POWER CONSUMPTION AND NOISE MARGIN COMPARISON BETWEEN SIMPLE TERNARY INVERTER AND BINARY INVERTER

Emilia SIPOS, Robert GROZA, Laura N. IVANCIU
Bases of Electronics Department, Technical University of Cluj-Napoca, Romania
Laura.Ivanciu@utcluj.ro

Abstract: The paper presents a comparative study between ternary and binary inverters from the point of view of power consumption and noise margin. Both circuits are supplied with 0.9 Vdc and use the same transistors W/L ratios. Simulations show that the power consumption is smaller for ternary inverter and doesn't reveal the output voltage edge type. The noise margin is 150mV for the ternary inverter. The results prove that the use of ternary logic is a promising method to design power attack resistant integrated circuits.

Keywords: digital circuits, short-circuit power, noise margin.

I. INTRODUCTION

The constant growth of the information that needs to be processed and transmitted implies a higher use of digital integrated circuits. A world without digital integrated circuit is now unconceivable. To design secured integrated circuits becomes a priority, especially when the circuits are used in applications where securing the data is a vital request (e.g. smartcards).

Conventional cryptanalysis treats cryptographic algorithms as purely mathematical objects, whilst side-channel cryptanalysis also takes the implementations of the algorithms into account [1]. Side-channel attacks exploit the indirect information provided during the functioning of the digital integrated circuits – power consumption, timing information, electromagnetic leaks, etc.

Power analysis attacks are side-channel attacks that goes after the modifications that occur in the power consumption trace of a circuit. Those attacks exploits the fact that for every transition, the power consumption trace will have a detectable variation (glitch) that depends on the type of the transition and the circuits' elements. The attacker needs to have detailed information about the system, in order to be able to perform a power attack [2].

The methods of protection for power attacks are: masking (randomizes the intermediate values of the transmitted signal), and hiding (modifies the power consumption traces) [2]. The implementation of these methods needs circuit/cell level modifications, by adding dedicated modules that perform the masking/hiding operations. For digital circuits, these modules increase the complexity of the circuit.

An alternative solution to the above discussed methods is the use of a logic that is resistant to power analysis attacks. This way, most power attacks become difficult to perform [3].

A first step in towards using a power analysis attacks resistant logic is achieved in [4], [5]. An asynchronous design methodology is proposed: it involves the elimination of the clock signal and the use of threshold gates, for which the output switches only when a certain number of inputs are active. Together with the elimination of the clock signal, the situations when the clock transitions could provide information that is vulnerable to power analysis attacks are also eliminated.

This paper is focused on a comparative study between ternary and binary inverter, in order to check the possibility to use ternary logic as an alternative to binary logic, to design secured integrated circuits. For secured integrated circuits, no correlation between processed data and power consumption is traceable.

A literature review shows an increased interest for ternary circuits with low static power dissipation: ternary adders [6], max-min circuit [7], and standard ternary inverter [8] are designed. To our best knowledge, ternary logic has not yet been used to design power attack resistant circuits.

The paper is organized as follows: Section II describes the parameters of integrated digital circuits that are important in the design process – power consumption and noise margin, Section III presents and discusses the simulation results and Section IV concludes the paper.

II. PARMETERS OF DIGITAL INTEGRATED CIRCUIS

Digital integrated circuits have a series of parameters, out of which some are important when dealing. From the point of view of the resistance to power attacks the most important parameter is power consumption, and from the point of view of the resistance to noise the one of the most important parameter is noise margin.

Three types of ternary inverters are defined: negative (NTI), positive (PTI) and simple or standard (STI). The simple ternary inverter circuit was chosen to be implemented and tested with respect to power consumption. The schematic is the one proposed by [9], where only enhancement transistors and capacitors are used. The circuit has two branches: one is dedicated to PTI and the other to NTI. Combining the output of those two branches, the STI

Manuscript received June 25, 2017; revised June 30, 2017

circuit is obtained (*Figure 1*).

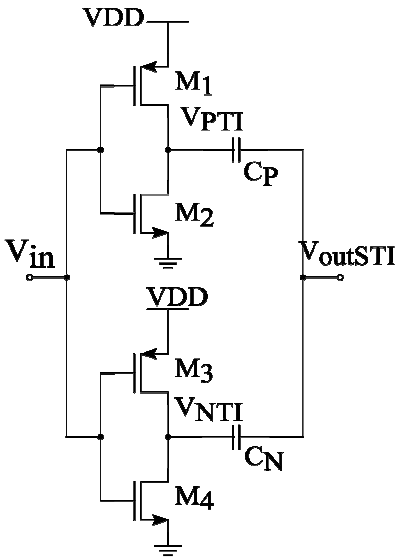

Figure 1. Simple ternary inverter – CMOS circuit.

A. Power consumption

Power analysis attacks exploit the dynamic power dissipation that occurs in binary circuits, for each transition. This power dissipation is caused by the partial short-circuit of the output CMOS structure (short-circuit power) and the output capacitive load.

The total power dissipation in a CMOS circuit is given by [10]:

$$P = P_t + P_S . \quad (1)$$

where P_t is the dissipated power inside the circuit, during the transitions of the output signal; P_s is the dissipated/consumed power inside the circuit, due to the output capacitive load.

For the ternary inverter, the output signal has 6 edges – 3 positive (rising) edges (0 to 1, 1 to 2, 0 to 2) and 3 negative (falling) edges (2 to 1, 1 to 0, 2 to 0). The short circuit power depends on the type of the output signal edge. For the circuit in Fig. 1, when the output signal goes from 0 to 1 and from 1 to 0, the shortcircuit power depends on transistors M_2 and M_4. For the 1 to 2 and 2 to 1 edges, the shortcircuit power consumption is given by transistors M_1 and M_2, while for the 0 to 2 and 2 to 0 edges, the shortcircuit power consumption is given by all four transistors. Because of that, the shortcircuit power consumption for 0 to 2 and 2 to 0 transitions is greater than for the other four types of transitions.

B. Noise margin

The noise margin is another important aspect in digital circuits. For binary circuits, the smaller the power supply, the smaller the noise margin. Noise margin values are carefully specified by producers, in order to ensure full compatibility between devices from the same family [10].

For binary circuits, there are two computed difference between the guaranteed output voltage level and the required input voltage level. The noise margin is the smallest value.

For ternary circuits, four of the aforementioned differences are computed, since there are three logical levels (one for each extreme level and two for the intermediate level) – *Figure 2*.

$$\begin{aligned} NM_{\ 0} &= V_{I,0} - V_{O,0} \\ NM_{\ 1-} &= V_{O,1-} - V_{I,1-} \\ NM_{\ 1+} &= V_{I,1+} - V_{O,1+} \\ NM_{\ 2} &= V_{O,2} - V_{I,2} \end{aligned} \quad (2)$$

The noise margin is given by:

$$NM_{\ ternary} = \min(NM_{\ 0}, NM_{\ 1-}, NM_{\ 1+}, NM_{\ 2}) \quad (3)$$

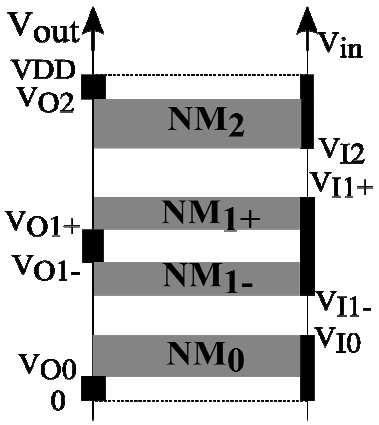

Figure. 2. Representation of noise margin for ternary circuits

III. RESULTS

The ternary and binary inverters were implemented in the Cadence environment, using the same technology. The parameters of the transistors can be found in Table I.

TABLE I
CMOS PARAMETERS

	M_1	M_2	M_3	M4
V_{th} (mV)	-318.1	737.3	-715	351.1
W (nm)	600	300	600	300
L (nm)	200	200	200	200

For a direct comparison between the ternary and binary inverters, power consumption values and noise margins were measured and analyzed. Both circuits are supplied with 0.9 Vdc, use the same transistors *W/L* ratios, working at a frequency of 1 MHz, and using a 1 fF capacitive load. The input voltage for the ternary inverter is designed to have all six possible edges. The waveforms for the simple ternary inverter are presented in *Figure 3*.

A. Power consumption

Ternary inverter

The logical sequence for the input of the ternary inverter is 0-1-2-1-0-1-2-0-2-1-0, as seen on the first waveform in

Figure 3. This sequence covers all six possible edges. The waveform of the power consumption from the power supplies is depicted in *Figure 4*.

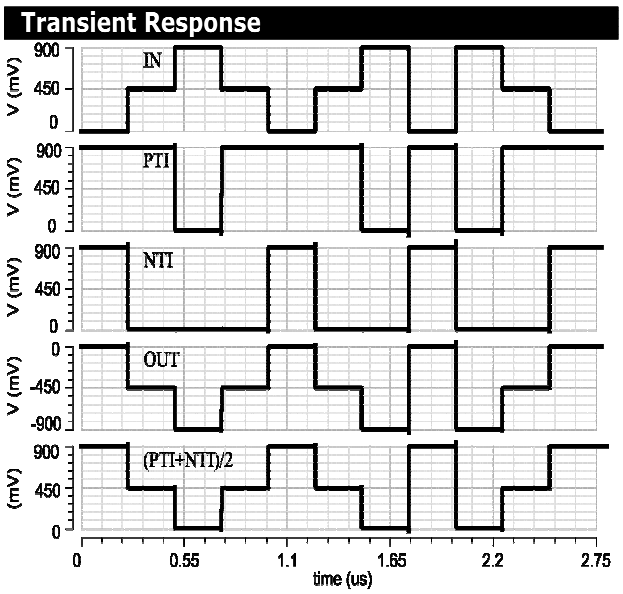

Figure 3. Simple ternary inverter – waveforms.

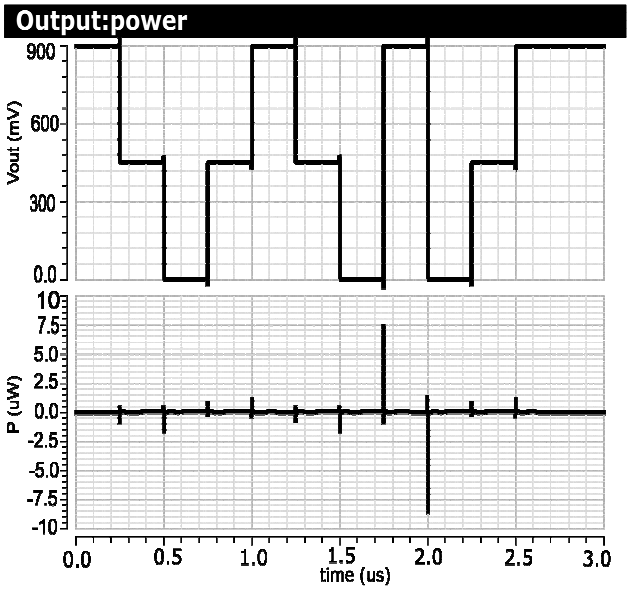

Figure 4. Power waveform of STI.

By analyzing the numerical values for the maximum power consumption, listed in Table II, one can easily observe that the power consumption is noticeably smaller for edges between intermediate levels than for extreme levels (0 to 2, 2 to 0).

TABLE II
MAXIMUM POWER CONSUMPTION

Switch	0-1	1-2	2-1	1-0	0-2	2-0
Power [10^{-6}W]	1	1.2	1	2	7.5	8.7

The values for intermediate level edges are similar, so they cannot be used to identify the transition type (positive/negative). The power consumption for edges between extreme values is about five times bigger than the one for intermediate levels and the edge of the output voltage can be identified.

Binary inverter

The power consumption waveform for the binary inverter is depicted in *Figure 5*. Compared to the values obtained for the extreme levels edges of the ternary inverter, the power consumption for the binary inverter is about 50% smaller, but still bigger than the values for the edges between intermediate levels. The edges of the output signal can easily be deduced by analyzing the power consumption, which makes the binary inverter vulnerable to power analysis attacks.

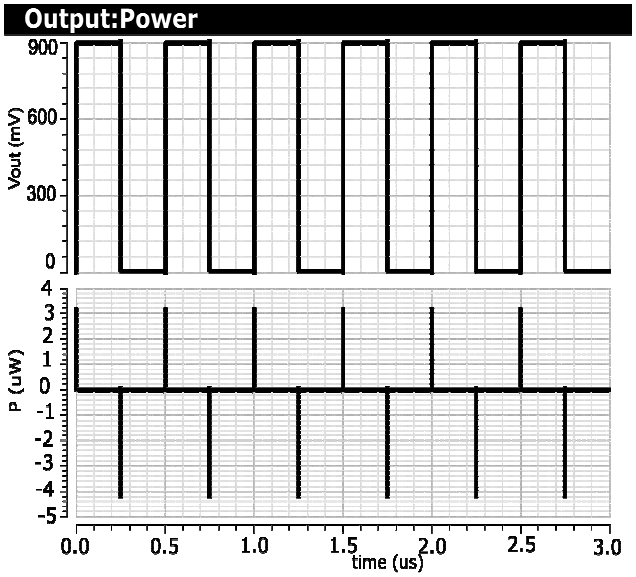

Figure 5. Power traces of binary inverter.

B. Noise margin

Ternary inverter

The four values of the noise margins were computed using data from the VTC $v_O(v_I)$ in *Figure 6* and the equations presented in Section II. Table III contains the measures values for input and output voltage levels. The four resulting noise margins are given in Table IV, out of which the minimum value is 153.4 mV.

TABLE III
MEASURED VALUED FOR INPUT AND OUTPUT LEVELS

V_I (mV)				V_O (mV)			
V_{I0}	V_{I1-}	V_{I1+}	V_{I2}	V_{O0}	V_{O1-}	V_{O1+}	V_{O2}
237	278	618.2	669.4	14.9	434.5	464.7	885

TABLE IV
NOISE MARGIN VALUES FOR TERNARY INVERTER

NM_0 (mV)	NM_{1-} (mV)	NM_{1+} (mV)	NM_2 (mV)
222.2	156.2	153.4	215.6

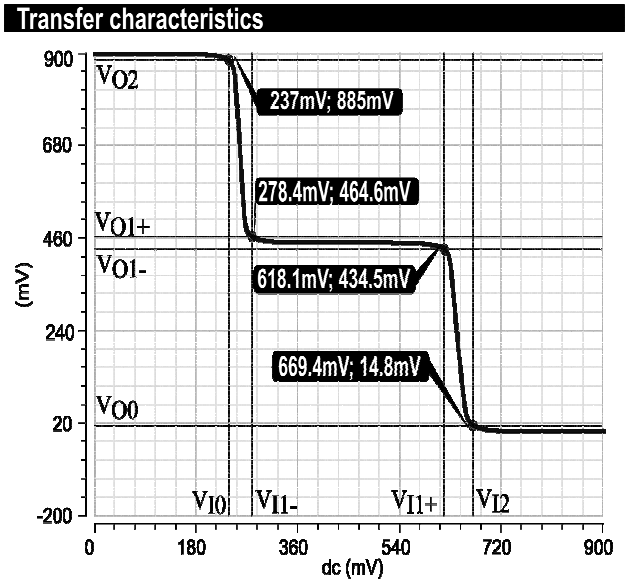

Figure 6. VTC of the ternary inverter.

Binary inverter

The VTC $v_o(v_i)$ for the binary inverter is depicted in *Figure 7*. The simulation values show a noise margin for the high logical level of 394.1 mV, respectively 389.5 mV for the low level. Hence, the noise margin of the binary inverter is 389.5 mV.

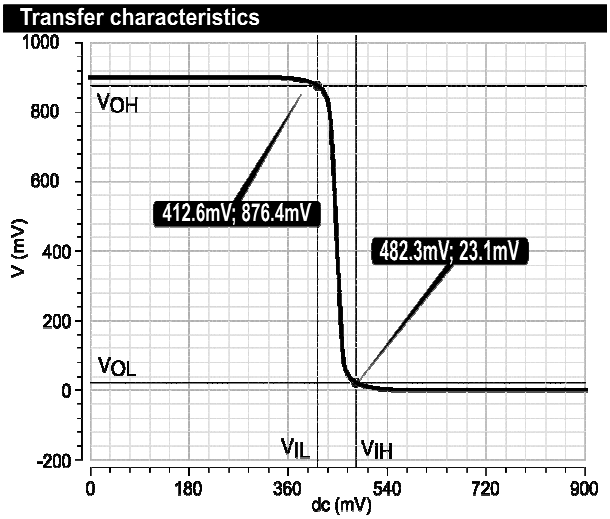

Figure 7. VTC of binary CMOS inverter.

IV. CONCLUSIONS

The paper compares the power consumption and noise margin for two digital circuits: simple ternary inverter and binary inverter.

The ternary and binary inverters were implemented and simulated, and the results were analyzed and compared, with respect to the power consumption values and noise margins.

Results show that for the ternary inverter, the edges of the output signal are undetectable/untraceable when analyzing the power consumption values, if these edges are between intermediate levels (0 to 1, 1 to 2, 2 to 1, 1 to 0). For edges between extreme values (0 to 2 and 2 to 0), the power consumption gives out the edge type. This is also valid for the binary inverter, where there are no intermediate levels, so the power consumption indicates the edge type.

The ternary inverter was also analyzed with respect to noise margin values. The noise margin is half for ternary inverter compared with the binary inverter, but a value of 150 mV is considered acceptable for the ternary inverter.

REFERENCES

[1] Zhou, Y., & Feng, D. (2005). Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. *IACR Cryptology ePrint Archive*, *2005*, 388.

[2] Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer, 2008.

[3] Giancane, Luca, et al. A new dynamic differential logic style as a countermeasure to power analysis attacks. In: Electronics, Circuits and Systems, 2008. ICECS 2008. 15th IEEE International Conference on. IEEE, 2008. p. 364-367.

[4] Porter, Christopher. Balancing delay-insensitive ternary logic circuit for mitigating side-channel attacks. UNIVERSITY OF ARKANSAS, 2011.

[5] Nair, Ravi Sankar Parameswaran, Scott C. Smith, and Jia Di. "Delay-Insensitive Ternary Logic." In CDES, pp. 3-0. 2009.

[6] R. F Mirzaee,., K Navi,., & N. Bagherzadeh, (2014), "High-efficient circuits for ternary addition,". *VLSI Design,* , vol. *x,* no. *x,* pp. *xxx-xxx,* Abbrev. Month, year *2014, 10.*

[7] Moradi, M., Mirzaee, R. F., & Navi, K. (2015). New current-mode integrated ternary Min/Max circuits without constant independent current sources. *Journal of Electrical and Computer Engineering,* 2015, 32.

[8] Shin, S., Jang, E., Jeong, J. W., & Kim, K. R. (2016, June). Demonstration of standrad ternary inverter based on CMOS technology. In *Silicon Nanoelectronics Workshop (SNW)*, 2016 IEEE (pp. 170-171). IEEE.

[9] Doostaregan, A., Moaiyeri, M. H., Navi, K., & Hashemipour, O. (2010, September). On the design of new low-power CMOS standard ternary logic gates. In Computer Architecture and Digital Systems (CADS), 2010 15th CSI International Symposium on (pp. 115-120). IEEE.

[10] Wakerkly, John F. Digital Design: principles & practices. Prentice Hall, 2010.