Design of an Ultra Low-Power RFID Baseband Processor Featuring an AES Cryptography Engine

Andrea Ricci, Matteo Grisanti, Ilaria De Munari and Paolo Ciampolini
University of Parma, Department of Information Engineering
Via G. P. Usberti, 181/A - I-43100 Parma, Italy
andrea.ricci@unipr.it

Abstract

Cheap passive radio frequency identification (RFID) tags operating in ultra high frequency (UHF) bands are fostering innovation in several field such as building access control, goods tracking, supply chains management and automatic product checkout. RFID transponders can also be coupled to tiny sensors, enabling non invasive monitoring of environmental and personal parameters. To ensure the privacy of highly sensitive data, encryption and authentication capabilities should be embedded in RFID devices, in a fashion compatible with tight power budgets of wireless devices. In this contribution, a baseband-processor is introduced, which complies with ISO 18000-6C (EPC Class1 Gen2) protocol and integrates AES primitives aimed at secure data transmission. Performance of passive RFID devices is limited by the available power, harvested from the incoming radiation. Power-saving strategies are devised, both at the system and the circuit levels. A set of standard cells has been designed, suitable for near-threshold voltage operations. Physical implementation on CMOS 0.18 μm technology has been carried out and the chip has being fabricated.

1. Introduction

Unique identification and tracking of items represents a major concern in several fields, such as manufacturing units, logistics and transportation. RFID transponders embody a cost-effective solution for object identification, enabling fully automation of supply chains [1]. RFID tags are candidate to replace the widespread optical barcode technologies, overcoming some of their inherent limitations: RFID does not require optical visibility of the tag, allows for longer read distance and for much larger data capacity. RFID transponders are also expected to become a key element in the "ubiquitous computing" scenario: tags will

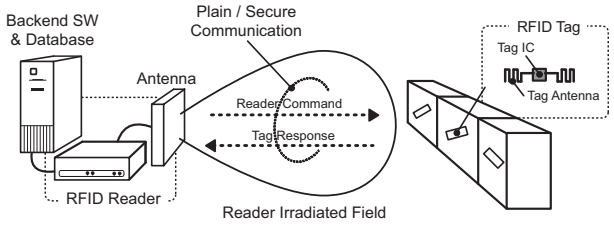

Figure 1. Architecture of an RFID system.

embed tiny sensors, and will enable low-cost devices for control of environmental parameters, as well as lightweight wearable sensors for personal health and safety monitoring. This may involve transmission of private or sensitive data, and thus raises critical security concerns. To make RFID devices suitable for such applications, security features must be embedded into RFID devices, supporting data *privacy* and *authentication* [2]. Low power implementation is needed at the tag side, to preserve battery life in active tags or to ensure the tag functionality and performance in passive ones. In this work, a low-power implementation of an RFID baseband processor is presented, fully compliant with the recent ISO 18000-6C standard (i.e. EPC Class1 Gen2, [3]). The system also serves as the tag central controller and includes an AES engine (*Advanced Encryption Standard*, [4]), devoted to data encryption and decryption. AES cipher could be exploited for data protection and reader authentication, improving communication security while preserving the standard protocol data flow. Design of the digital processing core accounts for a careful control of area and instantaneous power consumption. Near-threshold voltage operations are exploited, in order to reduce power dissipation at a minimum, still maintaining fair performance [5]. In order to push to the technology limit the power performance, a compact set of standard cells has been purposely designed, aimed at optimizing power-limited applications. Physical implementation on CMOS 0.18 μm technology has been carried out and the chip has

978-0-7695-3277-6/08 $25.00 © 2008 IEEE
DOI 10.1109/DSD.2008.129

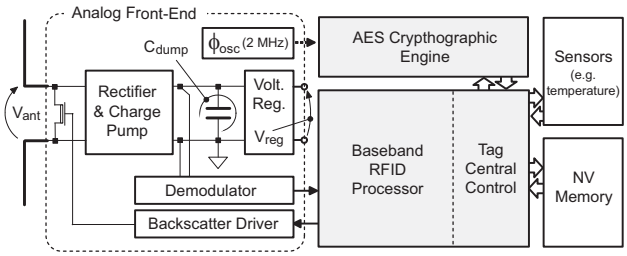

Figure 2. Architecture of the RFID transponder.

been fabricated.

In the following, the architecture and implementation of the baseband digital circuitry are described: in Sect. 2 below, the system requirements are reviewed. Sect. 3 more specifically describes the architecture of baseband communication core, whereas Sect. 4 deals with AES engine design. Next, Sect. 5 provides a detailed analysis of baseband-processor implementation, in terms of area and power consumption figures. Conclusions are eventually drawn in Sect. 6.

2. RFID System Requirements

Basic performance target of the tag consist in a read range as large as possible, while keeping lowest possible die cost and supporting interoperability. To achieve such a goal, several design aspects should be carefully considered: fabrication process, power consumption and air interface choice.

2.1. Fabrication Process

Since extremely low costs are necessary, the choice of fabrication technology should be mainly driven by die-cost considerations. In terms of performance, RFID tags usually pose no critical speed constraint, whereas power is the main concern. A further issue is related to the technologies maintenance, since long-running technology are needed to preserve the investment costs. In the present work, we selected a 0.18 µm CMOS technology node for the prototype tag physical implementation, in order to investigate its aptness for future development. Such a technology is mature enough to ensure proven reliability, at the same time still ensuring long-term running perspectives and not yet presenting too severe leakage current problems. More precisely, a commercial, mixed mode/RFCMOS technology (UMC 0.18 µm - 1.8V/3.3V-1P6M-MMC-EDR process) has been selected, featuring one polysilicon and six metal interconnection levels, and suitable for the implementation of the analog front-end section as well. Although the technology provides designers with transistors featuring different threshold voltages (high-V_{th} = 0.5 V and low-V_{th} = 0.35 V), only high-V_{th} devices were exploited in the digital core design, in order to minimize off-current leakage contribution to the power consumption. Target supply voltage was regulated close to the transistor threshold (i.e., V_{DD} = 0.6V), in order to limit dynamic power consumption as well and taking advantage of the relatively coarse speed requirement: simulations indeed predict adequate performance even at worst operating conditions.

2.2. Power Constraints

Due to the lack of internal power supply, performance of passive RFID systems in the UHF range is usually limited by the tag power constraints. Fig. 2 depicts the high-level block diagram of a passive transponder, which may include sensor devices (e.g., an integrated temperature sensor). Power is supplied to the digital core, non-volatile memory and sensor section by rectifying and regulating voltage extracted at the antenna terminals (V_{ant}). Such a voltage, in turn, depends on the power radiated by the forward link and available at the tag: for a given power needed by the tag, this limits the actual read range according to the Friis equation below [6]:

$$r \leq \frac{\lambda}{4\pi}\sqrt{\frac{\mathrm{P}_{EIRP}\mathrm{G}_{tag}}{\mathrm{P}_{tag}}} \qquad (1)$$

where P_{EIRP} is the reader effective radiated isotropic power, G_{tag} is the tag antenna gain, and λ is the RF carrier wavelength. An on-chip dumping capacitor (C_{dump}) is employed as energy-storage element, which is mandatory in order to maintain an adequate power supply level during the interrogation and backscatter phases. The dumping capacitor should be completely charged within the time interval that the standards reserve for the RFID powering up, just before the interrogation phase start ($t = t_0$). This initial condition can be expressed as follows:

$$V_{rect,t_0} = V_{rect,\max} = \frac{Q_{\max}}{C_{dump}} \cong 1\,V \qquad (2)$$

where V_{rect} represents the voltage level at the dumping capacitor terminals. Moreover, assuming a linear voltage regulator is used, a minimum input voltage

$$V_{rect}\,(t) > V_{rect,\min} \cong 0.8\,V \qquad (3)$$

should be maintained during the operating phase, in order to ensure the correct generation of regulated voltage (V_{reg}). This condition is fulfilled when the tag energy consumption,

$E_{out}(t)$, during the operating phase ($t_0 < t < t_{end}$), is limited as follows:

$$E_{out}(t) < E_{in}(t) + \\ + \frac{C_{dump}}{2}\left(V^2_{rect,t_0} - V^2_{rect,\min}\right) \quad (4)$$

where:

$$E_{out}(t) = \int_{t_0}^{t} P_{out}(\tau)\, d\tau = \\ = \int_{t_0}^{t} \left[V_{drop}(\tau) + V_{reg}(\tau)\right] I_{reg}(\tau)\, d\tau\ , \quad (5)$$

$$I_{reg} = I_{bp} + I_{mem} + I_{sens} + I_{osc} \quad (6)$$

and

$$E_{in}(t) = \int_{t_0}^{t} P_{in}(\tau)\, d\tau \cong \eta_{rect} G_{tag} \int_{t_0}^{t} P_{EIRP}(\tau)\ d\tau \quad (7)$$

where η_{rect} is the rectifier conversion efficiency, V_{rect} is the rectified voltage, V_{drop} is the voltage drop across the linear regulator and I_{reg} represents the sum of baseband processor, memory, sensors and oscillator current consumption. Theoretically, the tag's available instantaneous power ($dE_{out}(t)/dt$) is finite (limited by the incoming power $dE_{in}(t)/dt$), while the total energy can be infinite as long as the tag harvests power from the field irradiated by the reader. Equation (4) simply emphasizes the fact that the dumping capacitor acts as an energy reservoir, which may support the circuit whenever the required (output) power exceeds the incoming (input) one. In such cases, extra current is drained from the capacitor to preserve circuit operation, down to the limit when the rectified voltage (V_{rect}) decreases down to its minimum value $V_{rect,min}$.

Power-supply gating could be used to place sensor devices in stand-by while the tag is performing communication tasks (i.e., during transponders arbitration or while retrieving memory content). By cutting off the sensor current, whenever it is possible, negative impact on the read range is minimized.

To keep power consumption as low as possible, cells have been designed accounting for a supply voltage V_{DD} equal to 0.6 V, slightly larger than the threshold voltage of high-V_{th} devices. This allows for achieving low-power operations while still retaining a satisfactory performance [5] and tolerating fluctuation of the voltage regulator output. Since the library design was strictly targeted to the specific application, just a limited variety of cells has been actually implemented: however, it has been shown elsewhere [7, 8], that, even in a more general case, a reduced set of cells, if properly selected, does not significantly affect performance and may improve the efficiency of the synthesis process.

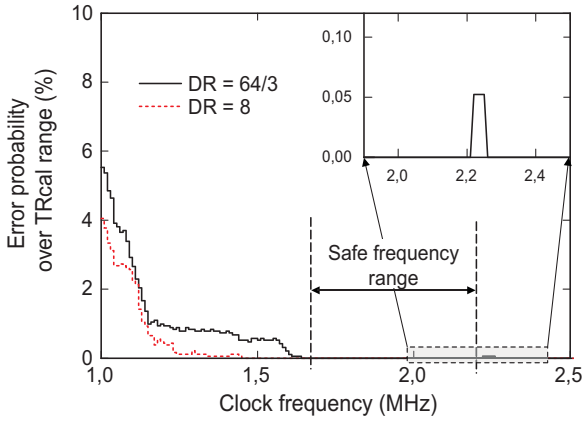

Figure 3. Baseband-processor clock frequency selection.

2.3. Air Interface Standard

According to ISO 18000-6C standard, interrogator-to-tag communication is based on a packet-based scheme [3]. Transmission data rate, defined by the interrogator, could be changed at each communication round. In order to receive PIE-encoded payload data (and to reply to the reader, if necessary) the tag measures reference time intervals (*Tari*, *RTcal* and, if needed, *TRcal*) included in the reader packet preamble. The measurement of *Tari* interval (i.e. the 0 symbol length, chosen in the $\{6.25\ \mu s, 12.5\ \mu s, 25\ \mu s\}$ set), and *RTcal* (i.e., data-0 plus data-1 length) can be reliably carried out with a reference clock frequency of at least 1 MHz.

The interrogator specifies tag's backscatter link frequency (LF, in the 40 KHz ÷ 640KHz range) by means of different combinations of the *TRcal* interval and divide ratio parameters (DR, included in the payload). The actual LF and its tolerance FT constrain the tag minimum clock frequency. With reference to (8) below, we have hence estimated such a frequency by means of simulations

$$|FT| = \frac{|T^{nom}_{LF} - \hat{n}T_{clk}|}{\hat{n}T_{clk}} \quad (8)$$

where

$$\hat{n} = \begin{cases} round\left(\left(3\left\lfloor\frac{TRcal}{Tclk/2}\right\rfloor\right)\Big/(64\cdot 2)\right) & DR = 64/3 \\ round\left(\left\lfloor\frac{TRcal}{Tclk/2}\right\rfloor\Big/(8\cdot 2)\right) & DR = 8\ . \end{cases} \quad (9)$$

The plot in Fig. 3 illustrates results for both DR$= 64/3$ and DR$= 8$: the percentage of backscatter frequencies (LF) that

do not satisfy frequency tolerance (FT) constraints are depicted, as a function of local oscillator frequency. The clock frequency should be chosen in the 1.6 MHz – 2.20 MHz safe range. A somehow larger figure (e.g. 2 MHz) respect to minimum reliable frequency is to be adopted if a coarse-precision ring oscillator is used as low-power local clock generator.

2.4. Security Issues

Communication with passive RFID transponders customarily do not account for security checks: the tag identifier and tag-acquired data (if any) are sent with no security validation upon reader interrogation. Tag privacy can thus be violated by misbehaving readers, and false authentication could be obtained by counterfeit transponders [9]. More secure communications could be obtained by making the tag capable of performing on-board data cyphering (e.g. by means of *symmetric-key encryption* processing). However, design and implementation of cryptographic primitives embedded into the tag digital processor should match its tight constraints: limited power (only a few μA current could be available) and limited circuit complexity (some thousands of equivalent gates). Among all symmetric-key encryption standards, AES-128 represents a feasible solution to enhance RFID communication channel security: the cipher algorithm can be implemented with a low gate-count whereas encryption time can be tuned to achieve a limited power consumption [9, 10].
In the following discussion, we consider an RFID system [9] which includes n tags, each embedding a unique identifier T_i and a distinct, randomly generated, secret key k_i. The list of secret keys is stored in a database accessible via secure connection by the RFID readers. After tag population arbitration, each tag, T_i, can authenticate itself to the reader according to the following procedure:

1. the reader generates a random 128-bit wide plaintext P, and stores it at a given location (a_{res}) in the memory of i-th tag and keeps irradiating transponder population;

2. the i-th tag computes $C = e\,[P, k_i]$ (where e represent the symmetric-key encryption function) and stores it back to its memory;

3. after a proper time interval, the interrogator requires to read the memory location and validates ciphertext C.

The above procedure allows to introduce secure transmission, without requiring any modification of ISO 18000-6C standard communication flow. Moreover, exchanging plain- and ciphertext by means of tag memory allows the tag for carrying out the encryption with no critical time constraints: this, in turn, permits to adopt relatively "slow" architectural solutions, reducing power consumption. Silicon area can be saved as well, since the reserved a_{res} memory location could coincide with AES state memory.
On-board encryption/decryption facilities can be exploited to provide secure sensor data two-way transfer: encrypted control signals could be embedded into data words by readers and written into the tags dedicated memory bank. The irradiated tag then verifies such a location, decrypts control bits and executes required action. Required data can then be packed by the AES encryption engine into the ciphered data exchange location, and thus securely received by the reader. By this strategy, secure embedded sensor control could be performed without introducing new *ad-hoc* packets.

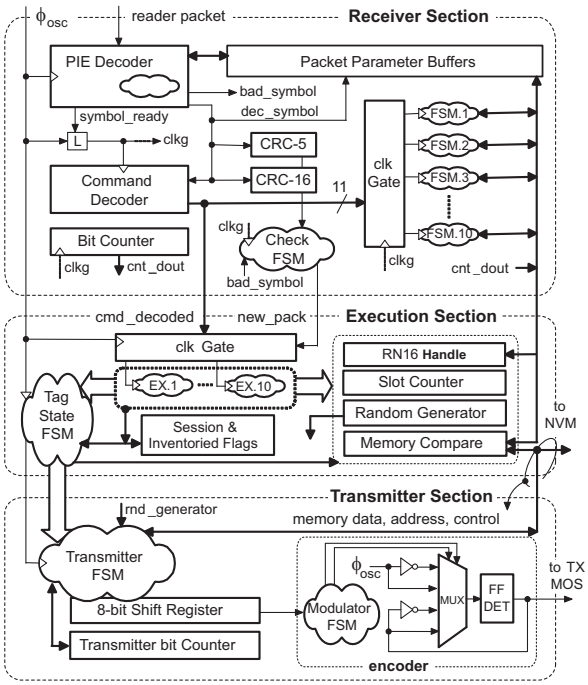

Figure 4. ISO 18000-6C baseband-processor architecture.

3. ISO 18000–6C Baseband Processor Architecture

In order to reduce dynamic power consumption, the processor design has been optimized to keep the switching activity and the driving clock frequency as low as possible. Fig. 4 shows the tag architecture: three main sections are highlighted, aimed at packet reception, command execution and transmission reply.

According to Section II-2, the input clock frequency (ϕ_{osc}) is set to 2 MHz. ϕ_{osc} feeds PIE Decoder block,

which samples incoming reader packets. Decoding operations are triggered by the packet delimiter identification. PIE Decoder embeds a binary counter and some buffers exploited for *Tari*, *RTcal* and *TRcal* measurement. A simple FSM uses the same counter to interpret subsequent interrogator symbols, comparing counter output with *RTcal/2*. When receiving a new symbol, the PIE decoder issues a T_{osc} wide pulse which is used to gate clock signal feeded to remaining packet reception circuitry. Command Decoder block analyzes the first decoded symbols to identify mandatory commands, while a 6-bit counter (Bit Counter) computes total received symbols. Ten independent FSM are implemented to manage different mandatory standard commands: by keeping them separate, more effective fine-grained clock-gating strategies can be adopted, at the expense of a slight area increase. Received symbols flow through error-processing elements (CRC-16 or CRC-5, depending on actual received command) to report bad PIE-encoded data.

The tag state is managed through an always active FSM, running at 2 MHz. Execution phase starts when the receiver Check FSM validates incoming packet. Execution data path includes four independent modules devoted to 16-bit random compare, Slot Counter operations, random generation and memory comparison.
Generation of 16-bit random numbers, required by the arbitration process, is accomplished by a LFSR-based random generator. Initialization is performed during power-up and while tag remains in ready state. During arbitration and transmission the random generator is normally turned off in order to reduce power dissipation. Short re-activations (T_{osc} wide) are used for further random number extraction, during arbitration process. Memory comparison is performed in a 8-bit serial fashion, to save area and switched capacity.

Transmitter operations include FM0 and Miller encoding of different data (random numbers and memory content). According to such schemes, a signal switch occurs at the end of each bit period; symbols "0" (FM0) or "1" (Miller) are encoded by an additional signal edge at the middle of the period. Thus, actual symbol switching may occur at a doubled frequency with respect to the selected clock. To avoid doubling the local clock frequency, a simple circuit solution has been devised, based on a four-input multiplexer. The encoder circuit is shown in Fig. 4 and its operation can be straightforwardly interpreted: the symbol boundary transitions are accomplished inverting the value of the output DET flip-flop, whereas the mid-symbol inversions are obtained sampling a single pulse clock. A finite state machine properly drives the multiplexer, depending on the transmitted data and the symbol period.

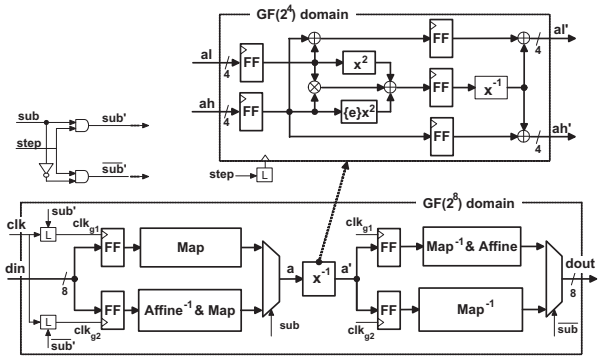

Figure 5. SubBytes/InvSubBytes submodule implementation.

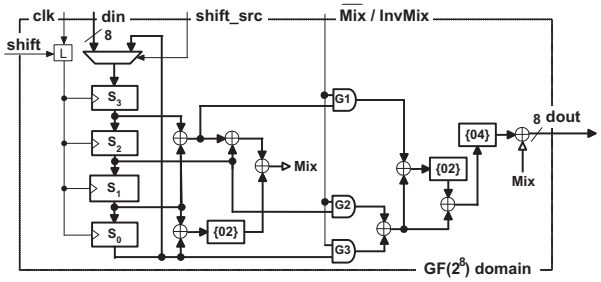

Figure 6. MixColumns/InvMixColumns submodule implementation.

4. AES Algorithm and Implementation

The standard AES algorithm [4] is a symmetric block cipher, based on arithmetic in a finite Galois field, $GF(2^8)$, supporting variable text and key length of 128, 196, or 256 bits. In this work, a fixed data and key length of 128 bits is used, suitable for RFID system security [11]. During encryption, a sequence (called *round*) of four primitive functions, (`SubBytes`, `ShiftRows`, `MixColumns` and `AddRoundKey`) is applied $N_r - 1$ times (with $N_r = 10$ for 128-bit text length) to the state block (the plain text, at the first round). An initialization `AddRoundKey` precedes the main loop, whereas `SubBytes`, `ShiftRows` and `AddRoundKey` operation follow the main elaborations. State block transformations require a key modification (`KeyExpansion`) procedure at each round. AES arithmetic features enable for functional step reordering and merging [9]: `AddRoundKey`, `SubBytes` and `ShiftRows` functions can be reduced to a single step (further referred as `MergedStep`) in order to save several clock cycles. Such a composed function is repeated for N_r times, followed by

MixColumns, or by AddRoundKey in the last step. Moreover, a simple modification to the keyExpansion routine [4] enables for similar cypher/decypher processing. The performance of the AES engine mostly depends on the SubBytes and MixColumns operations. In the present implementation, byte-oriented operations are exploited to minimize silicon area and power consumption. The AES architecture includes three main sections: datapath, controller and state/key memory. The datapath includes an S-Box [4] and several XOR banks for MergedStep implementation, whereas MixColumns sequential processing requires four 8-bit registers and simple XOR gates. The same HW resources are exploited for KeyExpansion processing. Two separate 32-byte memories are used for State and Key storage. Extensive clock-gating is implemented, to save dynamic power. Independent functional units are exploited in this case too to allow for fine tuning of clock gating strategies.

4.1. Merged AddRoundKey, SubBytes and ShiftRows Implementation

As introduced above, three AES primitive function has been merged [9] in a pipelined structure, to save clock cycles and improve cypher efficiency at 0.6 V supply voltage. The first pipeline stage computes the bitwise XOR operation between each State and Key byte (AddRoundKey function). The resulting byte enters the S-Box module depicted in Fig. 5 (SubBytes implementation). S-Box is a function based on inversion in the $GF(2^8)$ field, followed by an affine transformation [4]. Glue-logic implementation of S-Box [16] has been preferred to LUT [12] and BDD [13] approaches. Circuitry complexity reduction has been achieved by mapping $GF(2^8)$ inversion into composite field $GF(2^4)$ operations [10]. XOR gate count has been reduced by field mapping function with S-Box affine transformations. Latch-based clock-gating (L blocks in Fig. 5) has been exploited to reduce dynamic power during pipeline inactivity. Finally, ShiftRows function (i.e. cyclic shift of i bytes in the i-th State row) is managed by properly choosing the storing address of each modified State byte.

4.2. MixColumns Implementation

The MixColumns and InvMixColumns transformations operate on the State column-by-column, treating each column as a four-term polynomial over $GF(2^8)$. During MixColumns operations and inverse transformation, the columns are multiplied modulo $(x^4 + 1)$ with two fixed polynomials $a(x)$ and $a^{-1}(x)$. Eq. (10, 11) reports the MixColumns and inverse transformation polynomials: equations include common terms (enclosed in brackets)

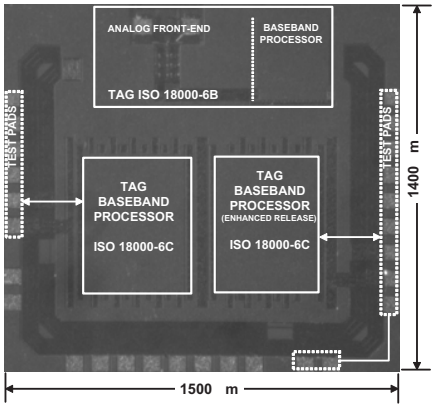

Figure 7. Microphotograph of test chip die.

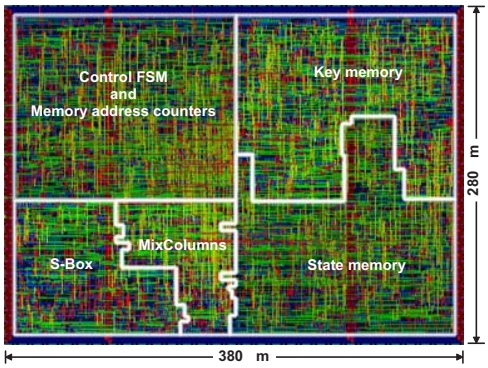

Figure 8. Layout of AES cipher engine.

which can be exploited to reduce hardware complexity.

$$\begin{aligned} a(x) &= \{03\}\,x^3 + \{01\}\,x^2 + \{01\}\,x + \{02\} = \\ &= \{02\}\,(x^3+1) + \{01\}\,(x^3+x) + \{01\}\,x^2 \end{aligned} \quad (10)$$

$$\begin{aligned} a^{-1}(x) &= \{0b\}\,x^3 + \{0d\}\,x^2 + \{09\}\,x + \{0e\} = \\ &= \{08\}\,x^3 + \{0c\}\,x^2 + \{08\}\,x + \{0c\} + a(x) = \\ &= \{04\}\,(\{02\}\,((x^3+x) + (x^2+1)) + \\ &\quad + (x^2+1)) + a(x) \end{aligned} \quad (11)$$

Following the above equations, Fig. 6 depicts the proposed combined MixColumns and InvMixColumns architecture. Such a circuitry calculates one fourth of the transformation in a clock cycle. Each byte of column operations can be computed by changing the order of the inputs. Four clock periods are required to load each State column into the shift register S0-S4, whereas inputs reordering calls for a three clock cycle operation. The reduction of MixColumns and inverse-transformation equations lead to an efficient datapath implementation where only XOR gates, and constant multiplications are required. To control power consump-

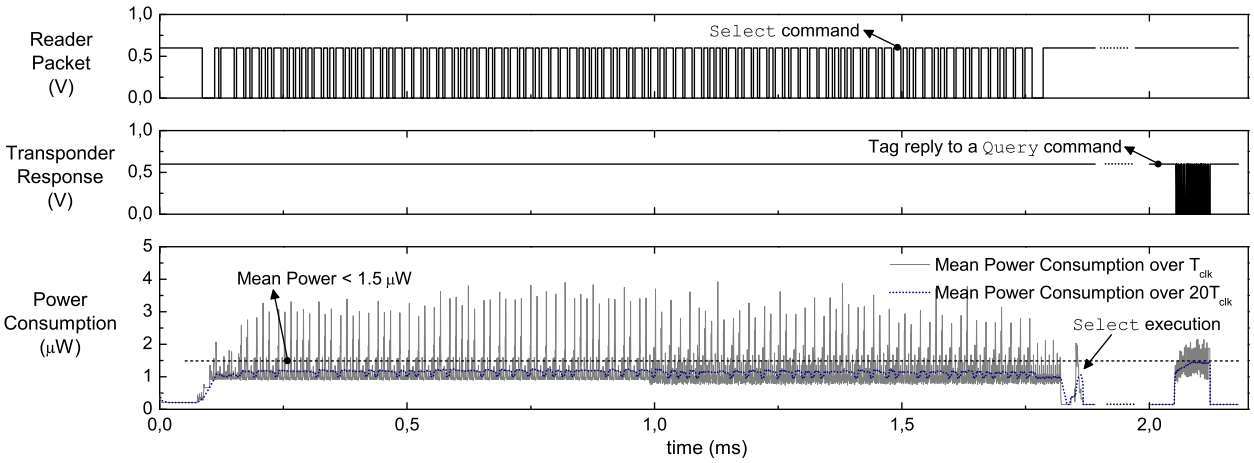

Figure 9. ISO-18000 6C baseband-processor power consumption versus time

tion, in addition to clock gating, output data ports are inhibited during `MixColumns` operations by G1 to G3 AND gates.

5. Results

The RFID baseband processor and AES engine have been described in VHDL language and synthesized with Synopsys Design Compiler , exploiting the compact standard-cell library characterized at 0.6 V and fully integrated within the standard industrial design-flow (based on Synopsys/Cadence tools). Layout operations have been performed exploiting Cadence Encounter. The overall area of ISO 18000-6C baseband processor is $380\,\mu\text{m} \times 540\,\mu\text{m}$ (Fig. 7), whereas the AES engine, depicted in Fig. 8, requires $380\,\mu\text{m} \times 280\,\mu\text{m}$ (i.e. about 6000 EG). Half of the AES silicon area is required by Key and State memory implementation.

Several simulations have been carried out, accounting for actual interrogator packets, in order to evaluate circuitry switching activity. Synopsys PrimeTime has been exploited for estimating the power consumption. Fig. 9 illustrates the power required by the tag baseband processor, while executing some typical commands. First, decode and execution of a "Select" command is shown, then the tag reply to a "Query" command is illustrated. Power plot shows the actual power, averaged over a single clock period and over a 20-clock cycles long moving window. Transponder baseband communication circuitry reaches its maximum mean power consumption of 1.5 μW during transponder reply, due to the high frequency of response (up to 640 KHz). Less power is required during reception and execution periods (1.2 μW and 1 μW, respectively). In particular, during reception operations, 50% of the actual power is required by the PIE decoder, due to its relatively high operating frequency. Baseband processor peak power (over a clock period) always remains below a maximum of 4 μW, which occurs during PIE decoding operations.

AES encoding and decoding average power consumption is equal to 2.0 μW, included State and Key memories (which accounts for 40 % of AES dissipation). Fig. 10 depicts AES cipher power consumption, while encoding a 128-bit plaintext. The ten AES rounds belonging to main loop (which can be identified by looking at `S-Box` and `MixColumns` control signals) clearly influence the power consumption behavior: maximum mean power consumption over a couple of clock periods is equal to 4 μW, and occurs when `MixColumns` function and `KeyExpansion` routine are executed at the same time. Power dissipation eventually decreases during the serial state data extraction. Moving-window average, instead, always remains below 2 μW. Finally, it is worth observing that most demanding task for the protocol processor and the AES engine typically take place during partially disjoined time intervals, so that the total dissipation of digital circuitry always remains below 2.5 μW.

Obtained results well compare with literature: ony a few articles reports with EPC Gen2 digital core implementations [11, 14, 15]. Lowest power dissipation figures reported there are in the order of some μW, significantly higher than the implementation described above. With respect to state-of-the-art low-cost implementations [16], the proposed AES implementation exhibits a slightly larger gate-count, due to the pipelined architecture. Such a feature, on the other hand, makes near-threshold operations possible, allowing for extremely low power dissipation.

A preliminary implementation of ISO 18000-6C baseband processor has been fabricated (Fig. 7). Testing is actual under way. Testing of a previous version of the chip have al-

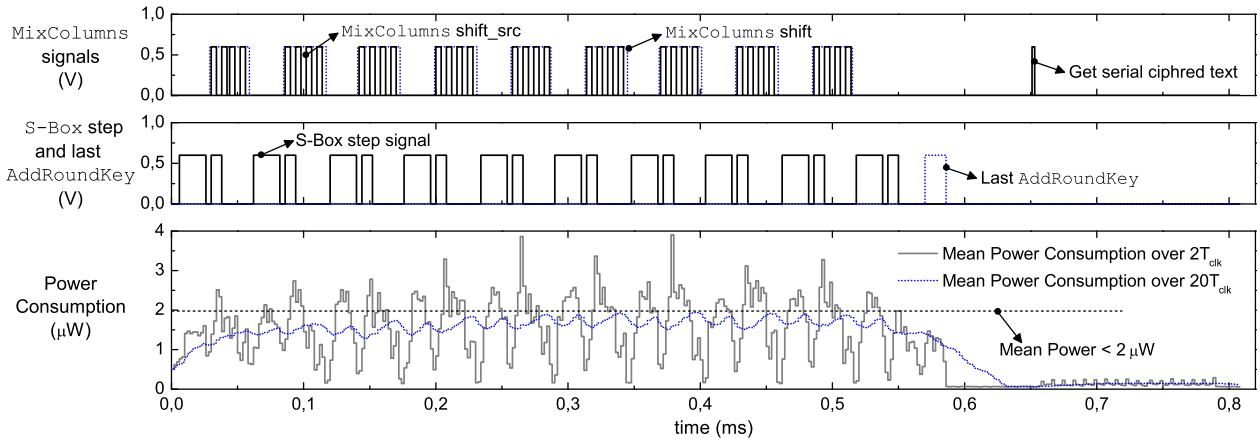

Figure 10. AES power consumption versus time

ready validated the simulation accuracy, both in terms of timing performance and power dissipation.

6. Conclusions

In this paper, the design of a complete baseband-processor for RFID UHF passive tag has been introduced. Cryptographic primitives has been added to basic transmission and arbitration circuitry to enhance communication channel security. High performance has been guaranteed by means of extreme supply voltage scaling and low-power design strategies, both at the circuit and system levels. Simulation results yield a total power dissipation below 2.5 μW (including both communication processor and AES cryptographic engine) which favorably compare with literature data.

References

[1] K. Finkenzeller. *RFID Handbook, Radio-Frequency Identifications Fundamentals and Applications. 2nd ed.* Wiley, New York, 2003.

[2] A. Juels. Rfid security and privacy: A research survey. *IEEE Journal on Selected Areas in Communication*, 24(2):381–394, February 2006.

[3] EPC Global. *EPC Radio-Frequency Identity Protocols Class1 Generation2 UHF, RFID Protocol for Communications at 860 MHz-960 MHz, Version 1.0.9*, January 2005.

[4] National Institute of Standards and Technology (NIST). *NIST: FIPS-197: Advanced Encription Standard. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf*, November 2001.

[5] J. M. Rabaey. Scaling the power wall. In *University Reception, Design Automation Conference*, June 2007.

[6] H.T. Friis. A note on simple transmission formula. *Proceedings of the Institute of Radio Engineers*, 34:254–256, May 1946.

[7] J. Masgonty, S. Cserveny, C. Arm, P. Pfister, and C. Piguet. Low-power low-voltage standard cell libraries with a limited number of cells. In *Proceedings of International Workshop - Power and Timing Modeling, Optimization and Simulation (PATMOS)*, September 2001.

[8] A. Ricci, I. D. Munari, and P. Ciapolini. An evolutionary approach for standard-cell library reduction. In *Proceedings of the Grate Lake Synposium on VLSI*, March 2007.

[9] M. Kim, J. Ryou, Y. Choi, and S. Jun. Low-cost cryptographic circuits for authentication in radio frequency identification systems. In *Proceedings of the IEEE International Symposium on Consumer Electronics*, pages 1–5, 2006.

[10] J. Wolkerstorfer, E. Oswald, and M. Lamberger. An asic implementation of the aes s-boxes. *CT-RSA 2002, Springer Lecture Notes in Computer Science*, 2271:67–78, 2002.

[11] A. Mann et al. Low Power VLSI Design for a RFID Passive Tag Baseband System Enhanced with an AES Cryptography Engine. In *Proceedings of the 1st Annual RFID Eurasia* , pages 1–6, September 2007.

[12] H. Qui, T. Sasao, and Y. Iguchi. A design of aes encryption circuit with 128-bit keys using look-up table ring on fpga. *IEICE Transaction on Information and Systems*, E89(3):1139–1147, March 2006.

[13] S. Morioka and A. Satoh. A 10-gbps full-aes crypto design with a twisted bdd s-box architecture. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 12(7):686–691, July 2004.

[14] H. Yan, H. Jianjun, L. Qiang, and M. Hao. Design of low-power baseband-processor for rfid tag. In *Proceedings of the International Symposium on Applications and the Internet Workshop*, pages 1585–1588, May 2006.

[15] A. Mann et al. Design and implementation of a low-power baseband-system for rfid tag. In *Proceedings of the IEEE International Symposium on Circuit and Systems*, pages 1585–1588, May 2006.

[16] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen. Aes implementation on a grain of sand. *IEE Proceedings on Information Security*, pages 13–20, June 2005.