power analysis attacks, the non-linear bijective function of the Kasumi algorithm (known as substitution box S7) was implemented with CMOS and MCML technology, and a set of attacks was performed using power traces derived from SPICE-level simulations. Although all keys were discovered for CMOS, only very few attacks to MCML were successful.

I. Introduction

During the past ten years, a number of new techniques for attacking implementations of cryptographic algorithms have been discovered. These techniques exploit information leaking from a device (e.g., a smart card) while data is being processed. The term *side-channel attacks* summarizes all possible ways of collecting the leaked information: power consumption, timing, and electromagnetic emission are possible examples [11]. Side-channel attacks which exploit the power consumed by a device were reported for the first time in 1999 by Kocher et al [10]. The power consumption of a device strongly depends on the data being processed, thus leaks information about the secret key. Among the different variants of power-based attacks, *differential power analysis (DPA)* and *correlation power analysis (CPA)* are of particular interest since they do not require specific knowledge about the implementation of the target device to be effective.

In this paper we analyse and demonstrate the robustness of a special logic style, namely MOS Current Mode Logic (MCML), against DPA and CPA attacks. Previous papers on this subject just argued robustness qualitatively or required hardware manufacturing to prove it. Contrary to past work we evaluated the robustness of MCML *with real attacks* and *without the need for manufacturing prototypes*. In fact, we developed a SPICE-level simulation environment that allows to collect power traces in reasonable time, paving the way to a more direct experimental study of DPA-resistance. Our results show that the traces obtained by simulating an S-box realised in MCML technology are difficult to attack. On the other hand, the same attacks were always successful when performed on a CMOS implementation of the S-box.

The remainder of this paper is organized as follows: Section II discusses related work, Section III overviews the Kasumi algorithm, and Section IV describes the MCML technology. The design flow proposed in this paper, including simulation-based power analysis, is explained in detail in Section V, and simulation results are presented in Section VI. Finally, conclusions are drawn in Section VII.

II. Background and Related Work

Side-channel cryptanalysis has emerged as a serious threat for smart cards and other types of embedded systems performing cryptographic operations. Some side-channel attacks are an extremely powerful and practical tool for breaking commercial implementations of cryptography. These attacks exploit the fact that any execution of a cryptographic algorithm on a physical device leaks information about sensitive data (e.g., secret keys) involved in the computations. Many sources of side-channel information have been discovered in recent years, including the power consumption and timing characteristics of a device [9], [10], as well as deliberately introduced computational faults [3].

Simple power analysis (SPA) uses the leaked information from a single computation, while differential power analysis (DPA) utilizes statistical methods to evaluate the information observed from multiple computations [10]. Currently, there exists no perfect protection against DPA attacks. However, by applying appropriate countermeasures, it is possible to make the attacker's task more difficult. Proposed countermeasures range from algorithmic techniques [6], [16] over architectural approaches [13], [14], [8] down to hardware-related methods

1-4244-1058-4/07/$25.00 ©2007 IEEE

[15], [17]. All algorithmic and architectural countermeasures have in common that they introduce either amplitude noise (to reduce the signal-to-noise ratio) or timing noise (to obscure the alignment of power traces). In both cases, more power traces must be captured to mount an attack.

A multitude of so-called *DPA-resistant logic styles* have been proposed during the past five years. The idea behind these logic styles is to tackle to problem of side-channel leakage at its actual root, namely at the hardware level. The power consumption of circuits realized with DPA-resistant logic cells is uniform and, in the ideal case, independent of the processed data and the performed operations. The first concrete implementation of a DPA-resistant logic style was reported by Tiri et al in 2002 [17]. Their *Sense Amplifier Based Logic (SABL)* combines the concepts of dual-rail logic and pre-charge logic [11]. SABL cells have a constant power consumption, provided that they are designed and implemented in a carefully balanced way. All SABL cells of a circuit are connected to the clock signal and become pre-charged simultaneously, which causes very high current peaks. Furthermore, SABL cells require at least twice as much silicon area as conventional CMOS cells and suffer also from high delay. Besides the logic cells also the wires connecting these cells must be routed in a special balanced way to achieve a uniform power profile.

III. Overview of the Kasumi Algorithm

We focus on the block cipher *Kasumi* [1], which represents the base of the standardized confidentiality algorithm of the 3GPP (3rd Generation Partnership Project). Kasumi is a Feistel cipher with eight rounds and produces a 64-bit output from a 64-bit input, whereby the secret key has a length of 128 bits. During encryption, the input I is divided into two 32-bit strings, called L_0 and R_0. Then, for the following i rounds, L_i and R_i are defined as

$$R_i = L_{i-1} \tag{1}$$

$$L_i = R_{i-1} \oplus f_i(L_{i-1}, RK_i) \tag{2}$$

where f_i denotes the round function within L_i and the round key RK_i. The round function f_i is constructed from sub-functions and has two different forms depending on whether it is an even or odd round. It uses two *S-boxes*: *S7*, which maps a 7-bit input to a 7-bit output, and *S9*, which maps a 9-bit input to a 9-bit output. These two S-boxes have been designed in such a way that they can be easily implemented using a look-up table as well as combinatorial logic.

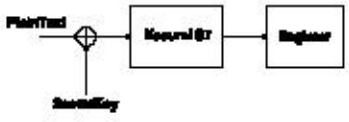

Fig. 1. Overview of the considered part of the Kasumi Algorithm.

In this paper we focus on the *S7* S-box. We implemented it as combinatorial logic composed of two level of AND-OR gates, as suggested in the standard specifications. Figure 1 shows a block diagram of the example that we consider in this paper. The secret key is added to the plaintext and the result is used to feed the substitution function. After the non-linear transformation is calculated, the result is stored in a bank of D flip-flops. Such a setup coarsely reflects a one-round-per-clock-cycle implementation, and is the basic configuration for a DPA attack. A real implementation may differ from the one considered here; however our goal is to estimate the level of robustness intrinsically given by the logic style, instead of attacking a particular implementation of the Kasumi block cipher.

IV. Design of DPA-Resistant Functional Units using MCML Gates

The circuit-level implementation of DPA-resistant logic gates requires systematic use of circuit techniques that: (i) have significantly suppressed power supply current levels, (ii) do not produce prominent current spikes or fluctuations during the switching events, and (iii) do not exhibit a significant input pattern-dependence with respect to current drawn from the power supply [18]. It is worth noting that the classical CMOS logic gates do not fare particularly well in any of these categories, and therefore, are not considered to be a good choice for DPA-resistance, in general. Standard CMOS digital gates are notorious for generating sharp and input-pattern dependent current pulses (also referred to as delta-I noise [7], [2]) due to charging and discharging of the gate's parasitic capacitances and fan-out. This delta-I noise is directly measurable as disturbances on the power supplies and the substrate, which can be an important drawback when designing a DPA-resistant system.

Several different circuit design styles have been explored as possible candidates for better DPA-resistance, including differential circuit techniques like SABL [17] and Current Mode Logic (CML). CML reduces the generated switching noise by about two orders of magnitude [19], [12], hence making it suitable for DPA-resistant hardware designs. This reduction is due to the differential and current steering nature of the logic style. The low delta-I noise generation combined with approximately the same amount of power dissipation as its CMOS counterpart makes the CML style an excellent candidate for DPA-resistant logic gate design.

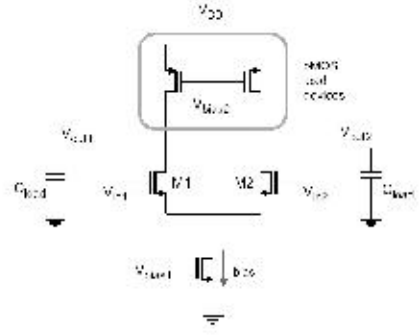

Fig. 2. Schematic of an MCML buffer (or MCML inverter, depending on the output signal definition).

A MOS Current Mode Logic (MCML) gate consists of a tail current source, a current steering logic core, and a differential load, as shown for the simplest MCML gate, the MCML buffer, in Figure 2. The operation of MCML circuits is based on the principle of re-directing (or switching) the current of a constant current source through a fully differential network of input transistors, and utilizing the reduced-swing voltage drop on a pair of complementary load devices as the output. Note that a logic inversion without additional delay is possible by simply exchanging the differential terminals. It is desired that the input voltage fully switches the tail current (I_{bias}) one way or the other. If the input pair is not completely switched, part of the tail current is common for both input transistors and does not contribute in the differential output signal. Furthermore, if the input pair is not fully switched, the actual differential output current will be sensitive to temperature and input pair offset voltage, which is an undesirable property. The operation principle already suggests that the power consumption is static (the circuit must dissipate the same amount of current continuously) regardless of the switching activity and fan-out conditions. True differential operation of the circuit with small output voltage swing ensures fast switching times. Note that the propagation delay is proportional to the output swing, and independent of the power supply voltage. Other advantages include better noise immunity compared to classical CMOS logic circuits, and significantly less switching noise.

The power dissipation of a CMOS gate is simply the product of operation frequency and the charging/discharging power per unit switching. Thus, the average current a CMOS gate draws from the supply line increases linearly with the operation frequency, while on the other hand, the operation frequency has little impact on the power dissipation of an MCML gate. The supply current fluctuation in MCML gates is typically 5% of the nominal tail current during switching events. Figure 3 shows the simulated current variation of an MCML buffer for a fan-out of 5. MCML circuits are also more robust against common-mode fluctuations (power supply noise) due to their inherent common-mode rejection as a result of full differential signaling property.

From the DPA-resistance point-of-view, it can be seen that the supply-current variation of the MCML gate will remain significantly smaller during switching events, compared to that of a conventional CMOS gate. At the same time, the magnitude of the supply-current variation is largely independent of the applied input vector, as well as of the fan-out load capacitance. The amount of static current dissipation can be reduced dramatically while preserving all of the advantages concerning the DPA-resistance, at a lower speed, when the transistor sizing is done to satisfy modest speed constraints (e.g., a typical switching speed of 400MHz). It is demonstrated in [19] that the designed MCML family using a standard 0.18μm process technology with 400mV_{pp} output voltage swing at 400MHz operation frequency, dissipates comparable power with respect to its CMOS counterpart operating at the same speed. In this work the bias current and active load size of MCML gates were adjusted to reach these

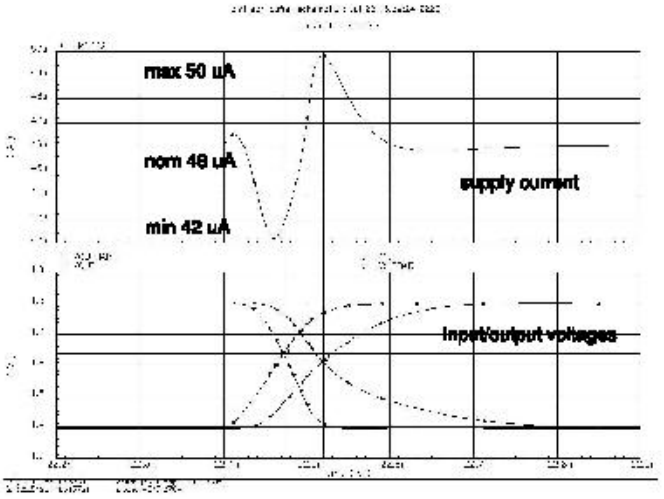

Fig. 3. Simulated gate delay and supply current fluctuation of an MCML buffer for a fan-out of 5.

design specifications. The lower bound on voltage swing was set to be 300mV_{pp} to ensure complete current switching even at the worst case design corner. The ratio between the power dissipation of the MCML XOR gate and the classical CMOS XOR gate was found to be less than a factor of two at this nominal frequency, which compares quite favorably with other DPA-resistant circuit styles.

The utility of the current-limited MCML gates in a DPA-resistant design was demonstrated in [19], using the 7-input Kasumi S-box function consisting of 105 two-input AND and 77 two-input XOR gates. It was also shown [19] that the peak current fluctuation of the classical CMOS realization is in the order of 28mA, while the current fluctuation of the MCML version remains confined to a narrow band of about 0.5mA, around the constant value of 11.5mA. A close-up view of the supply-current variation of the Kasumi S7 S-box function block clearly indicates the significant input-pattern dependence of the classical CMOS version. In contrast, the power supply current of the MCML version does not exhibit any noticeable variation that depends on the applied input patterns. The standard variation of the CMOS supply current is demonstrated to be in the order of 10mA (28mA peak), while the standard variation of the MCML supply current remains less than 0.2mA (1mA peak) [19]. Possible effects of measurement set-up on the readability of supply current variations in both circuits were also monitored in [19]. The probing instrument load was modelled, having a low-pass filter characteristic and the filtered output was monitored. As expected, the design based on CMOS logic still shows large variations (400μA peak), sufficient to be distinguished quite easily. On the other hand, the maximum current fluctuation in the MCML-based design remains below 25μA, further increasing DPA-resistance of the security-critical block.

V. Design Flow

The robustness of a hardware implementation of a block cipher against power analysis attacks can be evaluated at

different stages of the design flow. The decisive proof is obtained when the actual fabricated microchip is attacked using high frequency probes and an oscilloscope; nonetheless, *attacking the power consumption traces obtained with transistor-level simulation can be useful to get a good approximation of the actual level of DPA-resistance, and an indication of possible sources of weakness.*

The transistor-level simulation has been carried out at very high timing resolution (about 1ps) and with no additional noise coming from the measurement device, other parts of the circuit, or the environment. From one point of view, it is therefore a "best-case" attack; however there are certainly other effects that can not be correctly modelled, such as the effects of the fabrication process. An important advantage is that in this way it is also possible to iterate the design flow to investigate further points of optimisation.

In the following we describe the design and simulation flow that we have used to obtain power traces for both the CMOS and the MCML implementation of the Kasumi substitution box S7. Both implementations have the same block structure (which is described in Section III), but their code-entry and design process differs. The CMOS circuit has been described using the VHDL language, synthesized with Synopsys Design Compiler, and converted into SPICE format. The technology library used for the CMOS circuit models the UMC 0.18μm process installed and licensed in the EPFL Electrical Engineering Department. On the other hand, the MCML circuit has been described by hand using the Spectre language, reflecting a two-level AND-XOR logic implementation as suggested in the Kasumi specification document. Therefore, it is expected that both the latency and area of the second circuit are worse. However, the different design approach is necessary since commercial synthesis tools do not support non-standard differential logic libraries like our MCML library.

The interconnection parasitics have not been taken into account in the simulations, since a back-end phase followed by back-annotation would be necessary to do this. Such a back-end phase is meaningful only in the context of a complete description of the circuit considering also clock-tree expansion, floorplanning, and place & route steps. Thus, our results will be indicative of the intrinsic robustness of the logic primitives, more than the robustness of a particular implementation of the system that includes the Kasumi block cipher. Again, this is coherent with the goal of this paper.

Transistor level simulations have been performed with Synopsys Nanosim, at highest level of accuracy. The SPICE descriptions of the UMC18 and the MCML logic libraries instantiate the BSIM3 p-MOS and n-MOS transistor models [5]. Simulation results of Nanosim are comparable to those of SPICE, but the simulation process requires significantly less time to be carried out. The global current absorption of the two S-box circuits has been monitored and dumped at intervals of 1 ps. A post-processing step was performed on the dumped values to obtain the continuous current vectors readable by the application that performs the statistical analysis, as described in the following Section.

VI. Resistance against Power Analysis

In this section we describe the attacks we mounted on the CMOS and MCML implementations of the Kasumi S-box and we compare the results.

A typical DPA attack consists of the following steps: at first, an intermediate key dependent result is selected as the target, then the attacker encrypts (decrypts) a certain number of known plaintexts (ciphertexts) and measures the corresponding power consumption traces. Subsequently, hypothetical intermediate values are calculated based on a key guess and they are used as input of a selection function. This function is used to partition the power consumption traces into two sets, depending on the values of the intermediate results. The difference of means of the two sets is then calculated and shows a peak for the right key hypothesis in correspondence to the time frame where the information is leaked. For all other key guesses and points in time, the difference of means is close to zero.

An improvement with respect to DPA attack, called *correlation power analysis* (*CPA*), was discussed in [4]. It hypothesizes the Hamming weight of the targeted S-box output and evaluate the hypothesis statistically. The correlation $\rho_{(P(t),H)}$ between the power traces $P_n(t)$ and the hypothesis H is calculated using the following equation:

$$\rho_{(P(t),H)} = \frac{\mathrm{cov}(P(t),H)}{\sqrt{\sigma^2_{P(t)} \cdot \sigma^2_H}} \tag{3}$$

where $\sigma^2_{P(t)}$ and σ^2_H are the variance of the power traces $P_n(t)$ and the hypothesis H, while $\mathrm{cov}(P(t),H)$ denotes the covariance of the two. The correlation $\rho_{(P(t),H)}$ is a normalized value between $-1 \leq \rho \leq 1$ where $\rho = 1$ ($\rho = -1$) means that the variables $P(t)$ and H are perfectly correlated (anti-correlated) and $\rho = 0$ means there is no correlation at all. The adversary calculates the correlation for each key hypothesis and chooses the key which shows the strongest correlation. Usually CPA shows better results than DPA because it uses hypotheses based on multiple bits rather than the single bit approach of DPA.

Mounting the Attacks

Using the simulation flow described in Section V, we attacked the S7 S-box of Kasumi. It is important to notice the differences between the simulated and the real attack. In a real environment, an attacker has to collect a huge number of traces in order to filter out the noise. In fact, when power consumption of any device is measured, the collected traces include noise. Increasing the number of traces, the noise can be filtered out, as can be seen from Equation 4:

$$P(t) = \sum_g f(g,t) + N(t) \tag{4}$$

where $P(t)$ is the total power consumptions of the device, $f(g,t)$ is the power consumption of a gate g at time t, and $N(t)$ is an uncorrelated normally distributed random variable that represents the noise components.

Logic Style	DPA (bit used in the selection function)							CPA
	0	1	2	3	4	5	6	H.W.
CMOS	128	128	128	128	128	128	128	128
MCML	0	0	0	0	5	0	0	4

TABLE I
SECRET KEYS FOUND BY DPA AND CPA ATTACKS.

The simulation environment we used is noise free: neither white (thermal) noise nor algorithmic noise produced by other components appear in the power trace. Hence, to fully characterize the considered S-box, we need only $2^7 = 128$ measurements, one for each of the 128 different plain text inputs. Furthermore, the simulation was performed with a very high resolution both for the current (1μA) and the time (10ps), which is the best possible condition for an attacker.

DPA and CPA were performed on the two implementations of the Kasumi S-box shown in Figure 4, the first realized using CMOS technology and the second with MCML. The attack was focused on the input of the register, as depicted in Figure 4, since for CML, it is the part that we implemented using a completely differential logic. Hence this is the point of the circuit that was supposed to be fully protected.

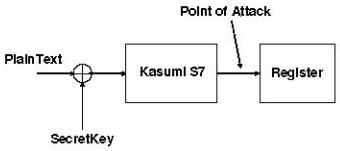

Fig. 4. Point of attack for DPA and CPA.

Table I reports the number of secret keys found while attacking the two different S-box implementations. We have repeated the DPA attack using all possible S-box output bits as selection function. The CPA attack has been performed with a selection function based on the Hamming weight. In all these cases our attacks on the CMOS logic were always successful. The differential trace of the correct key (plotted in black) is the one that shows the highest peak, thus it is clearly distinguishable from the remaining ones, as can be seen from Figure 5 (DPA using selection function on bit 1) and Figure 6 (CPA on the Hamming weight). In the latter case, a correlation value as high as $\rho_{(P(t),H)} = 1$ indicates the correct hypothesis.

The situation is completely different for the implementation based on MCML. As can be seen from Figure 7, the black line representing the correct key is not distinguishable from the remaining differential traces plotted in gray. The same situation is also valid for the correlation power attack depicted in Figure 8.

As reported in Table I, a total number of nine keys was found. Although this result can not be considered insignificant from a statistical point of view, it must be underlined that the successful attacks mounted to MCML do not show the usual situation for differential power analysis (DPA) and correlation power analysis (CPA). As can be seen from Figure 9, which shows an example of a successful DPA

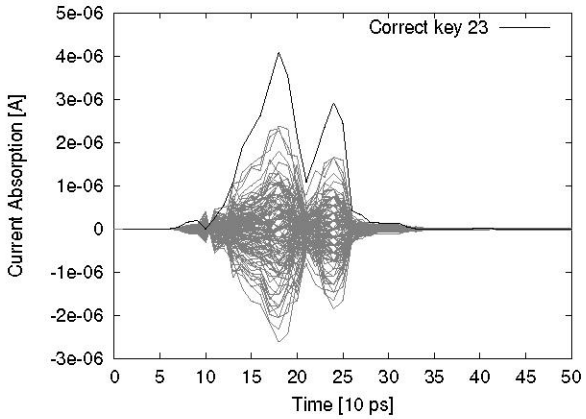

Fig. 5. DPA on CMOS technology.

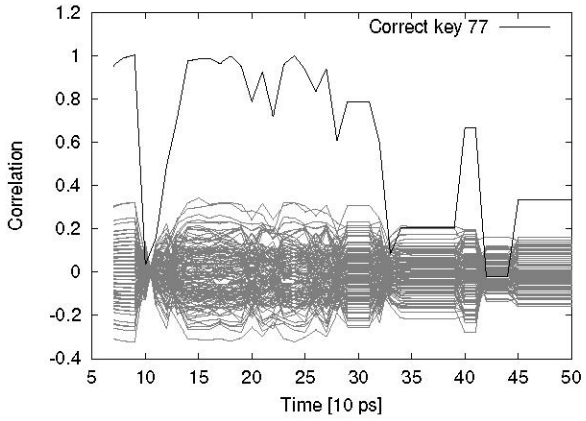

Fig. 6. CPA on CMOS technology.

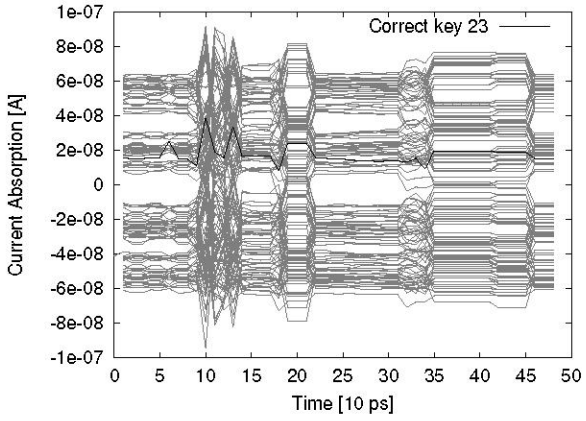

Fig. 7. DPA on MCML technology.

attack on bit 4 of the S-box output, the differential trace corresponding to the correct key has the same shape as all the others rather than clearly indicating a peak, thus the key guess results to be correct only because the corresponding trace is the external one. As a consequence, in an attack mounted on a real device, it could be completely hidden by so-called *ghost peaks* (peaks of similar height corresponding to a wrong key guess), making the attack more difficult.

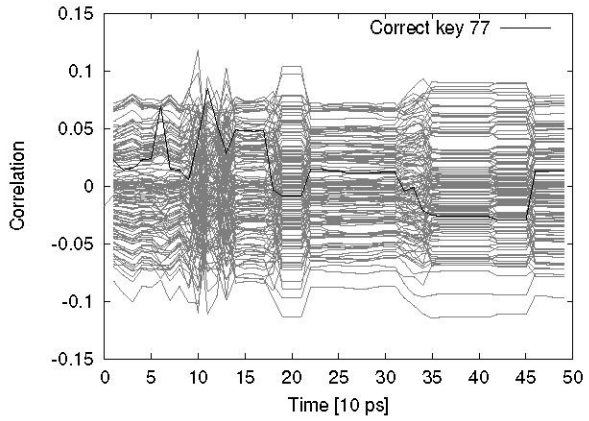

Fig. 8. CPA on MCML technology.

We want to stress that the attacks were mounted within a simulation environment, thus in ideal and best condition for an attacker, both in terms of sampling rate accuracy and absence of noise. We are currently evaluating if this eventual dependence can be effectively exploited on a real device.

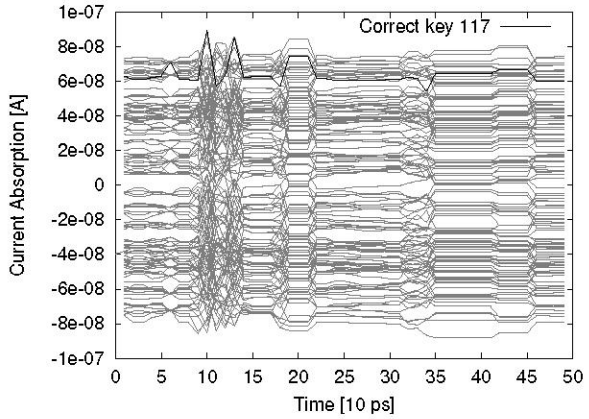

Fig. 9. Successful DPA attack on MCML technology.

VII. Conclusions

In this paper we introduced a simulation-based methodology for evaluating the resistance of cryptographic circuits to power analysis attacks. We validated our methodology on the MCML technology, and demonstrated the robustness of MCML against DPA and CPA attacks. Contrary to previous papers on this subject, we did not argue robustness just qualitatively, but with real attacks. Furthermore, since our approach is based on SPICE-level simulations, it does not rely on the manufacturing of prototypes, which allows a more direct experimental study of DPA-resistance.

Our results show that the power traces obtained by simulating the non-linear bijective function of the Kasumi algorithm realised in MCML are very difficult to attack, as opposed to a CMOS implementation for which the same attacks were always successful. We are currently evaluating the robustness of MCML against template attacks.

References

[1] 3GPP 35.202 Technical Specification version 3.1.1. Kasumi S-box function specifications. Available for download at `http://www.3gpp.org/ftp/Specs/archive/35_series/35.202/`, 2002.

[2] M. Anis, M. Allam, and M. Elmasry. Impact of technology scaling on CMOS logic styles. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 49(8):577–588, Aug. 2002.

[3] E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems. In *Advances in Cryptology — CRYPTO '97*, vol. 1294 of *Lecture Notes in Computer Science*, pp. 513–525. Springer Verlag, 1997.

[4] E. Brier, C. Clavier, and F. Olivier. Correlation power analysis with a leakage model. In *Cryptographic Hardware and Embedded Systems — CHES 2004*, vol. 3156 of *Lecture Notes in Computer Science*, pp. 16–29, Springer Verlag, 2004.

[5] BSIM3 Version 3.3.0 MOSFET Model. Avaliable for download at `http://www-device.eecs.berkeley.edu/~bsim3`, July 2005.

[6] J.-S. Coron and L. Goubin. On Boolean and arithmetic masking against differential power analysis. In *Cryptographic Hardware and Embedded Systems — CHES 2000*, vol. 1965 of *Lecture Notes in Computer Science*, pp. 231–237. Springer Verlag, 2000.

[7] J. Gonzalez and A. Rubio. Low delta-I noise CMOS circuits based on differential logic and current limiters. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 46(7):872–876, July 1999.

[8] J. Irwin, D. Page, and N. P. Smart. Instruction stream mutation for non-deterministic processors. In *Proceedings of the 13th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP 2002)*, pp. 286–295. IEEE Computer Society Press, July 2002.

[9] P. C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in Cryptology — CRYPTO '96*, vol. 1109 of *Lecture Notes in Computer Science*, pp. 104–113. Springer Verlag, 1996.

[10] P. C. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Advances in Cryptology — CRYPTO '99*, vol. 1666 of *Lecture Notes in Computer Science*, pp. 388–397. Springer Verlag, 1999.

[11] S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer Verlag, 2007.

[12] S. Maskai, S. Kiaei, and D. Allstot. Synthesis techniques for CMOS folded source-coupled logic circuits. *IEEE Journal of Solid-State Circuits*, 27(8):1157–1167, Aug. 1992.

[13] D. May, H. L. Muller, and N. P. Smart. Non-deterministic processors. In *Information Security and Privacy — ACISP 2001*, vol. 2119 of *Lecture Notes in Computer Science*, pp. 115–129. Springer Verlag, 2001.

[14] D. May, H. L. Muller, and N. P. Smart. Random register renaming to foil DPA. In *Cryptographic Hardware and Embedded Systems — CHES 2001*, vol. 2162 of *Lecture Notes in Computer Science*, pp. 28–38. Springer Verlag, 2001.

[15] S. W. Moore, R. J. Anderson, P. Cunningham, R. Mullins, and G. Taylor. Improving smart card security using self-timed circuits. In *Proceedings of the 8th International Symposium on Asynchronous Circuits and Systems (ASYNC 2002)*, pp. 193–200. IEEE Computer Society Press, 2002.

[16] A. G. Rostovtsev and O. V. Shemyakina. AES side channel attack protection using random isomorphisms. Cryptology ePrint Archive, Report 2005/087, avialable for download at `http://eprint.iacr.org`, 2005.

[17] K. Tiri, M. Akmal, and I. M. 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 (ESSCIRC 2002)*, pp. 403–406. University of Bologna, Italy, 2002.

[18] K. Tiri and I. Verbauwhede. Securing encryption algorithms against DPA at the logic level: Next generation smart card technology. In *Cryptographic Hardware and Embedded System — CHES 2003*, vol. 2779 of *Lecture Notes in Computer Science*, pp. 125–136. Springer Verlag, 2003.

[19] Z. Toprak, A. K. Verma, Y. Leblebici, P. Ienne, and C. Paar. Design of low-power DPA-resistant cryptographic functional units. In *Proceedings of the 1st ECRYPT Workshop on Cryptographic Advances in Secure Hardware (CRASH 2005)*, Leuven, Belgium, Sept. 2005.