International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:1, No:7, 2007

Proposal for a Ultra Low Voltage NAND gate to withstand Power Analysis Attacks

Omid Mirmotahari and Yngvar Berg

***Abstract*—**In this paper we promote the Ultra Low Voltage (ULV) NAND gate to replace either partly or entirely the encryption block of a design to withstand power analysis attack.

***Keywords*—**Differential Power Analysis (DPA), Low Voltage (LV), Ultra Low Voltage (ULV), Floating-Gate (FG) and supply current analysis.

I. Introduction and background

SECURITY and cryptography have always been research topics from the first ASIC many decades ago. Ever since IC's became smaller and technology progressed new areas and applications arise. One of the hot applications today that set high demands on security is Smart Cards, due to the fact that they have encrypted keys included in the IC. The work on security for Smart Card has until recently been mostly related to mathematical and statistical properties of the encryption algorithms. In the last decade attacks (side-channel) have been reported. These side-channel attacks exploit the information leaked through the physical implementation of those algorithms. These attacks are, among others, Differential Power Analysis attacks (DPA) [1], Timing attacks [2], Electromagnetic Analysis [3] or a combination of these attacks. Cryptographic researchers have begun to consider not only mathematical attacks but also side-channel attacks as well. This resulting in several proposed countermeasures which can roughly be classified into the following two groups: (a) *Algorithmic level* and (b) *Circuit level*. On the algorithmic level countermeasures such as random process interrupts, dummy instructions and random noise addition have been implemented to slowing down or preventing attacks. While on the circuit level, techniques include adding random power consuming operations or dummy instructions. For the purpose of this paper we focus on the circuit level. Different logic styles with power consumption independent of both logic values and the sequence of data input have been proposed: a Sense Amplifier Based Logic (SABL) based on Differential Cascade Voltage Switch Logic (DCVSL) [4], a Simple Dynamic Differential Logic (SDDL) and a Wave Dynamic Differential Logic (WDDL) [5]. A comparative analysis of five different logic styles for secure IC's against DPA attacks concludes by stating that dynamic current mode logic gives the lowest correlation between power consumption and data, while differential domino with strict clocking shows the best design complexity trade-off [6]. From this background we like to state that mainly three different logic styles appear: *(1)* static, *(2)* dynamic and *(3)* differential.

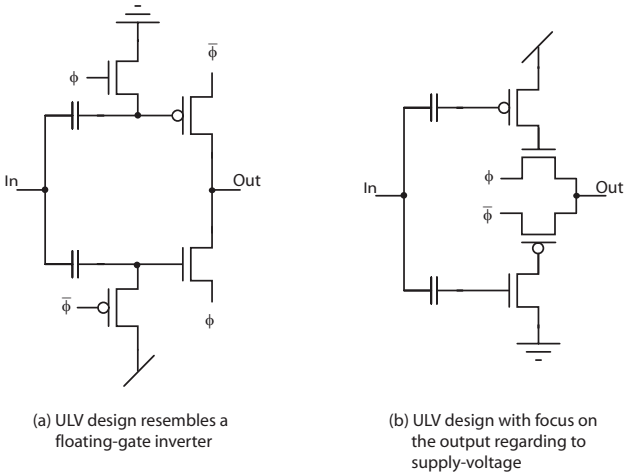
Omid Mirmotahari and Yngvar Berg are with the Nanoelectronic System Group at the Dept. of Informatics, University of Oslo in Norway, email: omidmi@ifi.uio.no

The floating-gate (FG) has been used for low voltage / low power designs [7]. A floating-gate is achieved by capacitively couple the input signal to the gate. In this manner the gate would only react to changes in the input voltage. As the name implies the actual gate of the transistor would be floating. In order to control and adjust the voltage level at the floating-gate there are basically two disciplines: (1) *"The once and for all" (non-volatile)* and (2) *the frequent recharging (volatile)*. It has been shown throughout the decades that the "once and for all" discipline is not a practical solution for modern CMOS technologies, because of the time consuming initializing of the floating-gates and due to the leakage. Although the "frequent recharging" is quite plug and play, the design has lead to more control overhead in terms of clocking strategies. A ultra low voltage (ULV) gate [8] has been presented using floating-gate and to unite and combine the advantages of disciplines (1) and (2). Furthermore, the ULV gate has been elaborated and demonstrated to withstand power analysis attacks [9]. The ULV-gate has shown good properties against power analysis because of its way to always force a transition and therefore camouflage the instantaneous supply current dissipation. Secondly, due to the fact that the outputs are not directly connected to the references (i.e. V_{dd} and Gnd).

The outline of this paper is as follows; in section II we give a presentation of the ultra low voltage gate with focus on its functionality and properties of withstanding power analysis. While in section III we propose different ULV NAND gates and elaborate on their ability to withstand a power analysis attack. Finally, the paper concludes with the benchmarks and pinpoint possible adjustments of the gates. Simulation results throughout this paper are obtained with Cadence at a STM 90nm process parameters.

II. The Ultra Low Voltage Gate

The ultra low voltage (ULV) gate was first introduced by Berg *et.al* [8] and demonstrated with measurements from 0.13um process with a supply-voltage of 0.4V. The ULV makes use of a frequent recharge/biasing scheme. The recharge/bias is applied to the gates at each clock period. Furthermore, by biasing the floating-gate directly we can assert any voltage level we desire. The ULV have a separate floating-gate for the nMOS-transistor and the pMOS-transistor, due to the fact that it is desirable to have different voltages and hence alter the threshold voltage for the transistors. By asserting V_{dd} on the floating-gate at the pMOS and Gnd on the floating-gate at



(a) ULV design resembles a floating-gate inverter

(b) ULV design with focus on the output regarding to supply-voltage

Fig. 1. The figure illustrates the ULV-gate. Both designs are logically and electrically equivalent. In (a) the design clearly shows the inverter and the biasing/recharging of the floating-gate, while (b) is designed to emphasize that the output is not directly connected to the supply voltage.

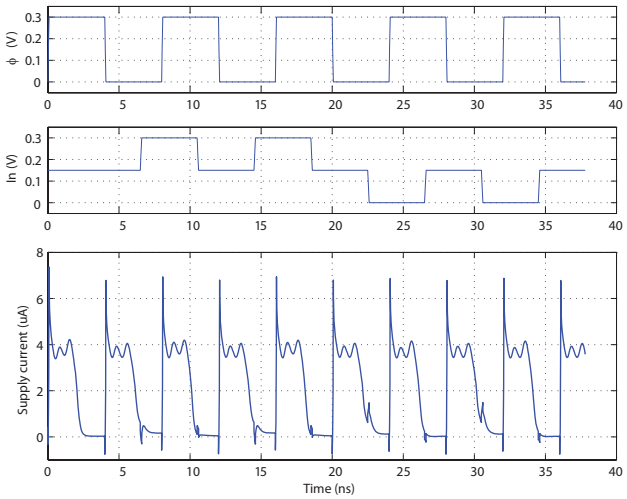


Fig. 2. The ULV gate has been simulated with a supply voltage of 0.3V and shows a operating frequency at 50MHz. As it is evident from the results the evaluation times is much faster than the recharge time. The evaluation is shown to be less than 1 ns.

the nMOS we would get a highly sensitive (fast) response for the changes on the input. The ULV gate is shown in Figure 1 and the simulation result obtained for a STM 90 nm process is shown in Figure 2. For the simulation condition we have used minimum matched transistors, i.e. pMOS 0.5/0.1um and nMOS 0.12/0.1um, while the input capacitors are kept at 0.8fF. A small load is also added to the output to simulate cascade coupled design. As it is evident from the simulation results in Figure 2, the recharge period demand more time than the evaluation. Note that in a larger design all the gates would recharge simultaneously and therefore not be a major concern. The propagation time in the evaluation period is the main key for choosing the operating frequency. The evaluation is found to be less than 0.3 ns, which implies a frequency response well above 1 GHz for 0.3V supply. Therefore the functionality/area ratio would become better for ULV-gates contrary to static CMOS or precharge. With the use of ULV gates in a design we have (looking at top-floor) transition in every period and at best 50% of the gates are evaluating a pull-up, while the other 50% are evaluating a pull-down.

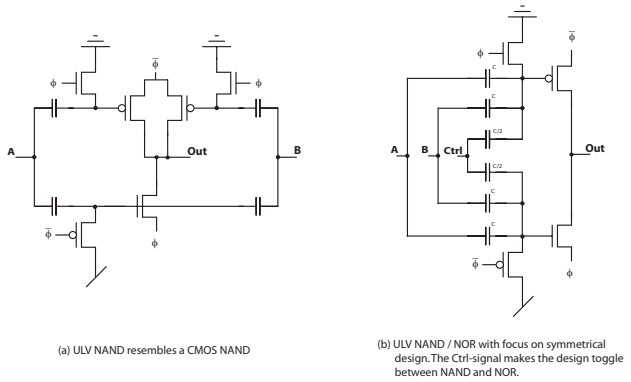
In power analysis attack resistant point of view one build up designs that have the supply current dissipation independent of the input patterns. As we see it there are different ways to make resistant designs: *(1)* One way is to make the signal propagation throughout the whole design to be quite complex and not input dependent, that is to have a quite complex design algorithm. While *(2)* the other way could be to focus on the building blocks (i.e. basic gates) to make the instantaneous supply current dissipation independent of the input. The ULV-gates differs from traditional CMOS on at least one very important point, the output is not directly connected to the supply voltage. As it is evident from Figure 1 the output is connected to the clock signal (ϕ) through a transistor. The ULV gate has been presented to have several strong attributes, like: very low (to none) correlation between the input pattern and the supply current dissipation, high frequency at very low voltages (ideal for mobile units), symmetrical design, showing symmetrical dissipation, there is a transition at every evaluation phase, no gate remains unchanged [9]. The instantaneous supply current dissipation for each gates can be neglected due to the dissipation generated by the clock signals. Thus, the instantaneous dissipation is camouflaged [9].

In the next following section we will adapt the ULV gate and propose different ULV NAND gates. We will elaborate on their ability to withstand power analysis attacks.

III. The Ultra Low Voltage NAND-gate

One of the simplest ways to design a ultra low voltage NAND gate is to use and make small changes to the traditional CMOS NAND as shown in Figure 3(a). This NAND gate is not very symmetrical and hence it is expected to reveal some information during a power analysis attack. The main weakness would be in the parallel pullup chain. Simulation results verifying the ULV NAND gate is shown in Figure 4 and demonstrates the supply current dissipation at the different evaluation periods. Although, there is quite difficult to spot the precise difference of the dissipation, we have collected some data as presented in Figure 5. The instantaneous current dissipation is the actual current drawn by one single NAND gate without the clock buffer, while the total current dissipation includes the NAND gate and the clock buffer. Naturally, the clock buffer dissipates much more (also illustrated in [9]) and therefore camouflage the instantaneous dissipation. In this table we see that the instantaneous current dissipation is approximately 1/20 of the total dissipation. One of the direct results of the in-symmetrica design is the variation in dissipation at different input combinations. We would like to make the instantaneous dissipation to have as low variation as possible (from the table we find that the variation for this ULV NAND gate is approx. 60%).

Another proposal for a ULV NAND is shown in Figure 3(b). This gate resembles much like threshold logic structures



(a) ULV NAND resembles a CMOS NAND

(b) ULV NAND / NOR with focus on symmetrical design. The Ctrl-signal makes the design toggle between NAND and NOR.

Fig. 3. The figure demonstrates two different ways to design a ultra low voltage NAND gate. In (a) the traditional CMOS NAND gate influences, while in (b) the threshold logic has been of interest. All transistors are kept minimum and matched.

[10], [11]. One of the key advantages with this design is the symmetrical aspect. In addition to obtain the symmetry, we also get another function for free. The third signal (which has lower weight) **Ctrl** can actually make the design to perform either a NAND or a NOR function. If the **Ctrl** is connected to ϕ the gate would behave as a NAND, while connected to $\overline{\phi}$ would behave as a NOR. Figures 6 and 7 verifies both logical

A	B	Out	$I_{instantaneous}$	I_{tot}
0	0	1	242 nA	4,39 uA
0	1	1	149 nA	4,39 uA
1	0	1	149 nA	4,39 uA
1	1	0	242 nA	4,39 uA

Fig. 5. The table lists up the data collected during simulation on the actual current dissipation both for the instantaneous and the total. The instantaneous current dissipation ($I_{\text{instantaneous}}$) is only the gate, while the supply current dissipation (I_{tot}) is the total dissipation including both the gate and the clock buffers.

behaviour and their respective supply current dissipations are shown. The supply current dissipations are quite similar to the other designs. The main difference can be found by looking at the instantaneous current dissipation and collecting data. In Figure 8 we see that the main improvement is the very low variation for the different input combinations (below 10%). Actually both in terms of the amount and variation has been lowered. Though, the NOR function comsumes more current than the NAND function, it is nevertheless better than the first NAND gate proposed. We would like to stress that the NOR function is actually a free option which follows the design. As a final view of the ULV NAND / NOR gate, we have simulated all the input combinations and all the possible

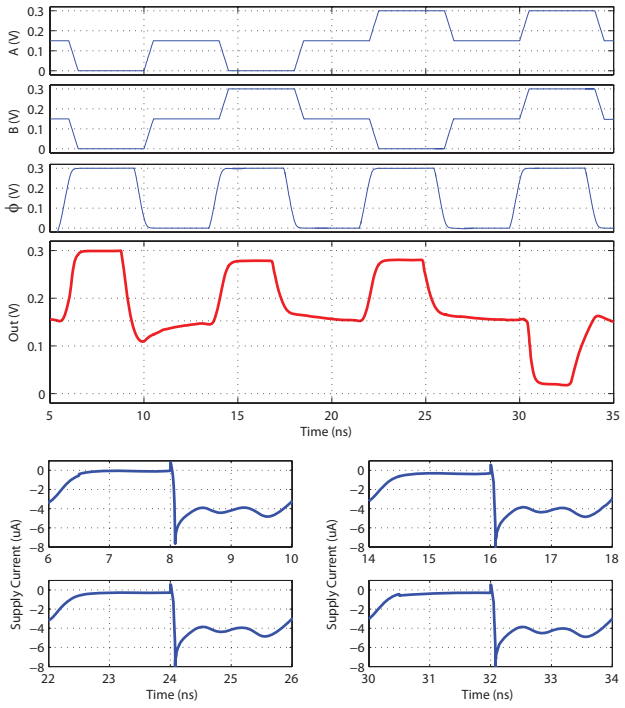


Fig. 4. The simulation results for the ULV NAND gate illustrated in Figure 3(a). The main purpose is to verify the logical behaviour of the gate. Even though that the recharge period consumes more time it would not be of concurn, due to the fact that all gates recharges simultaneously. The four lower plots show the supply current dissipation at the evaluation period for each of the input combinations.

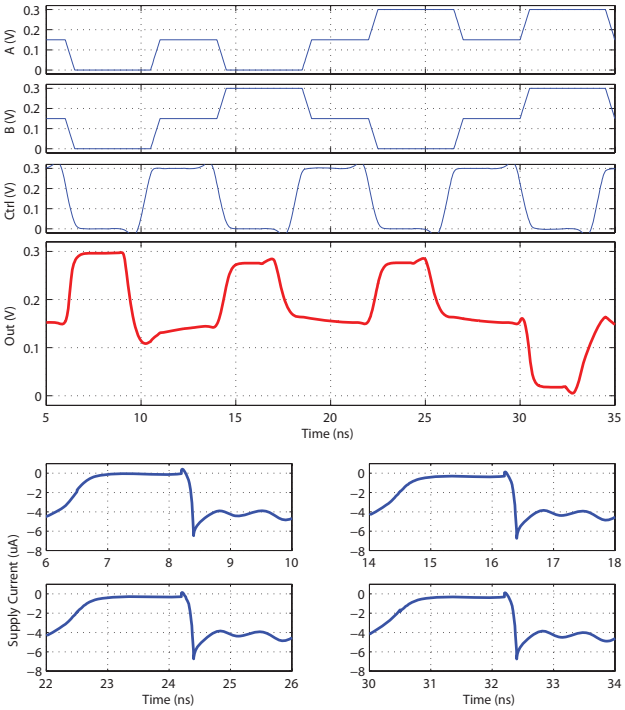


Fig. 6. The simulation results for the ULV NAND gate illustrated in Figure 3(b). In order to obtain the NAND function we have for this example connected the **Ctrl** signal to ϕ. The four lower plots show the supply current dissipation at the evaluation period for each of the input combinations. The results shows the same behaviour in supply current dissipation as the ULV gate. The only obvious difference is the lower amount.

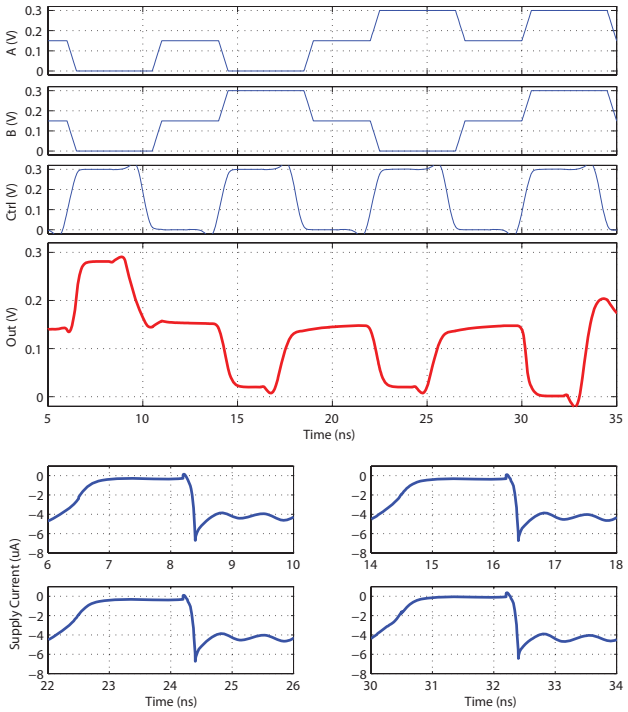


Fig. 7. The simulation results for the ULV NOR gate illustrated in Figure 3(b). In order to obtain the NOR function we have for this example connected the **Ctrl** signal to $\overline{\phi}$. The four lower plots show the supply current dissipation at the evaluation period for each of the input combinations. The results shows the same behaviour in supply current dissipation as the ULV gate. The only obvious difference is the lower amount. The supply current dissipation is quite close to the NAND gate.

Ctrl	A	B	Out	$I_{instantaneous}$	I_{tot}
0	0	0	1	120 nA	4,33 uA
0	0	1	1	110 nA	4,33 uA
0	1	0	1	110 nA	4,33 uA
0	1	1	0	120 nA	4,33 uA
1	0	0	1	150 nA	4,52 uA
1	0	1	0	170 nA	4,52 uA
1	1	0	0	170 nA	4,52 uA
1	1	1	0	110 nA	4,52 uA

Fig. 8. The table lists up the data collected during simulation on the actual current dissipation both for the instantaneous and the total. The instantaneous current dissipation ($I_{\text{instantaneous}}$) is only the gate, while the supply current dissipation (I_{tot}) is the total dissipation including both the gate and the clock buffers. When **Ctrl** = "0" the gate performs NAND, while **Ctrl** = "1" the gate performs a NOR function.

outputs together in one figure, namely Figure 9. In this figure we extracted out only the evaluation period of the gate and compared their respective current disspations. Detailed data collection shows that their dissipation are very similar and therefore quite difficult to seperate for use in power analysis.

IV. Discussion and Conclusion

We believe that we have throughout this paper elaborated on and proposed a design, namely the ultra low voltage NAND gate, to withstand power analysis attack. We have based our work on the ULV gates ability to camouflage the instantaneous current dissipation inside the total supply current dissipation. Furthermore, two different NAND designs are presented and their advantages and disadvanteges are discussesd. Specifically, the NAND / NOR gate has shown a very low, both in the context of variation and in actual amount, current dissipation. All results are obtained in a 90nm STM process.

References

[1] P. Kocher, J. Jaffe, B. Jun. "Differential Power Analysis". *The Proceedings of CRYPTO '99, Lecture Notes in Computer Science*, 2779:17–30, 1999.

[2] P. Kocher. "Timinig Attacks on Implementations of Diffie-Hellman, RSA, DSS and other systems". *Advances in Cryptology CRYPTO'96, Lecture Notes in Computer Science*, 1109:104–113, 1996.

[3] J. Quisquater, D. Samyde. "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*, 2140:200–210, 2001.

[4] K. Tiri, M. Akmal and I. Verbauwhede. "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards". *Proceedings of 28th European Solid-State Circuits Conference (ESSCIRC)*, pages 403–406, 2002.

[5] K. Tiri and I. Verbauwhede. "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation". *Proceedings of Design Automation and Test in Europe Conference and Exhibition*, 1:246–251, 2004.

[6] T. Sundstrom and A. Alvandpour. "A Comparative analysis of logic styles for secure IC's against DPA attacks". *IEEE Proceedings of NORCHIP Conference*, pages 1–4, November 2005.

[7] Y. Berg, D. T. Wisland and T. S. Lande. "Ultra Low-Voltage/Low-Power Digital Floating-Gate Circuits". *IEEE Transactions on Circuits and Systems*, 46(7):930–936, July 1996.

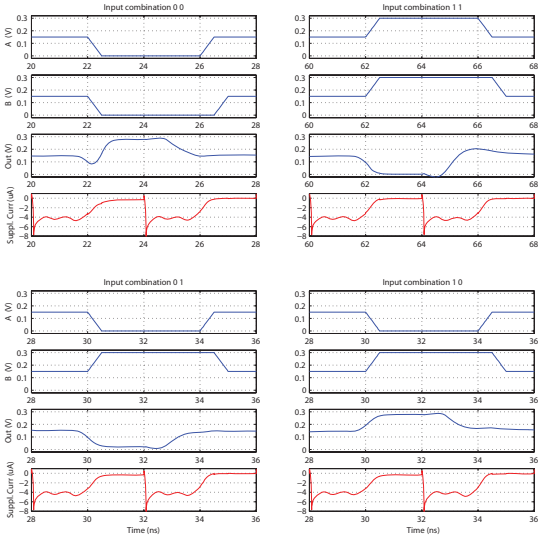


Fig. 9. Simulation results for all the possible input combinations and output combinations for the ULV NAND / NOR gate shown in Figure 3(b). As it is evident the supply current dissipation camouflages the instantaneous dissipation.

[8] Y. Berg, O. Mirmotahari, P.A. Norseng and S. Aunet. "Ultra Low Voltage CMOS Gate". *IEEE International Conference on Electronics, Circuits and System (ICECS)*, pages 818–821, Desember 2006.
[9] O. Mirmotahari and Y. Berg. "Low Voltage Design against Power Analysis Attacks". *Submitted to VLSI DESIGN 2007*, page 1, 1 1.
[10] S. Aunet, Y. Berg, O. Tjore, Ø. N æss, T. Sæther. "Four-MOSFET Floating-Gate UV-Programmable Elements for Multifunction Binary Logic". *Proceedings of the 5th World Multiconference on Systemics, Cybernetics and Informatics (SCI)*, 3:141–144, July 2001.
[11] B. Tongprasit, T.Shibata. "Power-balanced reconfigurable floating-gate-MOS logic circuit for tamper resistant VLSI". *IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 21–24, May 2006.

Omid Mirmotahari Omid Mirmotahari received the M.Sc. degrees in micro-electronics from the Department of Informatics, University of Oslo, Norway, in 2003. He is currently working on a Ph.D. degree at the same department. His research activity is mainly focused on low-voltage/low-power digital and analog floating-gate design.

Yngvar Berg Yngvar Berg received the M.Sc. and Ph.D. degrees in micro-electronics from the Department of Informatics, University of Oslo, Norway, in 1987 and 1992, respectively.

He is currently a Professor with the same department. His research activity is mainly focused on low-voltage/low-power digital and analog floating-gate design. He is the author or coauthor of more than 110 papers.