Assessment of 65nm subthreshold logic for smart RFID applications

Cédric Hocquet, David Bol, Dina Kamel, Jean-Didier Legat
Louvain School of Engineering, UCL, Belgium

Abstract— Nowadays, new ultra-low-power electronic applications require small digital circuits with an increasing number of functionalities and an always decreasing power budget, but compensated by a weak constraint on performances. RFID is such an example of application. In this context, this paper explores the efficiency of 65nm subthreshold logic in an AES coprocessor for smart RFID. The power consumption of such a circuit synthesized with a commercial 65nm library at nominal 1.2V $V_{dd}$ is 1.14µW at 100kHz. As the huge timing slack suggests, the supply voltage can be lowered to reduce the power. A recharacterized library down to 0.4V enables the synthesis of the circuit, still working at 100 kHz (worst-case process and temperature) with a power consumption of 57.5nW. Furthermore, the usefulness of the recharacterized library for logic synthesis in the subthreshold regime is demonstrated.

I. INTRODUCTION

From the highest ski resort of the Alps to the deepest tube of Brussels Underground, Radio Frequency IDentification (RFID) tags are used for rapidly granting access to various facilities. More recently, we saw the british vehicle’s license plates to be equiped with RFID tags for a reliable identification of the vehicles [1]. Those examples are just a small subset of what the RFID technology is used for nowadays.

RFID circuits fall in the category of weakly speed constrained but strongly power constrained circuits i.e. with a fixed small power budget. In addition, recent — and future — applications exhibit an increasing need of features to be packed within the chip, now called the smart RFID tag. Seeing that those devices exchange data wirelessly, such a feature can be the encryption of data, providing the tag with a good security level. The typical encryption scheme for low-cost applications is the Advanced Encryption Standard (AES) [2]. A second strong constraint of RFID tags is the size. A compact scaled technology is thus required. In this work, we target ultra-low-power implementation of an AES module in 65nm technology for smart RFID applications.

The most relevant works related to low-power AES circuits are [3] and [4]. In the first paper, the authors present a chip in 0.35 µm technology with an average power consumption of 4.5 µW at 100kHz. The second paper shows a 0.13µm circuit with an average power of 30µW/MHz. On the other hand, subthreshold logic has been proposed for various ultra-low-power applications. In [5], a microcontroller in 65nm subthreshold logic is implemented and targets biomedical applications. The circuit is operational down to 0.3V. In [6], the author presents a JPEG coprocessor for image processing applications. Working at 0.4V, it achieves an energy consumption 8.3× smaller than at 1.2V.

In the light of those encouraging results, it is compelling to assess the 65nm CMOS technology in subthreshold region with, this time, smart RFID tags as target applications. The remainder of this paper focuses on the following points. In first section, the general power and delay models of digital circuits is recalled. Then, the evolution of standard-cell performances when lowering $V_{dd}$, in terms of delay and power, is addressed. This leads to a first estimation of the expected power consumption reduction. The second section presents the particularisation to the AES circuit. Logic synthesis results with a commercial 65nm standard-cell library at nominal supply voltage $V_{dd}$ (1.2V) are shown. Finally, the recharacterized library at ultra-low $V_{dd}$ and the results for the AES circuit synthesized with this library are presented. It is also shown that logic synthesis with the ultra-low-$V_{dd}$ library provides a circuit with a lower power consumption than the synthesis with the nominal $V_{dd}$ library followed by a reduction of $V_{dd}$.

II. POWER AND DELAY CONSIDERATIONS

A. Power and delay modeling

The power consumption of a logic gate can be divided into two main parts: static power and dynamic power. The first term groups the power consumed when the circuit is at rest. It is exclusively composed of the leakage power. The second term includes all the power consumed when a node is charged or discharged, regardless if it leads to a transition at the output. This dynamic consumption can be again subdivided into two parts, internal consumption (short-circuit current and switching of the nodes inside the logic gate) and switching consumption (switching of the output node). As a reminder, here are the expressions for the power consumption:

$$P_{\text{dyn}} = C_l V_{dd}^2 f_{\text{clk}}$$  \hspace{1cm} (1)
$$P_{\text{stat}} = I_{\text{leak}} V_{dd}$$  \hspace{1cm} (2)

with $C_l$ the output load capacitance, $f_{\text{clk}}$ the clock frequency and $I_{\text{leak}}$ the leakage current, which is mainly composed of the subthreshold, gate and junction leakage. At first approach, we can say that both subthreshold and gate leakage decrease when lowering $V_{dd}$ and that junction leakage is negligible at room temperature.

The expression for the delay of logic gate is:

$$T_{\text{del}} = \frac{C_l V_{dd}}{I_{\text{on}}}$$  \hspace{1cm} (3)

Depending on the device regime, $I_{\text{on}}$ can be expressed as

$$I_{\text{on}} = \mu C_{ox} (W/L)(V_{dd} - V_t)^{\alpha}$$  \hspace{1cm} (4)
in the strong-inversion regime (with $\alpha = 1 \ldots 2$, depending on velocity saturation) [7] or

$$I_{on} = I_0 \frac{V_{dd}^{(1+\alpha)}}{1 - e^{-\frac{V_{th}}{V_{dd}}}}$$

(5)

in the subthreshold regime with the last term negligible for $V_{dd}$ higher than approximately 0.1V (with $I_0$ the bias-independent current, $S$ the subthreshold swing, $\eta$ the DIBL coefficient and $U_{th}$ the thermal voltage).

The careful reader will quickly notice the direct relation to $V_{dd}$ of each of those terms. Regarding the delay, we notice from Equation (4) its quasi linear increase when $V_{dd}$ decreases at high $V_{dd}$ (compared to $V_T$). But this increase is much more important when $V_{dd}$ become smaller as suggests the exponential dependance in Equation (5). Thus, looking at the power, the dynamic consumption will be strongly reduced when lowering $V_{dd}$ whose effect is combined with the engendered frequency reduction. Also, the static power will be reduced with $V_{dd}$ lowering.

B. Evolution of 65nm standard-cell performances with $V_{dd}$

Fig. 1 presents the evolution with $V_{dd}$ of the power and the delay of two std-$V_T$ cells from STMicroelectronics 65nm library. These two cells are an INVX4 (inverter) and an AOI21X2 (2 Input AND into 2 Input NOR). The cells are SPICE simulated with BSIM4 transistor model from STMicroelectronics. As expected, the delay increases when lowering $V_{dd}$ while the power decreases. In the given $V_{dd}$ range, the power at 100kHz input rate is reduced from 550pW to 12pW and from 618pW to 14pW, for the INVX4 and the AOI21X2 respectively. The delays increase from 12ps to 323ns and from 36ps to 961ns. The ratio of the power between the two cells is constant with a mean value of 1.15. The same remark stands for the delay with a mean value of 2.75. Considering a similar evolution for all cells, a good approximation of an entire circuit evolution can be extrapolated from the simulation of those two cells. In the region of interest (somewhere below 0.6V), the delay presents a strong exponential dependence on $V_{dd}$ but, the power presents a weak linear dependence instead.

This leads to the following observations: when choosing the right $V_{dd}$ for the application, it is necessary to consider a sufficient security margin regarding the variability of the devices. At the expense of a small power increase, choosing a $V_{dd}$ not too small ensures the circuit meets the robustness constraint. This will be addressed in the next section.

III. LOW-POWER AES CIRCUIT

Since the foundries do not characterize their libraries at ultra-low $V_{dd}$, the only way to study subthreshold circuits is to measure them once realized (if time-consuming SPICE simulations of the entire circuit are ignored). But no simulations are possible beforehand and, mostly, no optimizations are possible during the synthesis for ultra-low $V_{dd}$. So, the need for an ultra-low-$V_{dd}$ library characterization becomes more and more important when dealing with ultra-low-power circuits. A first approach is given here.

A. Synthesis at nominal $V_{dd}$

The 65nm standard-cell library from STMicroelectronics is used to synthesize the circuit with Synopsys Design Compiler, in low-power process ($L_{OX}=1.85nm$, $L_g=60nm$, std-$V_T=0.6$V). The area and gate count of the circuit are roughly 6400 $\mu$m$^2$ and 1300 gates, respectively. Fig. 2 presents the power consumption for different versions of that library. For each bar, the power is distributed between the leakage power, the internal power, and the switching power.

The first bar shows the results for the 1.2V std-$V_T$ library at 10MHz. The average power totalizes 70.3 $\mu$W and is largely dominated by dynamic power (<1% of static power). As RFID tags are not constrained by speed (to a certain extent), such a frequency of 10MHz is not needed. The data amount to be exchanged by RFID tags is generally rather small and the time to do it can be as high as some hundreds of milliseconds without any discomfort to the user. As an example, it takes roughly 500ms to read the entire memory (1kB) of the widely used EM4450 RFID chip from EM Microelectronics [8] at a frequency of 100kHz. Therefore, such a frequency can be considered here (provided that the circuit can furnish that throughput, which is the case for the AES module with an encryption time of 11.42ms at 100kHz for 128bits of data). The second bar of the figure shows the power using the same library, but at a frequency of 100kHz. Obviously, leakage power is identical, but dynamic power is greatly reduced (by a factor of 100). The total power now reaches...
1.14μW. As all power contributions (leakage, internal and switching) depend on $V_{dd}$, the easiest way to decrease the power consumption is to lower that $V_{dd}$. The next bar of the figure presents the results using the library characterized at the lowest $V_{dd}$ available from STMicroelectronics: 1.0V. At 1.0V, the total power is 0.76μW with a proportional reduction of the three components. Since the frequency is reduced to 100kHz, leakage power is quite important with 36% of the total power consumption. The last bar shows the power for high-$V_t$ ($V_t=0.7V$) devices, still at $V_{dd}=1.0V$. Since the leakage power exponentially depends on $V_t$, using a higher $V_t$ reduces the leakage power. The dynamic power remains on the other hand nearly unchanged.

This power reduction comes with a 24% delay increase when going from 1.2V to 1.0V, because of $I_{m}$ reduction. Since $I_{m}$ depends also on $V_t$ (apparent in Equation (4), comprised in $I_0$ in Equation (5)[9]), the delay increases again (by 48%) when using the high-$V_t$ library. But, thanks to the frequency reduction, the slack time is greatly increased, giving an opportunity for further $V_{dd}$ reduction. The following section will go through this reduction and give its limits.

B. Ultra-low-$V_{dd}$ library characterization and logic synthesis

From section II-B, the extrapolation of the delay for the entire AES circuit enables the estimation of the minimum $V_{dd}$ (restricted to 0.1V steps) leading to the minimum positive slack time i.e. respecting the 100kHz timing constraint. A delay of 9.2μs is obtained at 0.3V with an extrapolated power of 52nW. This serves as starting point for the following section. Synopsys Liberty NCX is used to perform the cell characterizations.

1) Cells selection: All the cells of the standard library from STMicroelectronics are not recharacterized. The following choices are made to determine the cells:

a. small amount of different functions. It has been shown in [10] that a limited number of cells for the synthesis results in a more efficient synthesis with a lower power consumption,

b. all the cells with a large driving strength are evicted. Because of the low speed constraint, it is more efficient to use smaller gates to limit the power consumption,

c. all the cells with a fan-in larger than 2 are evicted. This ensures cells without more than 2 stacked devices, thereby improving the output logic levels and static noise margins at ultra-low $V_{dd}$ [11].

The recharacterized library contains logic gate implementing 10 functions.

2) Cell’s driving strength impact: When designing low-power circuits, the first idea that comes to mind is to use the smallest gates as possible. For low-speed constrained circuits, this is only true at high $V_{dd}$ where the slack time is large enough. With that condition, the synthesizer will always pick up the smallest gates available to reduce the power. But, at ultra-low $V_{dd}$, where the speed constraint becomes significant, it is not the case. This can be observed in Fig.3. The bar (a) presents the power for the AES circuit synthesized at 0.3V with a small library containing only the minimum-size gates for each functions. The next bar (b) is the power for the AES circuit synthesized at 0.3V with a medium library containing 2 or 3 different (small) gate sizes for each functions. Using the medium library gives a power reduction of 17%.

3) Impact of the ultra-low-$V_{dd}$ library on synthesis: It is interesting to investigate the usefulness of the recharacterized ultra-low-$V_{dd}$ library for logic synthesis. To study that, the AES circuit is synthesized with the nominal 1.2V-$V_{dd}$ library. The resulting circuit is then translated to the 0.3V library but without any further optimization. This enables the estimation of the power of the circuit when synthesized at 1.2V but operated at 0.3V. After timing verification, it appears that the $V_{dd}$ has to be raised to 0.32V to meet the throughput constraint. The result is on bar (c) of Fig. 3. As compared to logic synthesis with the 0.3V library (bar (a)), the power is increased by 19%. A library characterized at the right operating $V_{dd}$ is thus necessary in order to efficiently synthesize the circuit with the smallest power.

4) $V_{dd}$ impact: The goal of the work is to reduce, as much as possible, the power consumption of the circuit (actually, a more practical goal should be to meet the energy or power budget available from the batteries or the electromagnetic field the RFID tag uses as power source). The constraint that limits $V_{dd}$ lowering is the speed, even if it is quite low. As explained above, a frequency of 100kHz is suitable for our application. Then, the lowest $V_{dd}$ enabling the circuit to operate at that frequency will be the best one, for power concern [9]. In order to choose the right minimum $V_{dd}$, one have to strongly consider variability. The minimum $V_{dd}$ must still be valid i.e. meet the timing constraint, in worst-case process and temperature conditions. For global variability, worst-case conditions with SS (slow NMOS, slow PMOS) process corner and a temperature of -25°C is considered (low temperature increases $V_t$ and thus gate delay). Fig. 4 shows the evolution of INVX2 inverter delay with $V_{dd}$ for

![Fig. 3. Power consumption with total power (white font) and timing slack [ns] (black font) for the AES circuit synthesized with (a) small library at 0.3V, (b) medium library at 0.3V and (c) small library at 1.2V then $V_{dd}$ lowered to 0.32V](image-url)
nominal (TT (typical NMOS, typical PMOS) process corner and +25°C temperature) and worst-case conditions. At 0.3V, the worst-case delay is 11.5× larger than the nominal one. The estimated $V_{dd}$ of 0.3V given above will have to be raised near 0.4V in order to still meet the timing constraint in worst-case conditions. For simplicity, the supply voltage is considered as ideal (i.e. no noise nor IR drop).

C. Synthesis results

Different characterizations of the library were carried out with $V_{dd}$ varying around the estimated one with the worst-case process and temperature conditions i.e. considering global variability. The lowest $V_{dd}$ still enabling a 100kHz operation is 0.4V. The total power is 57.5nW (with a timing slack of 20.35ns) in nominal (TT (typical NMOS, typical PMOS) process corner and +25°C temperature) and worst-case conditions. At 0.3V, the worst-case delay is 11.5× larger than the nominal one. The estimated $V_{dd}$ of 0.3V given above will have to be raised near 0.4V, in order to still meet the timing constraint in worst-case conditions. For simplicity, the supply voltage is considered as ideal (i.e. no noise nor IR drop).

In order to assess 65nm subthreshold logic for smart RFID applications with ultra-low-power consumption, this work brings up the following. After a brief review of the modeling of power and delay of logic cells, we present the consequences of the reduction of $V_{dd}$ for two basic cells. Then, it shows the logic synthesis results of a 1300-gate AES circuit at nominal supply voltage and points out the possible $V_{dd}$ reduction. It reveals the results of the synthesis with a recharacterized library at ultra-low $V_{dd}$: power consumption is reduced from 1.14μW at 1.2V to 31.3μW at 0.3V. It also proves that the recharacterized library at ultra-low $V_{dd}$ is useful for efficient synthesis regarding power. Considering global variability, a $V_{dd}$ of 0.4V is required to meet the timing constraint. This leads to a power consumption of 57.5nW. The addition of local variability will only require a further 20mV $V_{dd}$ increase.

A further work would be the study of high-$V_{t}$ cells for subthreshold logic.

V. ACKNOWLEDGMENTS

This work was supported in part by the Walloon Region project E-USER (WIST program). The authors would like to thank F. Gosset and F.-X. Staendaert from UCL Crypto Group for providing the VHDL source code of the AES core.

REFERENCES