A Dynamic Current Mode Logic to Counteract Power Analysis Attacks

F. Mace, F.-X. Standaert, I. Hassoune, J.-D. Legat, J.-J. Quisquater

UCL Crypto Group, Microelectronics Laboratory (DICE),
Université Catholique de Louvain (UCL), Belgium

mace,standaert,hassoune,legat,quisquater@dice.ucl.ac.be

Abstract: Since their publication in 1998, power analysis attacks have attracted significant attention within the cryptographic community. So far, they have been successfully applied to different kinds of implementations (*e.g.* smart cards, ASICs, FPGAs) of cryptographic algorithms. To protect such devices against power analysis attacks, it has been proposed to use a dynamic and differential logic style for which the power consumption does not depend on the data handled. In this paper, we suggest to use the Dynamic Current Mode Logic to counteract power analysis. The resulting circuits exhibit similar resistance to the previously published proposals but significantly reduce the power delay product. We also demonstrate that certain criteria previously used to evaluate the resistance against power analysis have no cryptographic relevance.

1 Introduction

Encryption algorithms have become a key element in many information systems and may usually be considered as secure in a mathematical point of view. In this context, cryptosystem designers frequently assume that secret parameters will be manipulated in closed, reliable environments. However, the realities of physical implementation can be extremely difficult to control and may result in the unintended leakage of side-channel information. In power analysis attacks, it is assumed that the power consumption of a circuit is correlated to the data handled. An attacker can therefore recover secret information by simply monitoring the power signals of a running device.

Protecting implementations against these "side-channel" attacks is usually difficult and expensive. For example, the use of random process interrupts and dummy instructions to avoid the sequential execution of the algorithm has been shown to be inefficient in [5]. Random noise addition has also been proposed but does not provide any fundamental countermeasure (the signal is still present and can still be recovered). Shamir suggested in [13] to use detachable power supplies, but the solution is not always practical for legacy systems and is susceptible to other attacks. Finally, software countermeasures are possible (*e.g.* masking all the data with random Boolean values), but they considerably reduce the implementation efficiency and still leak some information [8].

In general, these countermeasures only reduce the side-channel leakage and does not fundamentally prevent a power analysis attack. Therefore, an interesting alternative is to use a logic style for which the power consumption is independent of the data handled. Although it does not provide a theoretical countermeasure either (small power variations still appear in function of the input sequences), it has the advantage of making the attack significantly harder. Moreover, this solution can be combined with good performances if a good logic style is chosen.

In [15], it is proposed to implement the critical parts of encryption algorithms using Sense Amplifier Based Logic (SABL) gates and the circuits resistance against power analysis is evaluated according to the Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD). In this paper, we suggest to use the Dynamic Current Mode Logic (DyCML, [1]) to counteract power analysis. The resulting circuits exhibit similar resistance to SABL but significantly reduce the power delay product. In addition, we investigate the cryptographic relevance of the NED, NSD criteria and evaluate the practical influence of the logic family onto the efficiency of a power analysis attack. Different families are then compared according to their respective security against power analysis attacks.

This paper is structured as follows. A general model of power analysis attacks is given in Section 2. Section 3 describes and compares the SABL and DyCML logic families. Experiments based on the implementation of certain critical encryption algorithm components are in Section 4 and the results of these experiments are presented in Section 5 for different logic families. Section 6 discusses the cryptographic relevance of our experiments. Finally, conclusions are in Section 7.

2 Attack description

In Differential Power Analysis [6], an attacker uses a hypothetical model of the device under attack to predict its power consumption. These predictions are then compared to the real measured power consumption in order to recover secret information (*e.g.* secret key bits of cryptographic algorithms). The quality of the model has a strong impact on the effectiveness of the attack and it is therefore of primary importance.

For example, in CMOS gates, it is reasonable to assume that the main component of the power consumption is the dynamic power consumption. For a single CMOS gate, we can express it as follows [12]:

$$P_D = C_L V_{DD}^2 P_{0\to1} f \quad (1)$$

where C_L is the gate load capacitance, V_{DD} the supply voltage, $P_{0\to1}$ the probability of a $0 \to 1$ output transition and f the clock frequency. Equation (1) specifies that the power consumption of CMOS circuits is data-dependent. An attacker may consequently estimate a device power consumption at time t by the number of bit transitions inside the device at this time.

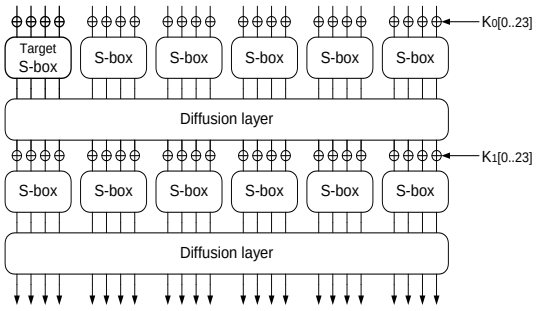

Figure 1. A simple SPN.

In practice, the use of secret key information in cryptographic designs only allows to predict a part of the bit transitions, but it is sufficient to recover secret key bits. We illustrate the attack principle with the simple Substitution-Permutation-Network of Figure 1, which contains the basic elements of most modern symmetric encryption algorithms, *e.g.* the Data Encryption Standard (DES) [9], Advanced Encryption Standard (AES) Rijndael [10] or Khazad [2].

Figure 1 contains:

- Bitwise XOR operations denoted as $\oplus$.
- Non-linear Boolean functions (S-boxes) acting on small data blocks, *e.g.* S-box : $GF(2)^4 \to GF(2)^4$.
- A diffusion layer acting on the whole block size.

Let the attacker target the 4 key bits entering the left S-box of Figure 1, denoted as $K_0[0..3]$. Then, for N different plaintexts, he first predicts the number of transitions at the S-box output, for every possible value of $K_0[0..3]$. The result of this prediction is a $N \times 2^4$ prediction matrix, containing numbers between 0 and 4.

In the second part of the attack, the attacker let the circuit encrypt the same N plaintexts, with the same key as during the prediction and he measures the power consumption of the device while the chip is operating the targeted operation. This results in a $N \times 1$ consumption vector.

Finally, the attacker computes the correlation between the consumption vector and all the columns of the prediction matrix (corresponding to all the possible key guesses). If the attack is successful, it is expected that only one value, corresponding to the correct key bits, leads to a high correlation. An efficient way to compute the correlation is to use the Pearson coefficient. Let M_i denote the ith measurement data and M the set of measurements. Let P_i denote the prediction for the ith measurement data P the set of such predictions. Then we calculate:

$$C(M,P) = \frac{\mu(M.P) - \mu(M).\mu(P)}{\sqrt{\sigma^2(M).\sigma^2(P)}} \quad . \quad (2)$$

where $\mu(M)$ denotes the mean of the set of measurements M and $\sigma^2(M)$ its variance.

From this discussion, it already appears that the attack efficiency depends on:

- The possibility to predict the power consumption of a device in function of its input data.
- The value of the correlation coefficient $C(M,P)$.

It is clear that the attack was applicable to CMOS devices because their power consumption significantly varies in function of their input data. Moreover, it can be easily predicted by simply evaluating the transitions in the circuit. In the next sections, we investigate the effect of a dynamic and differential logic style onto the feasibility of power analysis attacks.

3 DyCML vs SABL

3.1 DyCML

DyCML gates are based on classical CML gates. CML gates have the advantage of high speed execution and low commutation noise but also suffer from a static power dissipation that limits their interest. DyCML gates are formed by the combination of a standard CML block (differential pairs realize the logical function), a dynamic current source (suppressing the DC consumption) and a latch to maintain the result of the evaluation.

When the *clk* signal is low (precharge phase), the node `d` (see Figure 2 (a)) is pulled to `GND` and the outputs are set to `VDD`. During the evaluation phase, `Q1` acts initially like a current source charging the capacitance `C1` and thus discharging one of the output nodes, in a limitted amount. As a matter of fact, the power efficiency of the gate is directly linked to the value of both the capacitance `C1` and the output capacitance `CL`.

DyCML gates can be cascaded in two modes: a clock-delay scheme and a self-timed scheme, but they do not require inverters at the outputs like in Dynamic Cascode Voltage Swing Logic (DCVSL, [12]) and domino logic.

DyCML has also demonstrated its capacity to achieve better performances, in terms of reduction of the Power Delay Product (PDP) than many of other logic styles [1].

3.2 SABL

SABL logic is based on the Strong ARM 110 flip-flop from wich the sense amplifier was kept and the input differential pair was replaced by a Differential Pull-Down Network (DPDN). This DPDN is implemented in such a way that, for each stable input combination, all internal capacitances of the DPDN are connected to one output node, thanks to the transistor `M1` (see Figure 2 (b)) which is always on. This guarantees a discharge of all internal capacitances and prevents a floating node by serving as a path for subthreshold currents. During the evaluation phase, the crosscoupled inverters will toggle to a state and yield a stable output configuration, every time a direct path to ground is provided.

SABL gates can be designed as n-gates or p-gates, respectively controlled by clk and $\overline{clk}$. This allows two modes for cascading SABL gates: domino connection (by connecting the outputs of the gate to the inputs of the next gate through inverters) or np-connection (n-gates followed by p-gates like in np-logic).

3.3 Comparison

To compare the two logic styles, SPICE simulations were run on 0.13μm CMOS partially depleted SOI for V_{dd} = 1.2V, on two-input XOR gates, with a domino cascading scheme for the SABL gate (see Figure 2). Both gates were loaded with the same output capacitive load of 2 fF.

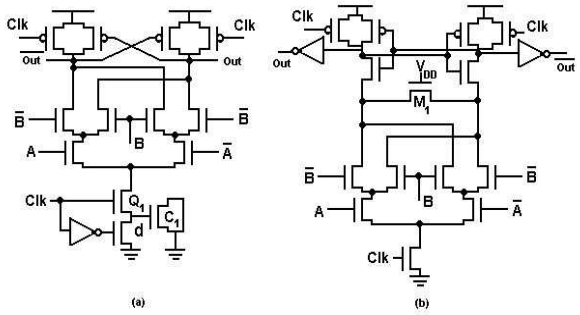

Figure 2. (a) DyCML XOR gate, (b) SABL XOR gate.

With the same evaluation tree, SABL requires an extra-circuitry of 10 transistors while DyCML only requires 9 transistors of which one acts as a virtual ground and has dimensions depending on both the output capacitance and the limitation of the output voltage swing.

The comparison of the two logic styles in terms of power, delay and Power Delay Product (PDP) for the 2-input XOR gates resulted in a 80% reduction of the PDP for the DyCML gate compared to the SABL gate.

	DyCML	**SABL**
Mean Power Consumption [μW]	1.1334	3.0894
Maximum delay [ns]	0.0776	0.1530
Power Delay Product 10^{-3}fJ	86.43	469.43

The difference in the gates power consumption is notably due to the fact that DyCML is a low-swing logic style for which the power consumption equals:

$$P = C_L V_{DD} V_{swing} f_{clk} + C_{clk} V_{DD}^2 f_{clk} \qquad (3)$$

where C_L represents the total output capacitance of the gate and C_{clk} is the capacitance at the node charged by the clock propagation circuitry which generates the full swing. This is to compare with the following expression for SABL gates:

$$P = C_L V_{DD}^2 f_{clk} + C_{clk} V_{DD}^2 f_{clk} \qquad (4)$$

where C_L is the total output capacitance, and C_{clk} the clock propagation circuitry capacitance. Moreover, because of its steady on `M1` transistor, both output branches of the DPDN are discharged every clock cycle, which doubles the capacitance to discharge compared to other logic styles. This transistor also increases the static power consumption.

As a consequence, with approximately the same clock propagation circuitry, the power consumption of SABL gates is logically higher than DyCML because SABL achieves a discharge of the total intrinsic capacitances of the gates for each clock cycle. Remark that a fair comparison between both logic styles would require additional investigation about their real area requirements, possibilities of design automation, verification,...

4 Experiments

In order to evaluate the effect of the logic style onto the resistance against power analysis, we performed experiments with the Khazad S-box [2] that is represented in Figure 3. For efficient implementations purposes this 8-bit S-box is built from smaller 4-bit S-boxes P and Q, representing Boolean functions P,Q : $GF(2)^4 \rightarrow GF(2)^4$. In our simulations, we implemented the P and Q boxes independently as well as the complete S-box, in various logic families:

- in CMOS and DCVSL for illustration purposes.
- in SABL and DyCML for comparison purposes.

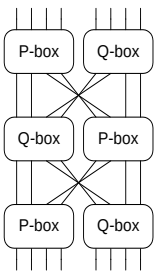

Figure 3. The Khazad S-box.

The CMOS function was realized using AND, NAND, OR, NOR gates and inverters. As the other logic styles are more adapted to construct complex logic functions with a lot of transistors in series, the logic trees were realized using a Differential Pull-Down network on the base of the S-boxes minterm expression.

The DyCML gates calculating the value of each P,Q output bit were designed to symmetrize the number of transistors connected to the output nodes, and thus the intrinsic output capacitance of the gate (see Figure 4). This was realized because the output swing, and thus the power consumption is dependent of the total output capacitance. This could be achieved for all the gates thanks to the symmetric hamming weight of the implemented functions. This modification was not necessary for SABL logic thanks to the transistor `M1` connecting the 2 intrinsic output capacitances of the DPDN.

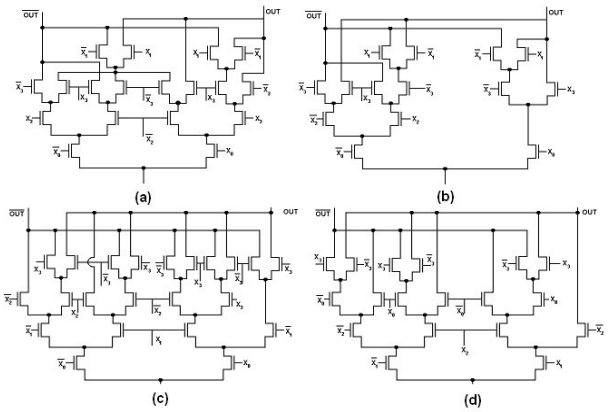

Figure 4. DyCML logic tree (Q-box).

A particular attention was also payed to the dimensioning of the DyCML gates because of the variation in fan-in, and thus in fan-out, of the cascaded gates.

5 Simulation results

To compare the performances of SABL and DyCML, SPICE simulations were run on 0.13μm CMOS partially depleted SOI for $V_{dd} = 1.2$V. This technology has a threshold voltage of respectively 0.4V and -0.39V for nMOS and pMOS devices. In order to get fair comparison between the logic styles, we first simulated every possible 4-bit input transitions for the P and Q boxes connected to a capacitive load of 2 fF. This was done in CMOS, DCVSL, SABL and DyCML (for 2 different output swings: 0.8V and 0.4V).

Then the complete S-box with input bits XORed with key bits was simulated in DCVSL, SABL and DyCML (again with the same 2 output swings). The S-box outputs were also connected to capacitive loads of 2 fF. For theses simulations, only static inputs were used, as we simulated Dynamic gates supposed to be feeded with stable inputs at the time of evaluation.

The simulations were executed at a 100 MHz frequency with a supply voltage of 1.2V. The average power consumption per cycle was extracted by averaging the consumption on 8 consecutive clock cycles. Then, the Mean Power Consumption (MPC, μ), the Power Consumption Standard Deviation (PCSD, σ), the Normalized Energy Deviation[1] (NED) and Normalized Standard Deviation[2] (NSD) were extracted for each simulated gate and each logic style.

Finally, in terms of transistor cost, the complete S-box required 754 transistors for the DyCML and 832 for the SABL, confirming the previous observations about the hardware cost of both logic styles.

It is also interesting to remark that gates with small output capacitance have a power consumption essentially dependent on the intrinsic output capacitance of the gate. If we compare the value of the total output capacitance for P and Q boxes, we can show that they are in a 0.944 ratio while their power consumption ratio is 0.946. The differences in power consumption between both boxes can thus be explained by their different intrinsic output capacitances. The following tables summarize our simulation results:

	NED	**NSD**	**MPC** [μW]	**PCSD** [μW]
CMOS	0.9338	0.3410	9.6511	3.2909
DCVSL	0.1950	0.0420	7.3813	0.3103
SABL	0.0666	0.0152	11.2641	0.1717
DyCML 08	0.0858	0.0199	6.9670	0.1388
DyCML 04	0.0807	0.0190	4.5558	0.0867
DyCML 04 LSI	0.0212	0.0038	4.4181	0.0167

Simulation results for the P-box.

	NED	**NSD**	**MPC** [μW]	**PCSD** [μW]
CMOS	0.8349	0.3166	9.6090	3.0424
DCVSL	0.8410	0.2949	8.1546	2.4051
SABL	0.0215	0.0050	15.9337	0.0803
DyCML 08	0.0870	0.0184	7.3671	0.1357
DyCML 04	0.0792	0.0116	4.4971	0.0522
DyCML 04 LSI	0.0193	0.0042	4.2937	0.0179

Simulation results for the Q-box.

	NED	**NSD**	**MPC** [μW]	**PCSD** [μW]
DCVSL	0.0548	0.0109	117.67	1.2827
SABL	0.0083	0.0021	145.65	0.3059
DyCML 08	0.0158	0.0032	96.51	0.3058
DyCML 04	0.0080	0.0020	73.08	0.1437

Simulation results for the complete S-box.

These results clearly exhibit that DyCML achieves similar performances to SABL in terms of NED, NSD. However, DyCML allows a reduction of the power consumption of almost 50%.

[1] NED = $\frac{max(energy/cycle) - min(energy/cycle)}{max(energy/cycle)}$

[2] NSD = $\frac{PCSD}{MPC}$

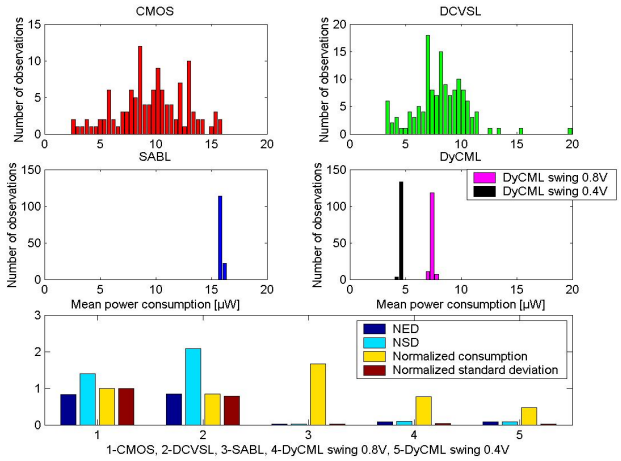

Figure 5. Comparisons for the Q-box.

6 Cryptographic relevance

6.1 Theoretical criteria

In [15], the resistance of a circuit to power analysis attacks is evaluated with the NED and NSD criteria. However, regarding the optimal statistical power analysis presented in [3], the attack efficiency only depends on the correlation between practical measurements and theoretical predictions of the device power consumption. We demonstrate in this section that a dynamic and differential logic style does not directly affect this correlation value.

Let us assume that the power consumption of an encryption circuit with random inputs may be simulated as a Gaussian distributed random noise with parameters μ and σ^2. For example, if we consider the CMOS Q-box, we have $\mu_{CMOS} = 9.6090$ μW and $\sigma_{CMOS} = 3.0424$ μW. Let us also assume that our encryption circuit only contains 8 S-boxes. We finally assume that the attacker is *able to perfectly predict and measure* the power consumption of one S-box and that the power consumption of the different boxes may be represented as independent random variables. To determine the dependencies of the correlation coefficient, we need the following theorem, demonstrated in [4]:

Theorem: The maximum correlation coefficient between the sum of n arbitrary independent identically distributed random variables and the sum of the first $m < n$ of these equals $\sqrt{m/n}$.

Therefore, if an attacker is able to predict the output transitions of one S-box out of eight, the correlation coefficient value $C(M, P)$ is theoretically approximated by $\sqrt{1/8}$. This clearly exhibits that the attack efficiency depends on the number of predictable transitions, regardless the NED and NSD values. We illustrate this statement with a simulated attack.

For this purpose, we generated the power consumption values for $N = 500$ different inputs and computed the correlation coefficient values of Section 2 for every possible key guess (*i.e.* 2^8 in our 8-bit S-boxes context). The result of this correlation attack is illustrated in Figures 6 for the DyCML logic family. We observe that the correct key guess leads to the highest correlation value after about 100 measurements and the correlation value is correctly predicted by $\sqrt{1/8} = 0.35$.

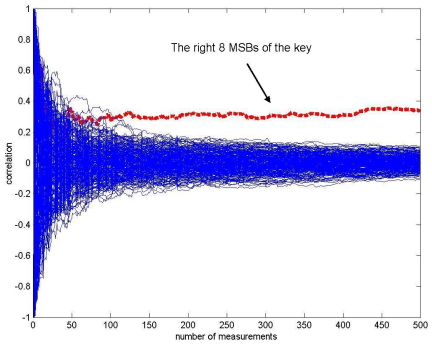

Figure 6. Simulated correlation attack.

Remark that a similar conclusion can be obtained by using the attack Signal to Noise Ratio defined in [7, 8]. Let S be the signal representing the power consumption of the targeted S-box. Let N be the noise representing the power consumption of the other S-boxes. Because the DC components of S and N are not relevant for the calculation of the correlation, only the AC components are considered in the ratio (see [7]):

$$SNR = \frac{\mathrm{Var}(S)}{\mathrm{Var}(N)} \tag{5}$$

It is clear that decreasing the power consumption variance will affect all the design S-boxes (*i.e.* S and N) in exactly the same way, and therefore not affect the *SNR*. Equation (5) also confirms that any constant power consumption in the design (*e.g.* the clock circuitry) do not affect the attack effectiveness either.

From these observations, we can conclude that the attack is still theoretically feasible against DyCML and SABL circuits. Moreover, *under the assumption that we can perfectly predict and measure the power consumption*, a circuit resistance is equal for any logic style. Nevertheless, in practice, measurements are not perfect and induce noise, independently of the logic style considered. This will cause a reduction of the correlation values, depending on the power consumption variances, although it is hard to evaluate and highly depends on the attacker measurement setup. In the next section, we show that a dynamic and differential logic style have much more impact on the attack feasibility than these theoretical predictions may lead to assume.

6.2 Practical consequences

In Section 2, we concluded that a power analysis attack efficiency depends on the possibility to predict the power consumption of a device in function of its input data and the value of the correlation coefficient $C(M, P)$. The previous discussion allowed us to exhibit that dynamic and differential logic styles does not theoretically affect the correlation values. However, from a practical point of view, a more critical concern is the predictability of the power consumption.

To understand this last statement, one should remember the origin of the power consumption differences in the different logic families. In CMOS gates, the main component of the power consumption is dynamic and depends on the probability of a $0 \rightarrow 1$ output transition. The consumption differences directly depends on the load (or not) of the output capacitance and therefore, are predictable in function of the input transitions without any knowledge about the circuit design.

In case of dynamic and differential circuits, the situations strongly differs because the output capacitance is loaded independently of the input transitions. The consumption differences are due to the presence of parasitic capacitances in the design and therefore, they cannot be predicted without a precise "transistor-level" knowledge of the circuit. As a consequence, an attacker can only target one specific implementation and preliminarily needs to build a table containing the power consumption differences in function of the circuit input data (*i.e.* an information that is usually not made available to the users). Therefore *the correlation values will be reduced according to the precision of the power consumption model used for the predictions.* At this point also, the NED and NSD criteria probably have a practical impact and this would require further research, *e.g.* on the exact relation between the power consumption model and the logic style. Anyway, regarding these conclusions, it is clear that the general considerations of Section 3 gain higher interest than security criteria. In this context, DyCML circuits present better implementation opportunities than SABL for power consumption and delay reasons. While not completely tamper resistant, both logic styles probably present sufficient security margins for most applications.

7 Conclusions

This paper investigated the use of dynamic and differential logic styles to counteract power analysis attacks. In particular, we compared the previously proposed SABL gates with Dynamic Current Mode Logic circuits. First we exhibited that both logic styles allow to significantly decrease the circuit energy variations if we compare them with a standard CMOS technology. Then we demonstrated that the theoretical impact of such observations is weak with respect to an optimal statistical power analysis [3]. Nevertheless, we illustrated that, for practical reasons, dynamic and differential logic styles offer opportunities to defeat most attackers. In this context, the predictability of the energy variations is more critical than their amplitude, which makes all dynamic and differential logic families somewhat comparable in terms of resistance against power analysis attacks. While not completely tamper resistant, they probably present acceptable security margins for general applications. Finally, for power consumption and delay reasons, we recommend the use of DyCML rather than SABL for secure integrated circuit applications.

Acknowledgements: The authors would like to thank Kris Tiri for the fruitful discussions we had about the final version of this paper.

References

[1] M.W. Allam, M.I. Elmasry, *Dynamic Current Mode Logic (DyCML): a New Low-Power High-Performance Logic Style*, IEEE Journal of Solid State Circuits, vol 36, pp 550-558, March 2001.

[2] P. Barreto, V. Rijmen, *The KHAZAD Legacy-Level Block Cipher*, NESSIE Project Home Page, https://www.cosic.esat.kuleuven.ac.be/nessie, 2001.

[3] E. Brier, C. Clavier, F. Olivier, *Optimal Statistical Power Analysis*, IACR e-print archive 2003/152, http://eprint.iacr.org, 2003.

[4] W. Bryc, A. Dembo, A. Kagan, *On the Maximum Correlation Coefficient*,Technical Report of the Department of Statistics, Stanford University, 2002-25, August 2002.

[5] C. Karlof, D. Wagner, *Hidden Markov Model Cryptanalysis*, in the proceedings of CHES 2003, Lecture Notes in Computer Sciences, vol 2779, pp 17-30, Springer-Verlag, 2003.

[6] P. Kocher, J. Jaffe, B. Jun, *Differential Power Analysis*, in the proceedings of Crypto 1999, Lecture Notes in Computer Sciences, vol 1666, pp 388-397, Springer-Verlag, 1999.

[7] S. Mangard, *Hardware Countermeasures against DPA - A Statistical Analysis of their Effectiveness*, in the proceedings of CT-RSA 2004, Lecture Notes in Computer Sciences, vol 2964, pp 222-235, Springer-Verlag, 2004.

[8] T.S. Messerges, *Using Second-Order Power Analysis to Attack DPA Resistant Software*, in the proceedings of CHES 2000, Lecture Notes in Computer Sciences, vol 1965, pp 71-77, Springer-Verlag, 2000.

[9] National Bureau of Standards, *FIPS PUB 46, The Data Encryption Standard*, Federal Information Processing Standard, NIST, U.S. Dept. of Commerce, Jan 1977.

[10] National Bureau of Standards, *FIPS 197, Advanced Encryption Standard,* Federal Information Processing Standard, NIST, U.S. Dept. of Commerce, November 2001.

[11] B. Nicolic *et al.*, *Improved Sense-Amplifier-Based Flip Flipflop: Design and Measurements*, IEEE Journal of Solid State Circuits, vol 35, pp 876-883, June 2000.

[12] J. Rabaey, *Digital Integrated Circuits*, Prentice Hall, 1996.

[13] A. Shamir, *Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies*, in the proceedings of CHES 2000, Lecture Notes in Computer Sciences, vol 1965, pp 238-251, Springer-Verlag, 2000.

[14] F.-X. Standaert, *Secure and Efficient Use of Reconfigurable Hardware Devices in Symmetric Cryptography*, PhD Thesis, UCL Crypto Group, Université Catholique de Louvain, June 2004.

[15] K. Tiri, M. Akmal, I.Verbauwhede, *A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards*, in the proceedings of ESSCIRC 2003.