# Scaling trends of the AES S-Box low power consumption in 130 and 65 nm CMOS technology nodes*

Dina Kamel, François-Xavier Standaert**, Denis Flandre
Microelectronics Laboratory, Université catholique de Louvain,
Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium.
e-mails : {Dina.kamel,fstandae,Denis.flandre}@uclouvain.be

***Abstract* — In the recent years, the power consumption of the AES (Advanced Encryption Standard) S-box has been a target for intensive optimization as the power budget of security enhanced RFID (Radio Frequency Identification Devices) tags is limited to a few µW. In this paper, 0.13 µm and 65 nm CMOS technology nodes are thoroughly investigated in order to select the most appropriate one in terms of power consumption and computation delay. Schematic simulation results of full custom S-boxes show that the optimum choice in our context is the LP (Low Power) flavor of the 65 nm node with Standard $V_t$ (SVT) devices. This leads to a power consumption below 100 nW at 100 kHz using nominal 1.2 V supply voltage which is an order of magnitude lower than what was previously published in the open literature. The reported delay is 2.35 ns. Our study then extends the reduction of the power consumption further by reducing the supply voltage. The power consumption at 100 kHz decreases by 60 % as the supply voltage is reduced to 0.8 V.**

## I. INTRODUCTION

Radio Frequency Identification is gaining more popularity in many applications such as access control, contactless payment, ticketing and supply chain management. Passive tags are the least expensive types of RFID tags. They do not contain a battery and rely on the power received from the reader which constrains the power consumption of the tag to a few µW and limits the communication range to less than 1m.

Along with the increased popularity of RFID, security and privacy issues are raised. This implies the need for a security-enhanced RFID system which comes at the cost of power consumption and die size. Therefore, the right choice of cryptographic function has to be made to optimize the tradeoff between security on one hand and power consumption and die area on the other hand. Symmetric cryptography-based protocols using the Advanced Encryption Standard (AES) Rijndael were proposed for these purposes in a number of publications, e.g. [1] and [2]. Such protocols rely on the existence of low power implementations of the AES that depend on various parameters. In this paper, we consequently investigate the impact of technology scaling on those concerns. In particular, we focus on low power implementations of the AES S-box that is usually considered as one of the most expensive parts of the algorithm.

Different implementations of the AES S-box are available in the literature. A straightforward one would be based on look-up tables (LUT), but it occupies large area [3]. The use of composite field arithmetic to implement the AES S-box with combinational logic reduces the power consumption and the gate count [3-5]. Interestingly, full-custom designs were not intensively addressed in literature: most referenced works use standard synthesis tools and cell libraries to implement the S-box. By contrast, this paper investigates the full-custom design of the S-box presented in [4] that we adopted for its efficient representation in terms of gates count.

With regards to the power consumption available for the AES S-box in passive RFID tag applications, it is stated in [6] that the current consumption budget of such tags is less than 15 µA for a supply voltage of 1.5 V to operate in a range of approximately one meter. For example, a passive RFID tag baseband system was designed in [2] and consumes 4.7 µW. This is a severe limitation to the power consumption of the AES system. Reference [1] reports a current consumption of 8.15 µA for the AES encryption at 100 kHz. An improved version of the AES system that includes decryption and uses several techniques to reduce the power consumption was presented in [7]. It consumes 4.5 µW at 100 kHz. The minimum power consumed by the AES encryption is stated by [8] and consumes 30 µW/MHz. Eventually and as far as the S-box is concerned, [1] uses a 0.35 µm technology and reports a current consumption of 670 nA at 100 kHz. The S-box in [8], which is implemented in a 0.13 µm technology, consumes 8.7 µW/MHz. To the best of the authors' knowledge, this is the minimum power consumption reported in the literature.

To be able to reduce the power consumption of the S-box, three mechanisms are adopted in this work. First, lowering the frequency of operation (without jeopardizing the timing constraints of the whole system) reduces the dynamic power. Thus, 100 kHz data rate is chosen for operation. At low frequencies the static power can no longer be neglected. Therefore the second mechanism aims to reduce the static power by selecting an appropriate advanced technology. The subthreshold leakage was the main contributor in older technologies, but gate leakage is starting to play a significant role in the static power of advanced ones. Another benefit of

* Research supported by the Walloon Region project
E-USER (WIST program). ** Associate researcher of the
Belgian Fund for Scientific Research (FNRS – F.R.S.).

using advanced technologies is the reduction of the die size. Finally, once the static power is reduced, dynamic power is again the target of power reduction by lowering the supply voltage which is the third adopted mechanism. In summary, this work has two main goals. First, we present the advantages of using and selecting advanced technologies to implement the AES S-box for low-power RFID systems. Second, we investigate the impact of reducing the supply voltage on the power consumption and computation delay.

The remainder of the paper is structured as follows. Section II describes the architecture of the S-box. Section III presents the trends of the technologies used. The simulation results of the S-box using different technology nodes are in section IV. Section V shows the impact of reducing the supply voltage. Finally our conclusions are given in section VI.

## II. AES S-Box

The AES S-box mainly consists of a multiplicative inverse in a Galois field GF($2^8$) and an affine transformation. Its gate complexity (and power consumption) is greatly reduced when composite field arithmetic is employed as proposed by [3]. But this requires a transformation matrix to map the elements of the original field GF($2^8$) to the field GF($((2^2)^2)^2$) and an inverse transformation to move back to the original field. In the following, we use the optimized S-box description given in [4]. Since it is not the focus of this paper, we do not detail the mathematical details of this S-box and only provide its high-level architecture in Fig. 1. The gates used in the S-box are implemented in static CMOS logic. The NAND gate has 4 transistors, the AND gate has 6 transistors, while the XNOR and XOR gates each have 12 transistors. The total number of transistors in the implemented S-box is 1,530 transistors which represents 382 NAND-equivalents.

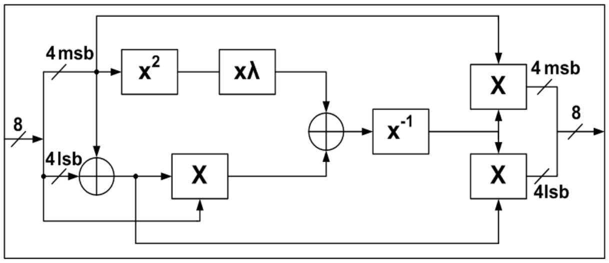

Figure 1. Multiplicative inverse over the composite field GF($((2^2)^2)^2$)

## III. Technology Trends

In general, high performance applications benefit from scaling while low power applications suffer from increased leakage [9]. This is the main reason for developing both the General Purpose (GP) and the Low Power (LP) flavors in advanced technology nodes such as the 65 nm to serve high performance and low power applications, respectively. Two technology nodes are under investigation in this paper, namely 0.13 μm and 65 nm nodes. The former one is available in GP flavor only. Table I shows the main properties of the High-Speed (HS) and the Low-Leakage (LL) NMOS transistors in this 0.13 μm technology. They mainly differ in threshold voltage ($V_t$) and thus differ in off current ($I_{off}$). It can be seen that $I_{off}$, which is dominated by the subthreshold leakage, is 96 % lower in the LL devices than in the HS devices. This is the result of the increased $V_t$. It is also worth mentioning that the gate leakage ($I_g$) is negligible when compared to $I_{off}$.

The main parameters of the 65 nm devices that are available in GP and LP flavors are presented in Table II. The supply voltage ($V_{dd}$) is reduced in the GP devices to reduce the drain induced barrier lowering (DIBL) effect that is becoming more pronounced in smaller technology nodes. Also the gate oxide thickness ($T_{ox}$) is scaled in order to increase the drive on current (hence speed) when the transistor is on and to reduce subthreshold leakage when the transistor is off, but this leads to a three order of magnitude increase in the gate leakage current such that it is no longer negligible with respect to the off current. The $I_{off}$ of the standard $V_t$ (SVT) device is comparable to the one of the HS devices in 0.13 μm node in spite of the reduced $T_{ox}$ due to the reduction in the channel length of the transistor. It can also be seen that the behavior of the $I_{off}$ when moving from SVT devices to High $V_t$ (HVT) devices is the same as in 0.13 μm node. The $I_{off}$ is reduced by 92 % due to the increase in $V_t$. On the other hand, the LP technology flavor aims to reduce both the gate leakage and the off currents. The $T_{ox}$ is increased which leads to a three order of magnitude reduction in gate leakage. The $I_{off}$ of the low $V_t$ (LVT) devices is the same as the one of the GP HVT devices despite the fact that the $V_t$ is lower, because the increase in poly gate length ($L_{poly}$) of LP devices compensates for the reduction of $V_t$. If high $V_t$ devices such as SVT and HVT are used, the $I_{off}$ is further reduced by one and two orders of magnitude, respectively. Although the increase of $T_{ox}$, $L_{poly}$ and $V_t$ in LP devices greatly reduces the subthreshold and gate leakage currents, the driving capability of the devices is degraded. So the supply voltage of the LP devices is increased to 1.2 V to maintain similar on currents ($I_{on}$).

## IV. Simulation results using proposed technologies

### A. Simulating Conditions

Simulations are done at the schematic level using typical device processes along with nominal supply voltage and room temperature of 27 °C. The AES S-box uses a standard CMOS logic style. It is simulated using Spice models provided by an industrial foundry at the chosen technology nodes. The inputs are driven by a buffer that consists of two inverters. The S-box outputs are loaded by 6 fF and 10 fF capacitors adequate for implementations in 65 nm and 0.13 μm technology nodes, respectively. Roughly estimated routing capacitances from layout are added to the internal nodes of the S-box. The input pattern used for simulation consists of 256 different combinations from a constant state to a random one.

### B. Simulation results

Simulation results indicate that at 100 kHz data rate, the power consumption of our S-boxes can be dominated by the static power, as shown in Table III. This directly implies the need for employing mechanisms to reduce this static power. Among them, a proper choice of technology comes at the first place.

TABLE I. MAIN PARAMETERS OF NMOS TRANSISTOR IN 0.13µm TECHNOLOGY (HS = HIGH SPEED, LL = LOW LEAKAGE)

| **Device Type** | **$V_{dd}$ (V)** | **$T_{ox}$ (nm)** | **$V_t$ (mV)** | **$I_{on}$ (µA/µm)** | **$I_{off}$ (nA/µm)** | **$I_g$ (pA/µm)** |
|---|---|---|---|---|---|---|
| HS | 1.2 | 2 | 247 | 670 | 46 | 9 |
| LL | 1.2 | 2 | 336 | 537 | 2 | 12 |

TABLE II. MAIN PARAMETERS OF NMOS TRANSISTOR IN 65 nm TECHNOLOGY (LVT = LOW $V_T$, SVT = STANDARD $V_T$ AND HVT = HIGH $V_T$)

| **Tech. flavor** | **Device Type** | **$V_{dd}$ (V)** | **$T_{ox}$ (nm)** | **$L_{poly}$ (nm)** | **$V_t$ (mV)** | **$I_{on}$ (µA/µm)** | **$I_{off}$ (nA/µm)** | **$I_g$ (pA/µm)** |
|---|---|---|---|---|---|---|---|---|
| GP | SVT | 1 | 1.3 | 45 | 475 | 896 | 62 | 8970 |
| | HVT | 1 | 1.3 | 45 | 555 | 740 | 4.7 | 6180 |
| LP | LVT | 1.2 | 1.85 | 57 | 507 | 855 | 4.2 | 11.4 |
| | SVT | 1.2 | 1.85 | 57 | 645 | 702 | 0.52 | 8 |
| | HVT | 1.2 | 1.85 | 57 | 721 | 501 | 0.036 | 5.4 |

We first observe that using a 0.13 µm node with HS low $V_t$ devices produces a power consumption of 4.95 µW for the S-box at 1 MHz which is comparable to the minimum 8.71 µW/MHz reported in [8]. By contrast, at 100 kHz (the frequency of interest), it consumes 3.71 µW which is dominated by the static power consumption. If LL high $V_t$ devices are used instead, the power consumption at 100 kHz is decreased by one order of magnitude due to the reduction of the static power as a result of increasing the $V_t$, while the S-box delay is increased by 50 %, but still compatible with the computation speed as shown in Table III.

Porting the design to the 65 nm node and using a GP flavor with SVT devices results in even higher power consumption at 100 kHz than for the 0.13 µm node with HS low $V_t$ devices. This is mainly due to the rising contribution of the gate leakage current. However at 10 MHz the power consumption is less than that of the 0.13 µm node with HS low $V_t$ devices because of the reduction of gate capacitance in the 65 nm node which in turn reduces the dynamic power consumption. On the other hand, the delay is reduced by an average of 50 %. If HVT devices are used, the power consumption at 100 kHz is reduced six times due to the reduction of the subthreshold leakage, but it is still 3.5 times higher than that of LL high $V_t$ devices of the 0.13 µm node because the gate leakage is three orders of magnitude higher as shown previously in Tables I and II. The delay of S-boxes using HVT devices increases by 36 % yet it is still lower than the S-box delay using 0.13 µm devices.

Table III also shows that using the LP technology flavor of the 65 nm node with LVT devices reduces the power consumption at 100 kHz three times, but it is still 1.2 times higher than the one of the LL high $V_t$ devices of the 0.13 µm nodes. This is due to the fact that LP flavor reduces the gate leakage current significantly compared to the GP flavor, but using LVT devices has not reduced the subthreshold leakage. On the contrary the off current is two times higher than the one of the LL high $V_t$ devices of the 0.13 µm node as shown in section III while the delay remains the same.

The static power consumption can be reduced by an order of magnitude if SVT devices are used as they decrease the subthreshold leakage current. This limits the contribution of the static power to the total power at 100 kHz to 30 % while the delay is still the same as the delay when using HS devices of 0.13 µm node. If HVT devices are used the static power is further reduced by one order of magnitude at the expense of an increased delay. However the power at 100 kHz is only reduced by 25 % since the dynamic power is now again dominant, while the delay becomes larger than in 0.13 µm node. Therefore the optimum choice would be the LP technology flavor of the 65 nm node using SVT devices to reduce the power to 90.6 nW at 100 kHz without greatly sacrificing the delay of the AES S-box.

## V. REDUCED SUPPLY VOLTAGE

Another important aspect which contributes to the power consumption is the choice of the supply voltage. Most of the power consumptions stated in the literature are given at nominal $V_{dd}$ of the considered technologies. In order to examine the impact of reducing the supply voltage on the performance of the AES S-box, simulations are done using 65 nm LP SVT devices at 100 kHz with different supply voltages. Table IV shows a reduction of power consumption with decreasing $V_{dd}$ which reaches about 60 nW at 1 V and 37 nW at 0.8 V where the devices still operate in super-threshold region as their $V_t$ is 645 mV. The reduction in power is almost quadratic since the dynamic power is dominant and depends quadratically on $V_{dd}$. The delay on the other hand increases to 3.6 ns at 1 V which still fairly compares with the reference 0.13 µm case and to 7.7 ns at 0.8 V which could still be accepted if respecting the timing constraints of the whole system. We mention that further reduction of the supply voltage below $V_t$ will lead to operations in the subthreshold region where robustness becomes an issue due to variability problems that arise in advanced technology nodes and this could cause the system to fail. Another impact of operating in the subthreshold region is the significantly increased delay which may not be tolerated by the whole system.

TABLE III. POWER CONUMPTION AND DELAY OF S-BOX IMPLEMENTED USING DIFFERENT TYPES OF TRANSISTORS IN BOTH 0.13 μm AND 65 nm TECHNOLOGY NODES

| Tech. node | Tech. flavor | Device Type | $V_{dd}$ | Power consumption at 10 MHz | Power consumption at 1 MHz | Power consumption at 100 kHz | Static Power consumption | Delay |
|---|---|---|---|---|---|---|---|---|
| 0.13 μm | GP | HS | 1.2 V | 17.3 μW | 4.95 μW | 3.71 μW | 3.58 μW | 2.2 ns |
| | | LL | 1.2 V | 12.1 μW | 1.34 μW | 262 nW | 142nW | 3.3 ns |
| 65 nm | GP | SVT | 1 V | 10.1 μW | 5.80 μW | 5.37 μW | 5.32 μW | 1.32 ns |
| | | HVT | 1 V | 5.01 μW | 1.31 μW | 934 nW | 895 nW | 1.8 ns |
| | LP | LVT | 1.2 V | 7.06 μW | 938 nW | 326 nW | 258 nW | 1.82 ns |
| | | SVT | 1.2 V | 6.57 μW | 680 nW | 90.6 nW | 25.2 nW | 2.35 ns |
| | | HVT | 1.2 V | 6.35 μW | 639 nW | 67.2 nW | 3.65 nW | 3.65 ns |

TABLE IV. EFFECT OF SUPPLY REDUCTION ON POWER CONSUMPTION AND DELAY PERFORMANCE OF THE AES S-BOX IMPLEMENTED USING 65 nm LP SVT DEVICES AT 100 KHZ

| | Vdd | | |
|---|---|---|---|
| | **1.2 V** | **1 V** | **0.8 V** |
| Power (nW) | 90.6 | 59.6 | 37 |
| Delay (ns) | 2.35 | 3.6 | 7.5 |

## VI. CONCLUSION

The main goal of this work is to take advantage of advanced technologies to reduce the power consumption of the AES S-box without increasing the delay to an extent that jeopardizes the system's timing constraint. Simulation results of the S-box using a 0.13 μm technology interestingly show that at 100 kHz the power consumption is dominated by static power. A thorough investigation was consequently conducted to select the most appropriate technology in order to minimize the power consumption of the S-box. A major disadvantage of advanced technologies is their high gate leakage but it can be mitigated by introducing LP flavor of the nodes. Similarly, using high $V_t$ devices can be used to reduce off current.

The minimum power consumption for the AES S-box reported in the literature is 8.7 μW/MHz [8]. If the static power is assumed to be negligible, which is the best case scenario, then, the power at 100 kHz is 870 nW. Our results conclude that by selecting the LP flavor of the 65 nm node with SVT devices, the power consumption can be reduced to 90 nW at 100 kHz which is one order of magnitude lower than the minimum power published in literature. This comes with insignificant increase in delay with respect to the 0.13 μm node. Further reduction of the power consumption can be achieved by lowering the supply voltage at the expense of increasing the delay. We report a 60 % reduction in power at 100 kHz by decreasing the supply voltage from nominal 1.2 V to 0.8 V which is still above the threshold voltage of the Standard $V_t$ devices used from the 65 nm LP technology. The drawback of this last technique is the increase in delay which is three times higher than at nominal supply voltage.

## REFERENCES

[1] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," In M. Joye, and J.-J. Quisquater (Eds): Sixth Int. Workshop on Cryptographic Hardware and Embedded Systems, Boston, USA, August 2004, LNCS 3156, pp. 357-370 (Springer, 2004).

[2] A. S. W. Man, E. S. Zhang, V. K. N. Lau, C. Y. Tsui, and H. C. Luong, "Low Power VLSI design for a RFID passive tag baseband system enhanced with an AES cryptography engine," RFID Eurasia, 2007 1st Annual.

[3] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-box optimization," In *Proc. 7th Int. Conf. on Theory and Application of Cryptology and Inf. Secur., Advances in Cryptology (ASIACRYPT 2001)*, pages 239–254, Gold Coast, Australia, 2001.

[4] N. Mentens, L. Batina, B. Preneel, and I. Verbauwhede, "A systematic evaluation of compact hardware implementations for the Rijndael S-BOX," In: CT-RSA. Volume 3376 of Lecture Notes in Computer Science., Springer (2005) 323 333.

[5] J. Wolkerstorfer, E. Oswald and M. Lamberger, "An ASIC implementation of the AES Sboxes," Topics in Cryptology – CT-RSA 2002, Proc. RSA Conf. 2002, Feb. 2002.

[6] M. Hutter, "Embedding Crypto on Low-Cost RFID Tags," Talk given at Praxistag RFID-Sicherheit, Oberhausen, Deutschland, December 12, 2007, IAIK, TUGraz.

[7] Y M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES implementation on a grain of sand," IEE Proceedings in Information Security, July, 2005.

[8] P. Hamalainen, T. Alho, M. Hannikainen, and T.D. Hamalainen, "Design and implementation of Low-Area and Low-Power AES encryption hardware core," 9th Euromicro Conference on Digital System Design - Architectures, Methods and Tools (DSD 2006), Cavtat, Croatia, August 30, 2006 - September 1, 2006, pp. 577-583.

[9] International Technology Roadmap for Semiconductors. ITRS Process Integration, Devices & Structures, 2007 eddition. Available at: http://public.itrs.net/