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, 1348 Louvain-la-Neuve, Belgium.
Email: 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 area. 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 have been proposed for these purposes in a number of publications, e.g. [2] and [8]. 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 substitution box (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, but it requires a large number of gates and therefore occupies large area [10]. The use of composite field arithmetic to implement the AES S-box reduces gate count [9]–[11], which reduces the power consumption. 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 [9] that we adopted because of its efficient representation in terms of gate counts.

With regards to the power consumption available for the AES S-box in passive RFID tag applications, it is stated in [5] 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 [8] and consumes 4.7 μW. This is a severe limitation to the power consumption of the AES system. Reference [2] 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 power consumption was presented in [3]. It consumes 4.5 μW at 100 kHz. The minimum power consumed by the AES encryption to date is stated by [4] and consumes 30 μW/MHz. Eventually and as far as the S-box is concerned, [2] and [3] use a 0.35 μm technology and report at 100 kHz a current consumption of 670 nA in [2] and a power consumption of 630 nW in [3]. The S-box in [4], which is implemented in 0.13 μm technology, consumes 8.7 μW/MHz. To the best of the authors' knowledge, these are the minimum S-box power consumptions reported in the literature.

The S-box design presented in this paper includes some of the low-power design methodologies explained in [7] such as minimizing the circuit size by choosing the gate count efficient representation of [9]. At the technological level, power reduction techniques such as choosing advanced technology nodes that offer low supply voltages, using high threshold voltage devices and transistor sizing are adopted. At the architectural level, path equalization using local transformation such as refactoring and pin swapping is used. In order to reduce the power consumption of the S-box more aggressively, three additional 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, a 100 kHz data rate is chosen for operation. At low frequencies, the static power due to leakage currents can no longer be neglected. Therefore, the second mechanism aims to reduce the static power by selecting an appropriate advanced technology. The MOSFET subthreshold leakage was the main contributor to static power in older technologies, but MOSFET gate leakage is starting to play a significant role in advanced ones. An additional benefit of using advanced technologies is the reduction of the die area. Finally, once the static power is reduced, dynamic power is again the target of optimization by lowering the supply voltage. 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 rest of the paper is structured as follows. Section II describes the architecture of the S-box. The trends of the technologies that we considered are presented in section III. 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, conclusions are in section VI.

II. AES S-BOX

The AES S-box mainly consists of a multiplicative inverse of 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 [10]. But this requires a transformation matrix to map the elements of the field GF(2^8) to the GF($((2^2)^2)^2$) composite field and an inverse transformation matrix to move back to the original field. In the following, we use the optimized S-box description given in [9]. Since it is not the focus of this paper, we do not explain the mathematical details of this S-box and only provide its high-level architecture in Fig. 1. The S-box uses only two input gates implemented in standard CMOS logic. The NAND and AND gates have 4 and 6 transistors, respectively, while the XNOR and XOR gates have 12 transistors each. The total number of transistors in the implemented S-box is 1,530 transistors which represents 382 NAND-equivalents.

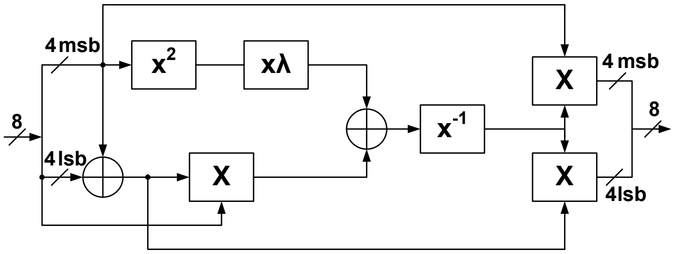

Fig. 1. Multiplicative inverse over the composite field GF($((2^2)^2)^2$).

III. TECHNOLOGY TRENDS

In general, high performance applications benefit from scaling while low power applications suffer from increased leakage [6]. 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 in off current (I_{off}). It can be seen that I_{off}, which is dominated by the subthreshold leakage, is 23 times lower in the LL devices than in the HS devices. This is the result of the increased V_t. It is 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 flavor to reduce dynamic power. Also the gate oxide thickness (T_{ox}) is scaled in order to increase the channel conductivity 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. It can also be seen that the behavior of the I_{off} when moving from Standard V_t (SVT) devices to High V_t (HVT) devices is the same as in 0.13 μm node. The I_{off} is reduced by a factor of 13 as a result of 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 that 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. Due to the increase of T_{ox}, L_{poly} and V_t in LP devices which greatly reduces the subthreshold and gate leakage currents, the driving capability of the devices is degraded. So supply voltage of LP devices is increased to 1.2 V to maintain similar on currents (I_{on}).

IV. SIMULATION RESULTS USING THE 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 is simulated using Spice models provided by the same industrial foundry for 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 fan-out capacitors adequate for implementations in 65 nm and 0.13 μm technology nodes, respectively. Routing capacitances, roughly estimated from

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

Tech. flavor	Device type	V_{dd} V	T_{ox} nm	V_t mV	I_{on} μA/μm	I_{off} nA/μm	I_g pA/μm
GP	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 VT, SVT = STANDARD VT AND HVT = HIGH VT)

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 nA/μm
GP	SVT	1	1.3	45	475	896	62	8.97
	HVT	1	1.3	45	555	740	4.7	6.18
LP	LVT	1.2	1.85	57	507	855	4.2	0.0114
	SVT	1.2	1.85	57	645	702	0.52	0.008
	HVT	1.2	1.85	57	721	501	0.036	0.0054

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 S-box power consumption can be dominated by 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. We first observe that using a 0.13 μm node with HS low Vt devices produces a power consumption of 4.95 W for the S-box at 1 MHz which is comparable to the 8.71 μW/MHz reported in [4] that uses the same technology node. 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 target computation speed as shown in Table III.

Porting the design to the 65 nm node and using 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 gate leakage current and also subthreshold leakage. 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. The power consumption scaling trend versus the data rate is further detailed in [1]. 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 by a factor of 6 thanks 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 the S-box using HVT devices increases by 36 % yet it is still lower than the S-box delay using 0.13 μm devices. Eventually, Table III also shows that using LP technology flavor of the 65 nm node with LVT devices reduces the power consumption at 100 kHz by a factor of 3, but it is still 1.2 times higher than that of the LL high V_t devices of the 0.13 μm node. 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. Meanwhile, 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 28 % 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 26 % since the dynamic power is now again dominant. 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 and 1.2 V of supply voltage without 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 technologies considered. 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}.

TABLE III
POWER CONSUMPTION 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 at 10 MHz	Power at 1 MHz	Power at 100 kHz	Static Power	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	142 nW	3.3 ns
65 nm	GP	SVT	1 V	10.1 μW	5.8 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

V_{dd}	1.2 V	1 V	0.8 V
Power (nW)	90.6	59.6	37
Delay (ns)	2.35	3.6	7.5

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 7.5 ns at 0.8 V which could still be accepted if it respects 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 because of 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.

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 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.

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 an insignificant increase in delay with respect to a 0.13 μm node using HS devices. 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 Vt devices used from the 65 nm LP technology. The drawback of this last technique is the increased delay, which is three times higher than at nominal supply voltage.

ACKNOWLEDGMENT

This work was supported in part by the Walloon Region project E-USER (WIST program). François-Xavier Standaert is an associate researched of the Belgian Fund for Scientific Research (FNRS-F.R.S.). The authors would like to thank David Bol for his help in preparing this article.

REFERENCES

[1] D. Bol, R. Ambroise, D. Flandre, and J.-D. Legat, *Interests and Limitations of Technology Scaling for Subthreshold Logic*, to appear in IEEE Transactions on VLSI Systems, 12 p, to appear, 2009.

[2] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, *Strong Authentication for RFID Systems Using the AES Algorithm*, in the proceedings of CHES 2004, LNCS 3156, pp 357-370, Boston, USA, August 2004.

[3] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, *AES Implementation on a Grain of Sand*, IEE Proceedings in Information Security, July, 2005.

[4] 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 (DSD 2006), pp 577-583, Cavtat, Croatia, August 2006.

[5] M. Hutter, *Embedding Crypto on Low-Cost RFID Tags*, Talk given at Praxistag RFID-Sicherheit, Oberhausen, Deutschland, December 2007.

[6] International Technology Roadmap for Semiconductors, *ITRS Process Integration, Devices & Structures*, 2007 eddition.

[7] J.-P. Kaps, *Cryptography for Ultra-Low Power Devices*, PhD Dissertation, Worcester Polytechnic Institute, May 2006.

[8] 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.

[9] N. Mentens, L. Batina, B. Preneel, and I. Verbauwhede, *A Systematic Evaluation of Compact Hardware Implementations for the Rijndael S-BOX*, in the proceedings of CT-RSA 2005, Lecture Notes in Computer Science, vol 3376 pp 323-333, San Francisco, USA, March 2005.

[10] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, *A compact Rijndael hardware architecture with S-box optimization*, in the proceedings of ASIACRYPT 2001, Lecture Notes in Computer Science, vol 2248, pp 239-254, Gold Coast, Australia, December 2001.

[11] J. Wolkerstorfer, E. Oswald, and M. Lamberger, *An ASIC implementation of the AES Sboxes*, in the proceedings of CT-RSA 2002, Lecture Notes in Computer Science, vol 2271, pp 67-78, San Jose, USA, February 2002.