Recommendations for Secure IC's and ASIC's

F. Mace[1], F.-X. Standaert, J.D. Legat, J.-J. Quisquater
UCL Crypto Group, Microelectronics laboratory(DICE),
Universite Catholique de Louvain(UCL), Belgium
email: mace, standaert, legat, quisquater@dice.ucl.ac.be

Abstract. For the last ten years, security of integrated circuits has attracted a greater attention from the cryptographic community. Several sources of information leakage within the circuits have been emphasized. Power consumption based attacks have been mounted successfully against various types of circuits like ASIC, smartcards or FPGA. To counter them, specific high level solutions were developed, but none of them achieved a total prevention of such attacks. Circuit and transistor level solutions have also been developed with better results. We present here an interesting alternative to those solutions, using Dynamic Current Mode Logic. This type of logic style gives the same security margins as the other proposed alternatives to CMOS, with better performances in terms of power, delay, complexity of implemented functions and the possibility of an asynchronous mode of the signal propagation.

1 Introduction

The security criteria of cryptographic applications have been related to mathematical and statistical properties of the encryption algorithms implemented. However, the reality of data manipulation is far from the assumed closed reliable environments. As a matter of fact, during the last ten years, different attacks have been developed using information leakage caused by the physical implementation of those algorithms. These attacks are, among others, Timing attack [1], Simple and Differential Power Analysis Attacks[2], Electromagnetic Analysis[3] or combinations of these attacks. In Power Analysis Attacks, the attacker assumes that the power consumption of a circuit is correlated to the data handled by this one. By monitoring the power traces of the attacked devices, she becomes able to recover secret informations.

To prevent these attacks, high-level countermeasures were developed, such as random process interrupts, dummy instructions or random noise addition. But nevertheless, none of them achieved a total securisation of the targeted implementations, and their use has been shown to be inefficient in [4]. Software countermeasures were also proposed but have the drawbacks of reducing the implementation efficiency and still leaking secret information [5].

Interesting alternatives consist in using logic styles with a power consumption not correlated to the handled data. Even if this does not totally prevent such attacks, it has the advantage of making the attack significantly harder, and can be combined with good performances if the appropriate logic style is chosen. One of these solutions was given by Tiri et al. in [6]. They proposed to implement cryptographic applications using Sense Amplifier Based Logic (SABL) and gave some criteria to evaluate security margins in terms of Normalized Standard Deviation (NSD) and Normalized Energy Deviation (NED). As it was previously done in [7], we will show here the interest of using Dynamic Current Mode Logic(DyCML) [8]. We will also show a design methodology and make some comparison between DyCML implementation and other logic styles implementations.

The structure of this paper will be the following. We will briefly introduce the principles of Power Analysis Attacks in Section 2. In Section 3 we will shortly present SABL, and DyCML. In this section we will also give a design methodology for DyCML and recall some comparison results between SABL and DyCML, achieved in [7]. Section 4 will show the experiments led and the achieved results for different circuits. We will finally conclude in section 5 and give some guidelines to implement secure IC's.

[1]This work was supported by the FRIA grant of the FNRS Belgium

2 Power Analysis Attacks: the principles

In the Differential Power Analysis described in [2], the attacker relies on a hypothetical model of the device under attack to predict the power consumption. He then compares these predictions with real power measurements in order to recover secret information. The results of this attack are strongly conditioned by the quality of both the prediction model and the measurements.

Let us give an example on a CMOS implementation. For a CMOS device, we assume that the power consumption can be expressed like in [9]:

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

where C_L is the output load capacitance, V_{DD} the power supply voltage, $P_{0\to1}$ the probability of an output transition from a low level to a high level and f the clock frequency. The attacker uses this model to estimate the power consumption of the circuit at time t as an image of the number of transitions within the circuit from a low level to a high level. We will now illustrate the principle of the Power Analysis Attack on a simple SPN (Substitution-Permutation Network) wich contains the basic elements of most modern symmetric encryption algorithms like DES[10], AES Rijndael[11] or Khazad[12].

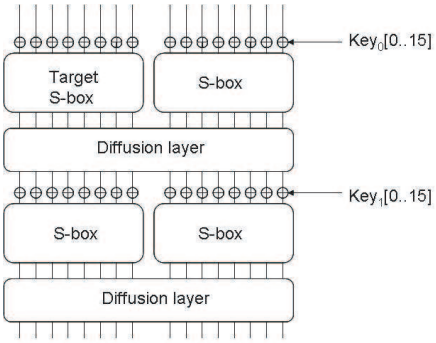

Figure 1: A Simple SPN

The different components of the simple SPN are:

- Bitwise XOR operations ($\oplus$)
- Non-linear boolean functions (implemented within the S-boxes) acting on small data blocks
- Diffusion layer acting on the whole block size

If the attacker targets the 8 MSBs of the left S-box in figure 1, then, for N different plaintexts, she will first have to predict the number of transitions occurring in the targeted S-box for all possible values of the key $K_0[0..7]$. The second part of the attack consists in taking real power measurement of the SPN encrypting the same N plaintexts as those used during the prediction phase. The last step consists in computing the correlation between each prediction and the power measurement, this is classically done straightforwardly by using the Pearson coefficient. From this, it is already clear that the quality of the attack will be influenced by the quality of both the prediction and the measurements.

3 SABL and DyCML

3.1 SABL

SABL was introduced by Tiri et al. in [6]. Thanks to the structure of the gate, all its internal capacitance is discharged for each evaluation cycle. This allows us to have a pretty much constant power consumption for the gate and thus minimization of the variations of this consumption. A generic SABL gate is presented in figure 2-b with inverters at the outputs for domino connection between gates.

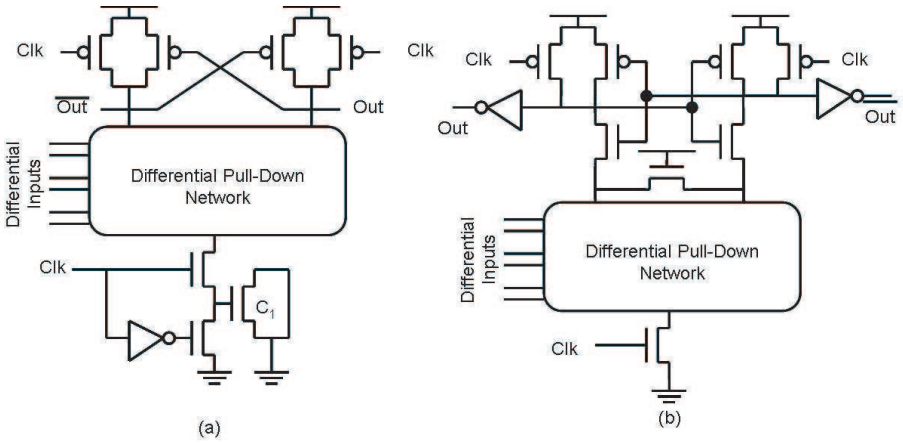

Figure 2: Generic DyCML (a) and SABL (b) gates

3.2 DyCML

DyCML was introduced by M. Allam et al. in [8]. DyCML gates are based on the structure of MOS CML gates, from which the load resistors were replaced by precharge pMOS transistor and a pMOS latch used to maintain the high level on one output. The current source of the CML gates was replaced by a dynamic current source to suppress the DC power consumption of CML. This dynamic current source is composed of 2 n MOS transistors driven by clk and $\overline{clk}$, and of a capacitor mounted nMOS transistor, C_1. This transistor will be the virtual ground used during the evaluation phase. The structure of a generic DyCML gate is shown at figure 2-a.

DyCML gates can be cascaded in two modes: a clock-delay scheme (synchronous) and a self-timed scheme (asynchronous). In the first one, the clk signal is simply delayed between two cascaded gates. Using seft-timed clock propagation requires the use a special circuit driven by clk, $\overline{clk}$ and the signal applied to the gate of transistor C_1. DyCML does not require the use of inverter to buffer the output signal towards the next gate because it does not suffer from charge sharing effects.

In their paper, M. Allam et al. gave comparisons of performances achieved by different circuits implemented in different logic styles (CMOS, Domino Logic, CPL, DDCVSL and CML). Those comparisons stated that DyCML outperforms all this logic styles for both power and delay, achieving, compared to CMOS, reductions in Energy-Delay Product up to 92 percents for a full adder cell.

3.3 Dimensioning DyCML gates

To obtain good performances, precise sizing of transistors should be achieved. By taking the dimensions yielding to the best PDP (Power - Delay Product) for the gate, we selected the best compromise between power and delay. Several sets of dimension were tested. We finally chose the one for which the dimensions of the pMOS of the upper part of the gate have the same size as the nMOS of the Differential Pull-Down Network.

The second part of the dimensioning consisted in selecting the dimensions for transistor C_1 that generate the desired output swing. However, the value of this swing, as mentioned in [8] , is dependent on both the value of the output load capacitance (taking into account the total contributions of both the internal and external load capacitances of the gate) and the dimensions of transistor C_1. As the values of the diffusion capacitances of a transistor are strongly dependant on the voltages applied to its input [13], the dimensioning of the gate requires several steps, using an iterative method.

The first step consists in extracting, from fixed dimensions and the obtained output swing, the value of the total capacitance connected to the output node, using the following formula:

$$C_L = \frac{W_{C_1} L_{C_1} C_{ox} (V_{DD} - V_{swing})}{V_{swing}} \tag{2}$$

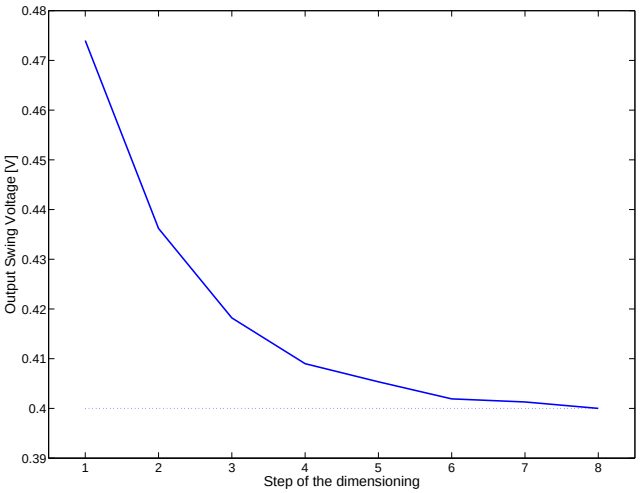

Figure 3: Evolution of the output swing during the sizing of a carry gate

where W_{C_1} and L_{C_1} are the width and length of transistor C_1, C_{ox} is the oxide capacitance in the used technology, V_{DD} is the power supply voltage and V_{swing} is the obtained output swing. With this value of C_L, we can calculate the dimension of next iteration using the formula:

$$W_{C_1} = L_{C_1} = \sqrt{\frac{V_{swing} C_L}{C_{ox}(V_{DD} - V_{swing})}} \tag{3}$$

where V_{swing} is, this time, the desired output swing.
These two steps will be repeated until the desired swing is effectively obtained. Figure 3 shows the evolution of the output swing during the dimensioning of a carry gate in DyCML. Figure 3 shows the evolution of the output swing of a gate calculating the carry of a sum, for the different sizing steps.

3.4 Comparison

In [7], we gave some comparison results between XOR gates implemented in both SABL and DyCML. These comparisons showed that DyCML achieved highly better performances in terms of both power and delay. Simulations revealed that, for a 2 inputs XOR gate, DyCML achieved a reduction of 80 percents of the Power-Delay Product.

4 Experiments and Results

In order to show the advantages of DyCML over SABL, and more, over CMOS, we will now make some comparison between the power consumption behavior of different circuits implemented in those logic styles. We will firstly remind the experiments led in [7], concerning the analysis of the power consumption behavior of a KHAZAD Sbox [12]. As the Khazad Sbox is built on smaller 4-bit blocks, called the P and Q blocks, we will recall here only the simulation results of those blocks. We also will show the behavior in power consumption of more classical circuits: a 4-bit ripple carry adder, a 4-bit carry lookahead adder and a multiplexor. Moreover, as DyCML provides asynchronous signal propagation, this version of DyCML was also explored for its application to the design of the Sbox.

Simulations were run using a $0.13\mu m$ partially depleted SOI technology, with a power supply voltage of $1.2V$ and minimal width of $0.5\mu m$ for both p and n transistors. For the Sbox, the simulations were run at a frequency of $100MHz$ while for the other circuits, we used a frequency of $330MHz$. We extracted the power consumption behavior of each circuit, for several input sets using SPICE simulations. For CMOS, we simulated more than 10000 different input sets, as the power consumption is dependant on the transitions occurring in the circuit. For DyCML and SABL implementations, we simulation the different possible input combinations, as the evaluation starts on clock transitions and not on input transitions.

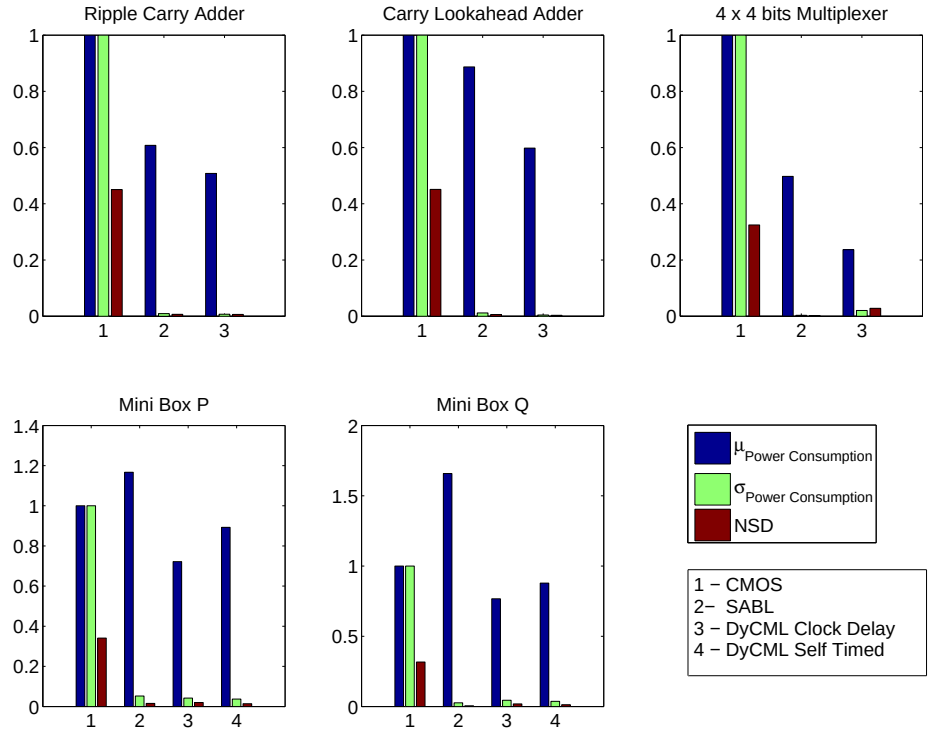

Figure 4: Simulation Results

Once we had extracted the power consumption for each implementation of each circuit, we calculated, for each, the mean power consumption μ, the standard deviation of the power consumption σ and the NSD (Normalized Standard Deviation), $NSD = \frac{\mu}{\sigma}$.

We present the simulation results in figure 4, where the mean power consumption and the standard deviation of the power consumption are normalized to the values of CMOS. We can see that for each circuit, DyCML and SABL achieve a reduction of the variation in power consumption of almost the same level. However, as it was shown in [7], and as you can see on the graphs, DyCML also achieve a reduction of the mean value of the power consumption. As the relative difference of the mean power consumption and of the standard deviation of the power consumption between DyCML and SABL are the same, the NSD remains unchanged between these two logic styles. Moreover, as shown for the P and Q mini-boxes, the use of the self-timed version of DyCML allows us to reduce a little more the variations of the power consumption, thanks to more stable inputs applied to the gates. The drawback of self-timed DyCML is that it hasn't as good performances as the clock-delayed version.

5 Conclusions

We could emphasize here the interest of using DyCML implementation of circuits for secured applications. Even if the security margins achieved by DyCML are the same as the one obtained for SABL, the advantage of DyCML lies in its better performances in term of power consumption and evaluation delay. For these reasons, we thus recommend to use DyCML for secured applications.

Moreover, we also gave here a systematic methodology for the sizing of DyCML gates that allows taking into account the dependance of intrinsic capacitors of transistors to the applied voltages at their inputs. We gave some comparison results too between clock-delayed and self-timed version of the DyCML. These results show that, even if the self-timed version is less performative than the clock-delayed one, it manages to reduce a little more the variations of the power consumption.

To conclude, let us have the following remark. Particular attention must be given to the entire design of a secured application. It means that every step of the design should be carefully examined to ensure no leakage of information is created. Even if, by using DyCML, gate security can be toughen, we should not forget that a particular attention should be given to the way we connect gates between them. As a matter of fact, we should use interconnections that match the output capacitances connected to both output of the differential gate to avoid creating information leakage due to dissymmetry of the output capacitance[14].

References

[1] P. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other systems*, Advances in Cryptology CRYPTO'96 , Lecture Notes in Computer Science, Springer-Verlag, vol. 1109, pp. 104-113, 1996.

[2] P. Kocher, J. Jaffe, B. Jun, *Differential Power Analysis*, in The Proceedings of CRYPTO'99, Lecture Notes in Computer Science, vol. 2779, pp.17-30, Springer-Verlag, 1999.

[3] D. Samyde, J.-J. Quisquater, *ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards*, Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security, Lecture Notes in Computer Science, vol. 2140, pp.200-210, Springer-Verlag, 2001

[4] 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

[5] 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.

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

[7] F. Mace, F.-X. Standaert, I. Hassoune, J.-D. Legat, J.-J. Quisquater, *A Dynamic Current Mode Logic to Counteract Power Analysis Attacks*, in The Proceedings of DCIS 2004, pp. 186-191, ISBN 2-9522971-0-X

[8] 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.

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

[10] National Bureau Of Standards, FIPS PUB 46, The Data Encryption Standard, FIPS, NIST, U.S. Dept. of Commerce, 1977

[11] National Bureau Of Standards, FIPS 197, The Advanced Encryption Standard, FIPS, NIST, U.S. Dept. of Commerce, 2001

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

[13] C.C. Enz, F. Krummenacher, E.A. Vittoz, *An Analytical MOS transistor Model Valid in All Regions of Operation and Dedicated to Low-Voltage and Low-Current Applications*, Analogue integrated circuits and signal processing, pp. 83–114, July 1995.

[14] K. Tiri, I. Verbauwhede, *Place and Route for Secure Standard Cell Design*, in The Proceedings of the 6th International Conference on Smart Cards Research and Advanced Applications (CARDIS 2004), pp. 143-158, August 2004