J Cryptogr Eng (2011) 1:79–86
DOI 10.1007/s13389-011-0005-z

REGULAR PAPER

# Harvesting the potential of nano-CMOS for lightweight cryptography: an ultra-low-voltage 65 nm AES coprocessor for passive RFID tags

**Cédric Hocquet · Dina Kamel · Francesco Regazzoni · Jean-Didier Legat · Denis Flandre · David Bol · François-Xavier Standaert**

Received: 18 November 2010 / Accepted: 16 January 2011 / Published online: 18 February 2011
© Springer-Verlag 2011

**Abstract** An important challenge associated with the current massive deployment of Radio Frequency Identification solutions is to provide security to passive tags while meeting their micro Watt power budget. This can either be achieved by designing new lightweight ciphers, or by proposing advanced low-power implementations of standard ciphers. In this paper, we show that the AES algorithm can fit into this micro Watt power budget by combining ultra-low-voltage implementations with a proper selection of the process flavor in a low-cost nanometer CMOS technology. Interestingly, this approach only requires slight modifications to the standard EDA tool flow, without incurring the engineering costs of architecture optimizations. In order to demonstrate this claim, we successfully designed and manufactured an AES coprocessor in a 65 nm low-power CMOS process. We prove with measurement results obtained from a set of 20 manufactured dies that the proposed coprocessor can be safely operated down to 0.32 V with an energy per 128-bit encryption/decryption at least 2.75× lower than in previously published low-power AES implementations.

**Keywords** AES · RFID · Low power implementations

C. Hocquet (✉) · D. Kamel · F. Regazzoni · J.-D. Legat · D. Flandre · D. Bol · F.-X. Standaert
ICTEAM Institute, Université catholique de Louvain, Louvain-la-Neuve, Belgium
e-mail: cedric.hocquet@uclouvain.be

*Present Address:*
C. Hocquet
3 Place du Levant, 1348 Louvain-la-Neuve, Belgium

## 1 Introduction

Radio Frequency Identification (RFID) is a ubiquitous technology that enables identification of non-line-of-sight objects or subjects. Based on cheap RF micro-circuits—called tags—apposed on or incorporated into the items to identify, the RFID technology is widely deployed in our everyday live. Several billion RFID tags are spread every year, in applications as diverse as pet identification, supply chain management, Alzheimer's patient tracking, cattle counting, etc. [12]. RFID tags suited to such applications do not cost more than a few tens of cents [37]. As a result of this emerging deployment, the need of security features for such devices also increases. But since RFID tags either operate on tiny batteries (active tags) or harvest energy from a wireless link (passive tags), they are strongly constrained in terms of power consumption.

Protecting data manipulated by small embedded devices can typically be done using block ciphers, for which different approaches can be considered. First, as the task of implementing cryptographic algorithms within the very strict area and power budget of an RFID is particularly challenging, one can take advantage of so-called lightweight ciphers [29]. That is, block ciphers that have been specially designed with low cost issues in mind. Solutions in the literature range from new ciphers, e.g. PRESENT [4], to slightly modified standard algorithms, e.g. based on the DES [26]. While low cost cryptography is an important research area, its drawback is that lightweight ciphers are generally less investigated than standard ones, hence leading to a reduced confidence of the users (which may not be founded though, as long as no practical attacks is exhibited against them). Hence, another approach is to implement standard ciphers directly, e.g. the AES Rijndael [34], trying to reduce the power consumption on the circuit side, rather than on the algorithmic one. In this respect, the

effect of technological enhancements may have a high impact on the final results, and is certainly worth to be investigated as deeply as the design of new ciphers.

In this paper, we typically follow this second approach. We show that it is possible to address the issues of lightweight cryptography by fully exploiting the improved low-power features of nanometer CMOS, and by aggressively adopting established methodologies to reduce the power consumption of digital circuits. In addition, as already observed in previous works, the power and area budget are critical for passive RFIDs, but the throughput constraint can be relaxed below the Mbps range [20]. This allows a significant down scaling of both the supply voltage $V_{dd}$ and the clock frequency $f_{clk}$. This scaling generally reduces the power consumption drastically, and can be effectively combined with a proper flavor of nanometer CMOS technologies. In particular, the widespread Low-Power (LP) CMOS technology flavor at 65/45 nm node allows minimizing the energy consumption of logic circuits at ultra-low voltage (0.3–0.5 V), when operating at $f_{clk}$ in the range of 0.1–1 MHz [6,7]. Finally, 65 nm CMOS technologies feature low fabrication costs for high-volume production and are thus particularly appealing for mass production devices such as passive RFID tags.

In order to validate our claims, we implemented an ultra-low-power AES coprocessor for smart RFID applications, which completely exploits the advantages offered by the adoption of a 65 nm LP technology. In particular, we implemented a 128-bit core of which the architecture is similar to the one proposed by Feldhofer et al. [14] and further reduced its power consumption using classical circuit optimization techniques. The designed core was finally fabricated and we verified experimentally, based on a set of 20 manufactured chips, that our coprocessor can reliably operate down to 0.32 V, leading, to the best of our knowledge, to the smallest power consumption achieved by an AES coprocessor to date. Our work consequently proves that the full exploitation of technology enhancements is an interesting tradeoff between the need of low power consumption and the optimization efforts to reach such a result.

The remainder of the paper is organized as follows. In Sect. 2, we review some important related works. In Sect. 3, we recall the AES algorithm and the constraints of passive RFID tags. We then present our design choices in Sect. 4, while the proposed coprocessor architecture and its ultra-low-voltage implementation are presented in Sect. 5. Finally, measurement results are reported in Sect. 6.

## 2 Related works

While some important research efforts have been recently dedicated to the implementation of public key cryptographic coprocessors for RFID tags (e.g. the work of Batina et al. [2]), symmetric cryptography and block ciphers remain by far the most deeply investigated solution to provide low cost security features in this context. As previously mentioned, there exist several lightweight ciphers tailored for this purpose. As the focus of this work is on standard ciphers, in particular the AES Rijndael, we mainly review important results in this line. More precisely, and among the large variety of implementation works on this cipher, the ones of Good et al. [16] and Feldhofer et al. [14] have goals that are remarkably close to ours. The latter presents a design of AES that can be realized using approximately 3400 gates. The proposed implementation has a datapath of 8 bits and uses a single S-box (denoting the non-linear substitution function in the block cipher), where the substitution values are calculated using algorithmically optimized combinatorial logic. The maximum operating frequency is 80 MHz at 3.3 V, and significantly decreases (together with the power consumption) when the design is operated at lower voltage. Eventually, the results in [14] are obtained using a 0.35 µm CMOS technology, which is a significant difference with the work presented here. Particular attention should also be ported to the work of Hämäläinen et al. [17]. They present another 8-bit implementation of an AES core, but with a parallel datapath instead of the sequential iterative datapath. This enables a lower cycle count and a higher throughput but increases the area of the core (estimated by the authors, for both encryption/decryption functionality, to 3,875 gates). Since the core presented by Feldhofer et al. is, to the best of our knowledge, the smallest possible implementations of an AES core in the literature, we use this reference as a starting point to design our ultra-low-power AES coprocessor in 65 nm CMOS technology.

## 3 AES specifications and implementation constraints for passive RFID

This section first recalls the principles of the AES algorithm and highlights the main components of passive RFID tags. Then, their power and throughput requirements, which will drive the design choices, are reviewed.

The AES algorithm supports key size of 128, 192 or 256 bits, and block size of 128 bits. It is an iterative algorithm repeating the same transformations over the matrix of data, called the state. The encryption begins with the first key addition, then the round function is iterated a specific number of times, depending on the key size. For the encryption, the round is composed of the following four transformations: *SubBytes*, which is a non-linear byte substitution transformation composed of the multiplicative inverse in the finite field GF($2^8$) followed by an affine transformation over GF(2), *ShiftRows*, which cyclically shifts to the left the bytes in the last three rows of the state with different offsets,

*MixColumns*, which multiplies modulo $x^4+1$ the columns of the state by the polynomial $\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$, and finally *AddRoundKey*, which simply adds the round key to the state. The round keys are generated from the secret key by means of an expansion routine. The round transformations are cyclically executed at each round, with the only difference of the last one, which does not include the *MixColumns* transformation. Further details about the AES algorithm can be found in the standard specification [34]. For low-cost application, the typical choice is to support only the key size of 128 bits.

When implementing the AES for passive RFID tags, it is of crucial importance to meet the area constraints typically ranging from a hundreds to a few thousands of gates [21], and to fit within a limited power budget. In fact, passive RFID tags are typically battery-less devices, which harvest energy from a wireless link. Passive tags are composed of three main parts: an analog front-end to communicate with the reader, a non volatile memory, and a logic part, where the cryptographic function has to be integrated [13]. The power budged for the full tag varies with the class of RFID, those operating in the UHF band being more constrained than those operating in the HF band. Some recent passive UHF RFID tag implementations, without cryptographic functionality, present a power consumption in the 1–10 μW range [11,19]. Thus we have to reasonably consider that the power budget devoted to the cryptographic function must be lower than 1 μW. In opposition to the power and area limitation, the throughput requirement of passive RFIDs is significantly relaxed. As a result, with an operational frequency $f_{clk}$ in the range of 0.1–1 MHz, a coprocessor that performs a 128-bit encryption in around 1,000 clock cycles gives acceptable latency (1–10 ms) and throughput (10–100 kbps) [24].

## 4 Design choices

For fitting the AES into the passive RFID power budget, we rely on an ASIC implementation of an AES coprocessor with two aggressive design choices to save power at circuit level: the use of a nanometer CMOS technology and the operation at ultra-low voltage.

### 4.1 CMOS technology selection

CMOS technology scaling aims at doubling the number of transistors per die every two years, according to the famous Moore's law [28]. For ultra-low-power systems such as RFID tags, the most advanced CMOS technologies are often discarded, even within the research community [1,38], because of their high mask and fab equipment cost. In particular, recent ultra-low-power AES coprocessors are implemented in 0.35–0.13 μm CMOS technologies [14,16]. However, with the continuous CMOS scaling, 65 nm fabs will hopefully be amortized in a couple of years and could be made available for fabrication of RFIDs with more advanced functionalities, i.e. smart tags, thanks to more transistors available on the same die area.

Besides these cost considerations, power consumption is a key technical factor in the selection of a CMOS technology. As technology scales down, dynamic power decreases thanks to the reduction of load capacitances. But this positive effect comes at the cost of an increased contribution of the leakage power, which becomes more and more pronounced, due to the inherent reduction of the threshold voltage $V_t$ (leading to subthreshold leakage) and gate oxide thickness $T_{ox}$ (leading to gate leakage), to maintain speed at scaled supply voltages for high-performance applications. At the low target clock frequencies of RFID applications, leakage power might dominate, which makes CMOS technology scaling not desirable [18]. Therefore, in nanometer CMOS technologies, such as 65 nm, both General-Purpose (GP) and Low-Power (LP) flavors are developed. Each one comprises several threshold voltage $V_t$ options in order to achieve various speed/leakage trade-offs.

In order to best motivate our selection of technology, we first performed simulations of an AES S-box at two technology nodes [22]: 0.13 μm and 65 nm nodes, at their respective nominal $V_{dd}$. For the latter, we considered the two flavors available: GP and LP. Figure 1 shows the comparison of both leakage and dynamic power at 1 MHz. Without loss of generality, standard-$V_t$ (SVT) devices with minimum sizes are considered for the sake of simplicity. The benefit of using the 65 nm GP over the 0.13 μm technology node is clearly seen as the dynamic power is reduced by almost 60%. However, the leakage power increases by more than one order of magnitude. This is a direct result of increased subthreshold and gate leakage currents. The use of 65 nm LP flavor yields an interesting trade-off between dynamic and leakage power as seen from Fig. 1. In 65 nm LP flavor, the printed gate length

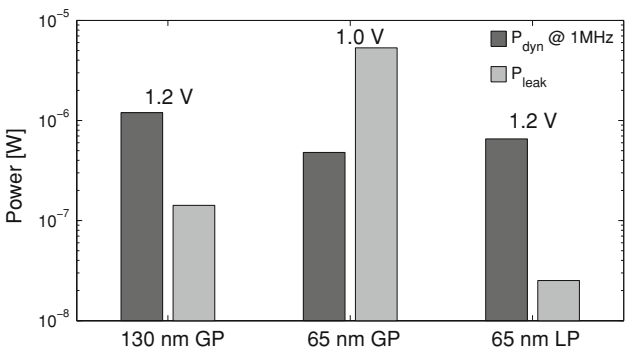



**Fig. 1** Simulation results of S-box power consumption using both 130 and 65 nm GP/LP technologies (SVT devices) at nominal supply voltages

is increased by 15 nm and $V_t$ is increased by 200 mV to reduce subthreshold leakage. In addition, $T_{ox}$ is increased by 0.6 nm to reduce gate leakage. As a result, leakage power of the S-box is reduced by more than two orders of magnitude, while the dynamic power is increased by only 36% due to the higher nominal $V_{dd}$. This shows that 65 nm LP technology is a viable choice for passive RFIDs regarding power consumption.

### 4.2 Ultra-low voltage operation

In order to further reduce the power/energy consumption, ultra-low voltage operation is chosen. Ultra-low voltage (ULV) circuits in submicron CMOS technologies have been proposed in the late 1990's to enable new ultra-low-power applications [32]. The idea is to scale aggressively the supply voltage to save dynamic energy $E_{dyn} \propto C_L V_{dd}^2$ associated to the switching of on-chip capacitances [9]. This comes with large speed penalty when the supply voltage becomes close or even below $V_t$, leading to subthreshold operation. Indeed, in subthreshold regime, the on current of MOSFETs is exponentially reduced with a corresponding increase in gate delay and thus cycle time $T_{cycle}$. This is only acceptable in applications with relaxed timing constraints. Many ultra-low-voltage circuits have recently been demonstrated: microcontrollers for biomedical applications [25,33], for wireless sensor nodes as well as dedicated ASICs for communication [35] or image processing [15,30].

The speed penalty of ultra-low-voltage circuits also increases leakage energy $E_{leak} = V_{dd} \times I_{leak} \times T_{cycle}$, due to the integration of leakage power over $T_{cycle}$. This leads to a trade-off between $E_{dyn}$ reduction and $E_{leak}$ increase when scaling down $V_{dd}$ to minimize energy. This trade-off is known as the minimum-energy point i.e. the supply voltage that minimizes total energy [9], which is often between 0.3 and 0.5 V, depending on the circuit characteristics and the technology. This minimum-energy point appears for one particular clock frequency [5] and it has recently been shown that in 65/45 nm LP CMOS technologies, it is reached for clock frequencies between 100 kHz and 1 MHz, depending on the circuit characteristics [7]. This frequency range matches the target for passive RFIDs, thereby motivating the use of a 65 nm LP technology at ultra-low voltage.

To validate this choice, we performed measurements of the S-box from Mentens et al. [27] that we use in this work, and have been previously implemented on silicon in a 65 nm technology with LP flavor and SVT (standard $V_t$) devices. Those measurements for both total energy and delay, as $V_{dd}$ is scaled down from nominal to ultra-low values, are presented in Fig. 2. It can be seen that at 0.4 V the delay reaches almost 1 µs indicating a maximum frequency of operation of ~1 MHz, while total energy is minimized around 1 MHz, which is consistent with [7]. This confirms the interest of ultra-low-voltage logic in 65 nm LP for passive RFID applications.

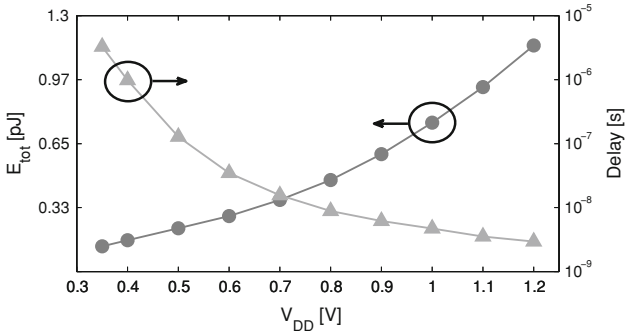



**Fig. 2** Measured total energy and delay scaling with $V_{DD}$ of S-box

## 5 AES coprocessor implementation

### 5.1 AES architecture

It is well know that the S-box is one of the most critical parts of the full AES design for power, area, and performance concerns. For this reason, it is the typical starting point when an AES coprocessor is optimized. Many different S-box architectures were proposed in the past. The most straightforward implementation is obtained by HDL coding the S-box function as look-up table, letting the synthesis tool optimize its implementation with logic gates. Since this is the approach used very frequently, we use it as a baseline for the comparison.

Concerning low area, an interesting S-box was proposed by Satoh et al. [31]. The authors exploit the mathematical properties behind the non-linear transformation to implement its function as a multiplicative inverse over the composite Galois field $GF(((2^2)^2)^2)$, with subsequent forward and inverse transformation from and to $GF(2^8)$. It results in a very area-efficient design characterized by a limited gate count. This design was further optimized by Mentens et al. in [27] and Canright et al. in [10]. The version of Mentens is the one used in our comparisons.

Finally, the architecture proposed by Bertoni et al. [3], is particularly appealing for low power implementations, since it limits the spurious switching activity by one-hot coding the $2^N$ possibilities for the $N$-bit input vector. The S-box transformation is thus a simple permutation of the one-hot bit lines. Those permuted lines are then re-encoded into an $N$-bit vector to form the output.

Synthesis and place/route of the S-box with these three different architectures have been carried out with a library that we recharacterized at 0.4 V. Post-layout simulation results are given in Table 1. All the three architectures are able to

**Table 1** Comparison of S-box architectures at 0.4 V

| S-box architecture | Area ($\mu m^2$) | $P_{dyn}$ @1 MHz (nW) | $P_{leak}$ (nW) | $P_{tot}$ (nW) |
|---|---|---|---|---|
| Baseline (look-up table) | 3,190 | 61.9 | 3.24 | 65.1 |
| $GF(((2^2)^2)^2)$ [27,31] | 1,150 | 136 | 1.03 | 137 |
| One-hot coding [3] | 3,110 | 48.7 | 3.03 | 51.7 |

meet a micro seconds timing constraint, which will allow reaching the 0.1–1 MHz for the full AES coprocessor. As expected, the $GF(((2^2)^2)^2)$ S-box is the most compact by almost a factor 3. Consequently, it exhibits the lowest leakage power $P_{leak}$. On the other hand, the significant dynamic power $P_{dyn}$ reduction of the one-hot coding version makes it the most interesting for power concern. At the scale of the full AES coprocessor, we finally selected the $GF(((2^2)^2)^2)$ S-box, as it allows saving 13% of area penalty at the cost of only 6% of additional power consumption.

Once the S-box is chosen, we looked at the full AES coprocessor. As discussed in Sect. 2, we started from the implementation proposed by Feldhofer et al. [14]. In particular, it supports key size of 128 bits, is based on an 8-bit datapath, and has memory requirements limited to a RAM of only 32 bytes. The datapath, depicted in Fig. 3, features a single S-box module (to implement both the *SubBytes* operation and the key expansion), a module able to calculate a quarter of the *MixColumn* operation per clock cycle, and a small submodule to add the round constant value. The *ShiftRows* operation is performed by accessing the register in the appropriate way. Since this is the smallest implementation reported up to now and since additional optimization would require significant efforts while leading to very limited improvements, we selected the same architecture for implementing the proposed coprocessor, with the only exception of the S-box, that we replaced by the one used by Mentens et al. with the $GF(((2^2)^2)^2)$ composite field version previously discussed.

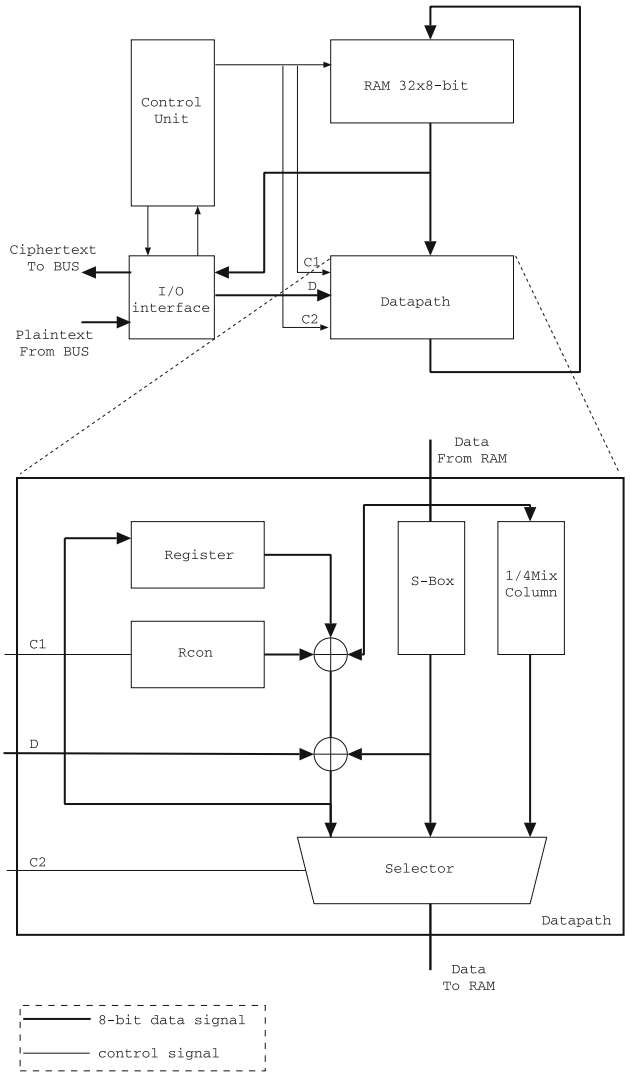
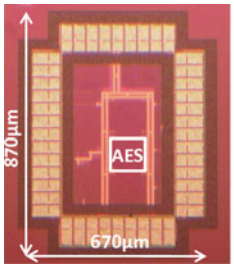



**Fig. 3** Architectural block diagram of the AES module proposed by Feldhofer et al. [14]

## 5.2 Ultra-low-voltage implementation

For low engineering cost concern, we used a semi-custom flow with a standard-cell library of logic gates and mainstream EDA tools. However, at ultra-low voltage the $I_{on}/I_{off}$ ratio is dramatically reduced, which degrades noise margins of logic gates. In 65/45 nm technologies, the high random $V_t$ variability and Drain-Induced Barrier Lowering (DIBL) effect may result in functional failures (stuck-at faults) due to vanishing noise margins [6]. For solving this problem, we first selected a library with upsized gate length i.e. 80 nm instead of 60 nm for the baseline library. Indeed, an upsized gate length MOSFET strongly mitigates DIBL effect and limits variability, which improves noise margins [6]. For the same reasons as well as subthreshold swing improvement, an upsized gate length further improves energy per operation while slightly boosting speed at ultra-low voltage thanks to reverse short-channel effect [23]. As the noise margin problem is more important in cells with many stacked or parallel devices [36], we exclude these cells from the library with upsized gate length to form a library with a restricted number of cells. For low-power concern, cells with large driving strengths are also excluded from this modified library. Finally, we only kept non-ratioed flip-flops that provide robustness at ultra-low voltage, to synthesize the RAM from Fig. 3. The modified library contains 74 cells (24 logic functions).

Given that the foundry libraries are only characterized at nominal $V_{dd}$ (1.2 V), it has to be re-characterized for timing, power and capacitive load at the target $V_{dd}$ of operation to enable proper netlist optimization. Indeed, synthesis at




| AES coprocessor | 128-bit encryption/decryption |
|---|---|
| Technology | 65nm LP CMOS – 7 metal layers |
| Silicon area | 135 µm × 135 µm (core) |
| Package | CQFP 44 |
| $V_{dd}$ range | 0.32-1.2V (core) / 1.2V (I/O) |
| Max. frequency | 890 kHz @0.4V |
| Power | 0.85µW @0.4V |

**Fig. 4** Die microphotograph and characteristics

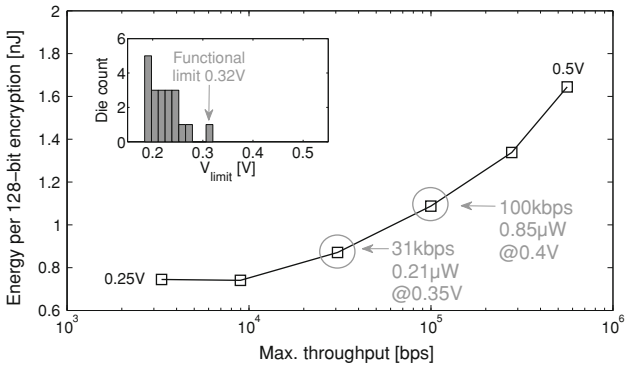



**Fig. 5** Measured energy per encryption versus maximum throughput at ultra-low voltage. The *inset* shows the minimum supply voltage ensuring correct functionality ($V_{limit}$) for the 20 measured dies

the target $V_{dd}$ allows power savings at a given clock frequency. Automatic recharacterization was performed with *Synopsys Liberty NCX* tool at 0.4 V and the recharacterized library was later used with standard EDA tools for synthesis and place/route. The recharacterization time for the modified library is 20 min on a 2 GHz Intel Xeon dual core machine under Linux operating system.

The actual implementation flow starts with a basic logic synthesis at a worst-case clock frequency of 100 kHz with *Synopsys Design Compiler* in worst-case timing condition: SS process corner (slow NMOS and slow PMOS transistors) and low temperature (−15°C is considered here). Indeed, low temperature reduces $I_{on}$ at ultra-low voltage and thereby increases delay, leading to worst-case timing conditions [8]. This first netlist is then back-annotated for switching activity at each net (by means of an HDL simulator) and an incremental synthesis is performed with the target to minimize power. Let us mention here that we do not use clock gating to ensure a safe timing closure, given the high gate delay variability at ultra-low voltage. The resulting optimized netlist is finally placed and routed in *Cadence SoC Encounter* where the timing is verified, now that the routing parasitics are known.

## 6 Measurement results

The AES coprocessor has been implemented in a 65 nm LP CMOS technology with seven interconnect metal layers, five layers being used in the core. Microphotograph of the die[1] and main characteristics are given in Fig. 4. The 20 available dies, encapsulated in CQFP44 packages, were successfully tested for both encryption and decryption.

Maximum frequency was extracted for different supply voltages at room temperature. A typical die supports 890 kHz (resp. 270 kHz) at 0.4 V (resp. 0.35 V). This gives a throughput of 100 kbps (resp. 31 kbps) with a latency of 1.3 ms (resp. 4.2 ms) for encryption/decryption of a 128-bit plain text. Measured power consumption is 0.85 µW (resp. 0.21 µW), which fully meets the power budget for the AES in a passive RFID tag. Figure 5 shows the energy/throughput tradeoff with $V_{dd}$ scaling. The minimum-energy point is close to 0.3 V ($V_{min}$) at 80 kHz ($f_{min}$), which is consistent with LP flavor in 65/45 nm technology [7]. The measured minimum energy ($E_{min}$) is 0.74 nJ per 128-bit encryption.

At ultra-low voltage, logic circuits in nanometer technologies are prone to functional failures due to (1) reduced noise margins (degraded output logic levels) caused by high $V_t$ variations and DIBL effect in logic gates and (2) hold time violations due to high $V_t$ variations in the clock tree [36]. In order to extract the functional limit ($V_{limit}$) of the AES coprocessor, we performed measurements of 20 dies at $V_{dd}$ from 0.15 to 0.4 V with 1 mV step at a relaxed clock frequency. The inset in Fig. 5 shows the $V_{limit}$ histogram. The best-case die correctly operates at 0.193 V while the worst-case needs 0.32 V. The functional failure of the worst-case die comes from hold time violations and not from logic levels degradation because the implementation choices of upsized gate length and restricted number of cells efficiently improves the noise margins. This shows that the AES coprocessor is fully functional at 0.4 V.

Finally, Table 2 compares the proposed AES chip with previous silicon realizations. For the sake of comparison fairness, we scaled the frequency and the supply voltage of the proposed corpocessor during mesurement to achieve a 36 kbps throughput equivalent to the results reported in [16]. At this throughput, compliant with passive RFID applications, the proposed AES coprocessor consumes at least 2.75× less power than previous realizations. To the authors' knowledge, the proposed chip is the best-in-class ultra-low-power AES implementation for RFID tags, showing the effectiveness of ultra-low-voltage design in nanometer CMOS technologies. In general, our results show that the important gains obtained by technological improvements offer additional budget for advanced applications in low cost embedded devices.

[1] The die includes other circuitry not covered in this work.

**Table 2** Comparison with state of the art in ultra-low-power AES chips

| AES chip | Gate count | CMOS technology | Core area ($mm^2$) | Cycle count | $V_{dd}$ range (V) | $V_{dd}$ (V) @ 36 kbps | Frequency (kHz) @ 36 kbps | Power (μW) @ 36 kbps |
|---|---|---|---|---|---|---|---|---|
| [14] | 3,400 GE | 0.35 μm | 0.25 | 1,032 | 0.65–3.3 | 0.65 | 290 | 2.45[b] |
| [16] | 5,500 GE | 0.13 μm | 0.021[a] | 356 | 0.75–1.3 | 0.75 | 100 | 0.69 |
| Proposed | 3,500 GE | 65 nm LP | 0.018 | 1,142 | 0.32–1.2 | 0.36 | 322 | 0.25 |

[a] Cell area only
[b] Extrapolated at minimum reported $V_{dd}$ with $V_{dd}^2 \times freq$ scaling law (neglecting leakage power in 0.35 μm CMOS)

## 7 Conclusions

An ultra-low-voltage AES coprocessor was manufactured in 65 nm LP CMOS technology for passive RFID tags. Compact design with an 8-bit architecture and an implementation flow slightly modified for robust ultra-low-voltage operation enable best-in-class power consumption for passive RFID tags. Measured power consumptions are 0.21 and 0.85 μW at 31 kbps/0.35 V and 100 kbps/0.4 V, respectively. This shows that combined ultra-low-voltage logic implementation and the use of a nanometer CMOS technology can be used to fit AES cipher within the minute power budget of passive RFID tags without time-consuming architecture optimizations.

**Acknowledgments** This work was supported by the Walloon Region under E.USER project. Cédric Hocquet is with UCL thanks to a grant from the Fonds pour la formation à la Recherche Industrielle et Agronomique (FRIA) of Belgium. David Bol and François-Xavier Standaert are with UCL as postdoctoral and associate researchers of the Fonds de la Recherche Scientifique—FNRS of Belgium.

## References

1. Barnett, R., Balachandran, G., Lazar, S., Kramer, B., Konnail, G., Rajasekhar, S., Drobny, V.: A passive UHF RFID transponder for EPC Gen 2 with-14dbm sensitivity in 0.13 μm CMOS. In: IEEE International Solid-State Circuits Conference, 2007. ISSCC 2007. Digest of Technical Papers, pp. 582–623. IEEE (2007)
2. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I.: An elliptic curve processor suitable for RFID-tags. IACR (2006, eprint)
3. Bertoni, G., Macchetti, M., Negri, L., Fragneto, P.: Power-efficient ASIC synthesis of cryptographic sboxes. In: Proceedings of the 14th ACM Great Lakes Symposium on VLSI, p. 281. ACM (2004)
4. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: Present: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) 9th International Workshop on Cryptographic Hardware and Embedded Systems—CHES 2007. Lecture Notes in Computer Science, vol. 4727, pp. 450–466. Springer, Berlin (2007)
5. Bol, D., Ambroise, R., Flandre, D., Legat, J.: Analysis and minimization of practical energy in 45 nm subthreshold logic circuits. In: IEEE International Conference on Computer Design, 2008. ICCD 2008, pp. 294–300. IEEE (2008)
6. Bol, D., Ambroise, R., Flandre, D., Legat, J.: Interests and limitations of technology scaling for subthreshold logic. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **17**(10), 1508–1519 (2009)
7. Bol, D., Flandre, D., Legat, J.: Technology flavor selection and adaptive techniques for timing-constrained 45 nm subthreshold circuits. In: Proceedings of the 14th ACM/IEEE International Symposium on Low power Electronics and Design, pp. 21–26. ACM (2009)
8. Bol, D., Hocquet, C., Flandre, D., Legat, J.: The Detrimental Impact of Negative Celsius Temperature on Ultra-Low-Voltage CMOS Logic. In: European Solid-State Circuits Conference ESSCIRC (2010)
9. Calhoun, B., Wang, A., Chandrakasan, A.: Modeling and sizing for minimum energy operation in subthreshold circuits. IEEE J. Solid State Circuits **40**(9), 1778–1786 (2005)
10. Canright, D.: A very compact S-Box for AES. In: Rao, J.R., Sunar, B. (eds.) Cryptographic Hardware and Embedded Systems—CHES 2005. Lecture Notes in Computer Science, vol. 3659, pp. 441–455. Springer, Berlin (2005)
11. Cho, N., Song, S.J., Kim, S., Kim, S., Yoo, H.J.: A 5.1 μW UHF RFID tag chip integrated with sensors for wireless environmental monitoring. In: Proceedings of the 31st European Solid-State Circuits Conference, 2005. ESSCIRC 2005, pp. 279–282 (2005)
12. Das, R., Harrop, P.: RFID forecasts, players and opportunities 2011–2021. IDTechEx Report (2010)
13. Feldhofer, M., Wolkerstorfer, J.: Strong crypto for RFID tags—a comparison of low-power hardware implementations. In: IEEE International Symposium on Circuits and Systems, 2007. ISCAS 2007, pp. 1839–1842. IEEE (2007)
14. Feldhofer, M., Wolkerstorfer, J., Rijmen, V.: AES implementation on a grain of sand. IEE Proc. Inf. Secur. **152**(1), 13–20 (2005)
15. Finchelstein, D., Sze, V., Sinangil, M., Koken, Y., Chandrakasan, A.: A low-power 0.7-V H. 264 720p video decoder. In: IEEE Asian Solid-State Circuits Conference, 2008. A-SSCC'08, pp. 173–176. IEEE (2008)
16. Good, T., Benaissa, M.: 692-nW Advanced Encryption Standard (AES) on a 0.13 μm. IEEE Transactions on Very Large Scale Integration (VLSI) Systems (99), 1 (2009)
17. Hamalainen, P., Alho, T., Hannikainen, M., Hamalainen, T.: Design and implementation of low-area and low-power aes encryption hardware core. In: 9th EUROMICRO Conference on Digital System Design, pp. 577–583. IEEE (2006)
18. Hempstead, M., Wei, G., Brooks, D.: Architecture and circuit techniques for low-throughput, energy-constrained systems across technology generations. In: Proceedings of the 2006 International Conference on Compilers, Architecture and Synthesis for Embedded Systems, pp. 368–378. ACM (2006)
19. Hong, Y., Chan, C.F., Guo, J., Ng, Y.S., Shi, W., Leung, L.K., Leung, K.N., Choy, C.S., Pun, K.P.: Design of passive UHF RFID tag in 130 nm CMOS technology. In: IEEE Asia Pacific Conference on Circuits and Systems, 2008. APCCAS 2008, pp. 1371 –1374 (2008)
20. EPCglobal Inc.: EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz Version 1.2.0 (2008). http://www.gs1.org/

21. Juels, A.: RFID security and privacy: a research survey. IEEE J. Sel. Areas Commun. **24**(2), 381–394 (2006)
22. Kamel, D., Standaert, F., Flandre, D.: Scaling trends of the AES S-Box low power consumption in 130 and 65 nm CMOS technology nodes. In: IEEE International Symposium on Circuits and Systems, 2009. ISCAS 2009, pp. 1385–1388. IEEE (2009)
23. Kim, T., Keane, J., Eom, H., Kim, C.: Utilizing reverse short-channel effect for optimal subthreshold circuit design. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **15**(7), 821–829 (2007)
24. Kitsos, P., Zhang, Y.: RFID Security—Techniques, Protocols and System-on-Chip Design. Springer, Berlin (2008)
25. Kwong, J., Chandrakasan, A.: Variation-driven device sizing for minimum energy sub-threshold circuits. In: Proceedings of the 2006 International Symposium on Low Power Electronics and Design, pp. 8–13. ACM (2006)
26. Leander, G., Paar, C., Poschmann, A., Schramm, K.: New lightweight DES variants. In: Fast Software Encryption, pp. 196–210. Springer, Berlin (2007)
27. Mentens, N., Batina, L., Preneel, B., Verbauwhede, I.: A systematic evaluation of compact hardware implementations for the Rijndael S-box. Topics in Cryptology—CT-RSA 2005, pp. 323–333 (2005)
28. Moore, G., et al.: Cramming more components onto integrated circuits. Proc. IEEE **86**(1), 82–85 (1998)
29. Poschmann, A.: Lightweight cryptography—cryptographic engineering for a pervasive world. Cryptology ePrint Archive, Report 2009/516 (2009). http://eprint.iacr.org/
30. Pu, Y., de Gyvez, J., Corporaal, H., Ha, Y.: An ultra-low-energy/frame multi-standard JPEG co-processor in 65nm CMOS with sub/near-threshold power supply. In: IEEE International Solid-State Circuits Conference. ISSCC 2009. Digest of Technical Papers, pp. 146–147. IEEE (2009)
31. Satoh, A., Morioka, S., Takano, K., Munetoh, S.: A Compact Rijndael Hardware Architecture with S-Box Optimization. In: Proceedings of ASIACRYPT 2001. LNCS, vol. 2248, pp. 239–254 (2000)
32. Soeleman, H., Roy, K.: Ultra-low power digital subthreshold logic circuits. In: Proceedings of the 1999 International Symposium on Low Power Electronics and Design, pp. 94–96. ACM (1999)
33. Sridhara, S., DiRenzo, M., Lingam, S., Lee, S., Blazquez, R., Maxey, J., Ghanem, S., Lee, Y., Abdallah, R., Singh, P., et al.: Microwatt embedded processor platform for medical system-on-chip applications. In: IEEE Symposium on VLSI Circuits (VLSIC), 2010, pp. 15–16. IEEE (2010)
34. National Institute of Standards Technology (NIST): Announcing the Advanced Encryption Standard AES. Federal Information Processing Standards Publication 197 (2001)
35. Sze, V., Chandrakasan, A.: A 0.4-V UWB baseband processor. In: Proceedings of the 2007 International Symposium on Low power Electronics and Design, pp. 262–267. ACM, New York (2007)
36. Verma, N., Kwong, J., Chandrakasan, A.: Nanometer MOSFET variation in minimum energy subthreshold circuits. IEEE Trans. Electron. Dev. **55**(1), 163–174 (2007)
37. Want, R.: An introduction to RFID technology. Pervasive Comput. **5**(1), 25–33 (2006)
38. Yeager, D., Zhang, F., Zarrasvand, A., George, N., Daniel, T., Otis, B.: A 9 μA, Addressable Gen2 Sensor Tag for Biosignal Acquisition. IEEE J. Solid State Circuits **45**(10), 2198–2209 (2010)