SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2014; **7**:365–375
Published online 9 May 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.723

SPECIAL ISSUE PAPER

A low-cost UHF RFID tag chip with AES cryptography engine

Lingzhi Fu, Xiang Shen, Linghao Zhu and Junyu Wang*

State Key Lab of ASIC and System, Fudan University, Shanghai, China

ABSTRACT

In this paper, the design of a low-cost ultra-high-frequency (UHF) Radio Frequency IDentification (RFID) tag chip with an advanced encryption standard (AES) cryptographic engine is presented. The design of digital baseband is verified on a Field-Programmable Gate Array (FPGA) platform. The whole chip, including a radio frequency frontend, an analog frontend, an Electrically Erasable Programmable Read-Only Memory (EEPROM), and a baseband with AES engine, is taped out on Semiconductor Manufacturing International Corporation (SMIC) 0.13μm process. The chip area is 1 × 1 mm2, in which 0.6 × 0.3 mm2 is covered by the digital baseband. The power consumption of the entire tag chip is 20.9 μW. The design can work on both two modes of the standard ISO 18000-6C mode and the security enhanced ISO 18000-6C mode. To the best of our knowledge, it is the first UHF passive RFID tag chip with AES algorithm in the baseband.

KEYWORDS
AES; low-cost, low-power; security and privacy; RFID; chip design

***Correspondence**
Junyu Wang, State Key Lab of ASIC and System, Fudan University, Shanghai, China.
E-mail: junyuwang@fudan.edu.cn

1. INTRODUCTION

As Radio Frequency IDentification (RFID) technology is widely used for micro-payment and item level tagging of supply chain management and asset management, RFID systems are suffered from many secure threats and attacks, especially for the RFID tags or related database containing private information which might be accessed illegally. Thus, the security and privacy issue of RFID requires much attention.

In 2007, Nohl in Virginia University proposed the physical analysis of Crypto-1 [23]. Garcia and Jacobs researched the Mifare technology, which is an HF RFID technology and accomplished the clone attack on an ov-chipkaart card [24]. Based on the study, Nocolas and Karsten attacked on the Oyster Cards in London public transportation system [25]. In 2008, Anderson in MIT conducted exhaustive attack on subway card in Boston (Charlie Card), which draws the attention on the security issue on public transportation [26].RFID attack methods include spoofing, inserting, eavesdropping, replay attacking, counterfeiting, unauthorized access, tampering, denial of service, physical attacking, and tracing [27]. To solve the security and privacy issues, many researches focus on the authenticating protocol. Recently, security protocols based on cryptographic algorithms attract more attention. One-way hash function, symmetric key algorithm, and public key algorithm are the 3 kinds of cryptographic algorithms used in RFID systems. For the low cost tag chip design, one-way hash function and symmetric key algorithm are used more frequently than the public key algorithm.

Literature [1] proposed the concept of “hash-lock” first. In the framework, only the value of hash is stored in a tag, and the key is stored in a background service. By temporary tag index meta-ID, the key can be attained. By sending the hash value of a key, users can lock the tag. In literature [2], the authors extend the hash-lock scheme with random index, and the “random-hash-lock” protocol improves the security significantly. RFID security protocols with hash algorithms are introduced in literatures [3] and [4].

Advance Encryption Standard (AES) algorithm is one of the most popular symmetric cryptographic algorithms. The overlapping authentication protocol with AES algorithms is first proposed in [11], to enhance the security of EPC system. In [5], a reader–tag authentication protocol based on AES is proposed to prevent cloning and replay attack. A gradual password transformation authenticating protocol further improve the safety of AES ([12]).In UHF RFID systems, EPC Class1 Generation2 (C1G2) standard or ISO 18000-6C, the security issues are more serious with the burst of applications in retail, healthcare, anti-counterfeiting, where the data attached with RFID tags are sensitive. Thus it requires security-enhanced communication in the MAC level, and encryption engines in the tag chips.

In this work, a low-cost UHF RFID tag chip conforming to ISO 18000-6C with an AES cryptographic engine is designed and taped out. It can work on standard mode and security enhance mode. The digital baseband is verified in FPGA and the chip design is simulated with power consumption, speed, and area. The chip is taped out and measured in real scenario, and the result shows that the security scheme and chip in this paper work well.To the best of our knowledge, it is the first UHF passive RFID tag chip with AES algorithm in the baseband.

The rest of the paper is organized as follow: Section 2 reviews the related work; Section 3 introduces the AES cryptographic algorithm; Section 4 explains the hardware design of the AES engine and the digital baseband in this paper, Section 5 shows the simulation and testing results of the design, and Section 6 concludes the paper.

2. RELATED WORK

2.1. Cryptographic Algorithms in RFID Systems

Symmetric key algorithms include Data Encryption Standard (DES), Tiny Encryption Algorithm (TEA), International Data Encryption Algorithm (IDEA), AES, etc. The symmetric key algorithms have simplified structures and are widely used in RFID security protocols. In the application of RFID system, the problem of key management and distribution still need to be solved.

Public key algorithms are safer, but require large amount of computation, making it hard to be used for low-cost RFID. As the development of RFID and low power circuit technology, public key algorithms become acceptable for RFID system. In [5] and [6], RFID authentication based on Elliptic curve cryptography is proposed. In [7], RFID security protocol based on RSA e-signature is applied in e-ticket.

UHF RFID tags are the most widely used ones because of low cost and low power. Electronic Product Code (EPC) global C1G2 protocol regulates the air-interface of the communication between the readers and tags, which is globally accepted nowadays. For the low cost applications, complicated cryptographic algorithms such as the public key algorithms are not applicable in the tag chip design.

Light weight security protocols and algorithms are researched for the purpose of low cost and high security. To reduce the complexity of computation, the computing resources in protocols are adopted and extended. In [8] and [9], the communication between the readers and tags are verified with the Cyclic Redundancy Check (CRC) function. The Canadian company Revere Security proposed Hummingbird algorithm in 2009, which is a special cryptographic algorithm suitable for RFID security [10].

2.2. AES in RFID Systems

AES cryptographic engine has been applied in some RFID systems. In [28], the authors proposed an RFID mutual authentication protocol based on AES algorithm, and researched on the real system of conveyor belt. In [29], the authors designed a digital baseband with AES cryptography engine, and the power consumption is optimized. In [30], an RFID Baseband Processor is designed and it can operate sensors. But to the best of our knowledge, there is no report of a design of a whole tag chip with an AES engine in the baseband.

Power consumption and cost are 2 major factors that influence the application of RFID systems. The cost of chip is mainly decided by the area of the design. Thus, in designing the baseband of passive tags, power consumption, area, and timing constraint need to the considered comprehensively, and low-cost is still of great significance.

The design of passive RFID tags with AES engine is also challenging. The architecture of digital baseband, analog frontend and RF frontend need to be optimized globally. To the best of our knowledge, none of the previous work paid much attention on this issue.

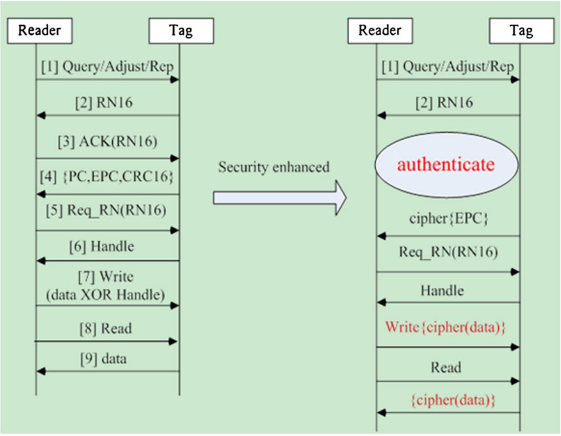


Figure 1. ISO 18000-6C communication process with authentication.

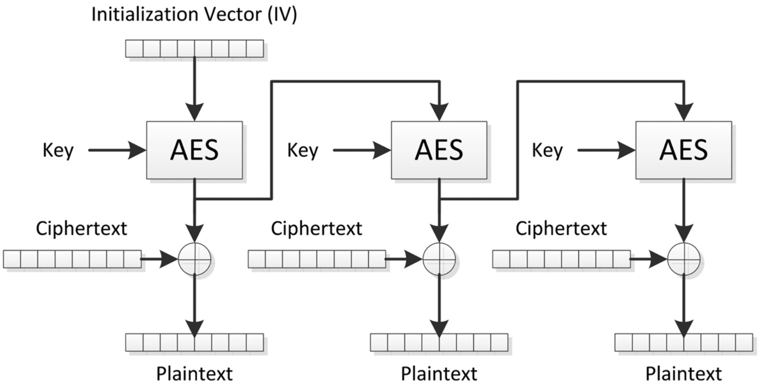


Figure 2. Output feedback mode.

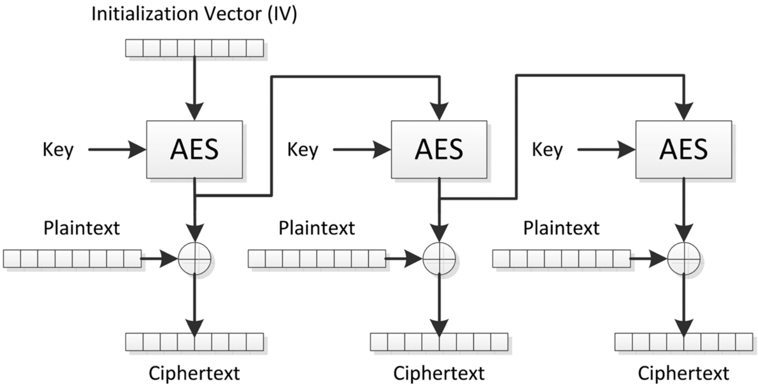


Figure 3. Round functions in AES.

3. AES CRYPTOGRAPHIC ALGORITHM

3.1. Proposed authenticating protocol for ISO 18000-6C

In the basic communication process in ISO 18000-6C, the reader sends Query/Adjust/Rep, the tag replies a 16-bit random number RN16, the reader sends ACK with the certain RN16, the tag replies PC and EPC if the ACK is verified, and the reader starts further manipulating the tag.

In security mode, the process of communication is modified as Figure 1. After the tag sends the RN16, an authenticating process is required before the tag sends EPC to the reader. The EPC and other data are also transmitted in ciphertext.

3.2. Encryption and decryption process of AES

Advance Encryption Standard is a block cryptographic algorithm, and the length of the message is fixed. The AES in this work adopts Output Feedback mode, which is shown in Figure 2.

In AES-128, a 128-bit block is encrypted in one AES engine. In the first block, an AES engine is used to generate a 128-bit output from key and initialization vector. The output is used in the next AES engine together with key to generate the output. The plaintext is segmented into several 128-bit plaintexts and ciphered with the output of each AES engine.

The decryption process is similar to the encryption, and the cipher text is processed with the outputs of AES engines to generate plaintext (Figure 3). The initialization vector of encryption and decryption must be the same.

3.3. Round functions in AES algorithm

For 128-bit AES, the 16-byte data are put in a $4*4$ byte array (called state). The array is processed for 10 rounds, and each round consists of four functions: SubBytes, ShiftRows, MixColumns, and AddRoundKey (Figure 3).

SubBytes (also called S-box) is applied on each byte of the state matrix. The S-box is a nonlinear transition with great complexity and little relationship between the input and the output. In the S-box of AES, the byte is inverted on GF(2^8) and affine-transformed with Equation (1). In decryption mode, the affine transformation equation is Equation (2).

$$\begin{bmatrix} b7 \\ b6 \\ b5 \\ b4 \\ b3 \\ b2 \\ b1 \\ b0 \end{bmatrix} = \begin{bmatrix} 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \\ 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&1&0&0&1 \end{bmatrix} \times \begin{bmatrix} a7 \\ a6 \\ a5 \\ a4 \\ a3 \\ a2 \\ a1 \\ a0 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \tag{1}$$

$$\begin{bmatrix} b7 \\ b6 \\ b5 \\ b4 \\ b3 \\ b2 \\ b1 \\ b0 \end{bmatrix} = \begin{bmatrix} 0&1&0&1&0&0&1&0 \\ 0&0&1&0&1&0&0&1 \\ 1&0&0&1&0&1&0&0 \\ 0&1&0&0&1&0&1&0 \\ 0&0&1&0&0&1&0&1 \\ 1&0&0&1&0&0&1&0 \\ 0&1&0&0&1&0&0&1 \\ 1&0&1&0&0&1&0&0 \end{bmatrix} \times \begin{bmatrix} a7 \\ a6 \\ a5 \\ a4 \\ a3 \\ a2 \\ a1 \\ a0 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \tag{2}$$

ShiftRows is a byte-shifting operation to one of the row in the matrix. In the AES-128, the first row is not changed, the bytes in the second row shift to the left for one step, the third row shift for two steps, and the last row shift for three steps. After the ShiftRows, each column consists of elements of different columns.

MixColumns works on the 4 bytes of a column. The 4 bytes of a column are taken as the coefficients of 1, x, x^2, and x^3, to form a polynomial on GF(2^8). The product of the polynomial and $c(x)$ is modulated by $x^4 + 1$. $c(x)$ is shown in Equation (3). The result is co-primed by $c(x)$. The operation can also be considered as the production operation on finite field, as Equation (4). In decryption, c (x) is replaced with $d(x)$ in Equation (5), and the matrix production is in Equation (6). In MixColumns, every input byte has influence on the output bytes; thus, ShiftRows and MixColumns provide extension for the cryptosystem.

$$\mathrm{c}(\mathrm{x}) = 03 \times \mathrm{x}^3 + 01 \times x^2 + 02 \tag{3}$$

$$\begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix} = \begin{bmatrix} 02&03&01&01 \\ 01&02&03&01 \\ 01&01&02&03 \\ 03&01&01&02 \end{bmatrix} \times \begin{bmatrix} a0 \\ a1 \\ a2 \\ a3 \end{bmatrix} \tag{4}$$

$$d(x) = 0B \times x^3 + 0D \times x^2 + 0E \tag{5}$$

$$\begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix} = \begin{bmatrix} 0E&0B&0D&09 \\ 09&0E&0B&0D \\ 0D&09&0E&0B \\ 0B&0D&09&0E \end{bmatrix} \times \begin{bmatrix} a0 \\ a1 \\ a2 \\ a3 \end{bmatrix} \tag{6}$$

In the AddRoundKey, the 128-bit key and the state matrix are processed with exclusive-or (XOR) operation by bytes.

The four functions form one round of the operation, and the number of rounds in one AES engine depends on the length of the key. For 128-bit, 192-bit, and 256-bit keys, the numbers of rounds are 10, 12, and 14. The first round only contains AddRoundKey, and the last round consists of SubBytes, ShiftRows, and AddRoundKey.

4. HARDWARE IMPLEMENTATION OF TAG CHIP WITH AES ALGORITHM

4.1. System Architecture of Tag Chip

The passive RFID tag chip consists of digital baseband (including memory), RF/analog frontend, and PADs. Figure 4 shows the system architecture.The digital baseband conducts the process of protocol, encryption, memory control, and the modulation and demodulation in digital field.

The RF/analog frontend converts the digital signal into analog signal, and modulates them with carrier and sub-carrier, when sending data. In receiving data, the RF/analog frontend receives RF signal, demodulates it into low frequency signal, and converts it into digital signal for digital baseband.

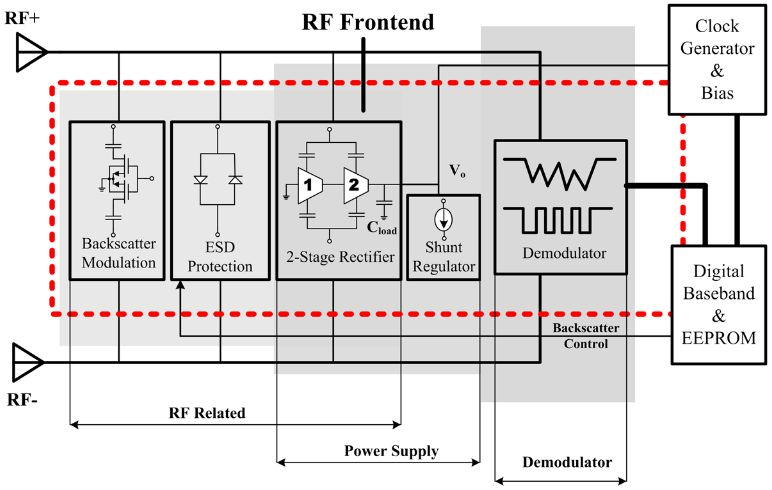


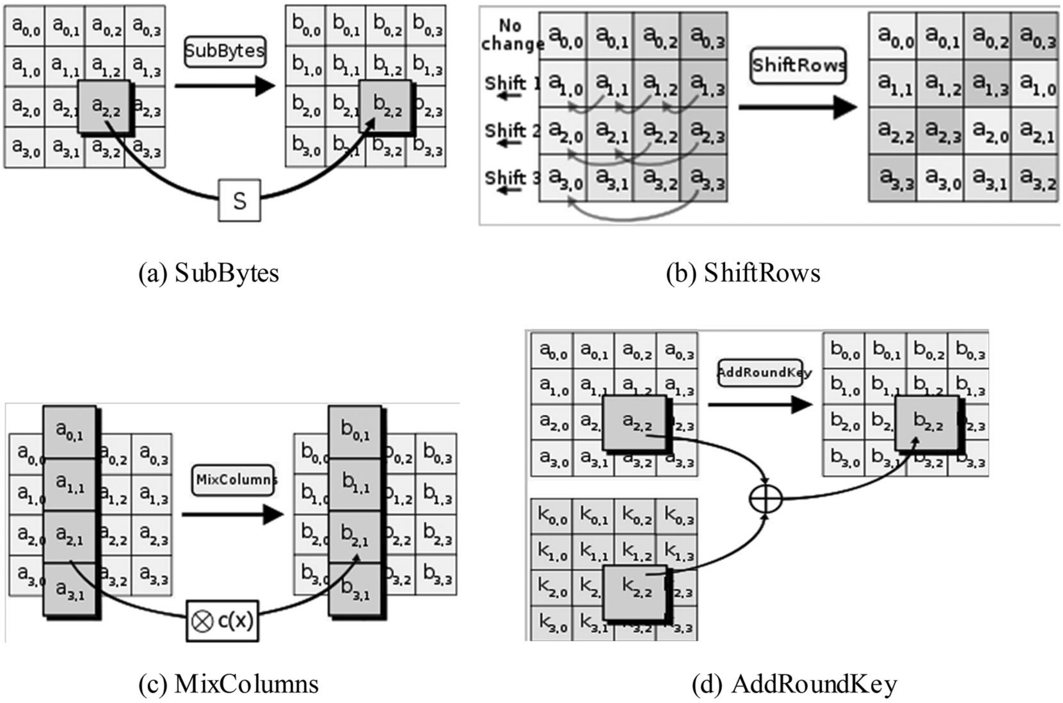
Figure 4. System Architecture of passive RFID tag chip.

The RF/analog frontend consists of RF related circuit, power supply, and demodulator.

The RF related circuit has great influence on the performance, including input impedence, Q factor, and parallel parameters. The module consists of backscattering circuit, ESD protect, rectifier, envelope extractor. All the modules are coupled to RF frontend. Power supply module converts high frequency energy into DC energy. It consists of rectifier and power regulator. The demodulator fulfills the power detection and demodulation. It consists of envelope extractor, active load, low-pass filter, and hysteresis comparator. The major challenge is to optimize power consumption and area according to sensitivity.

4.2. Structure of digital baseband

The structure of digital baseband of a tag is shown in Figure 5. The input of digital baseband is PIE code



(a) SubBytes

(b) ShiftRows

(c) MixColumns

(d) AddRoundKey

Figure 5. Structure of digital baseband.

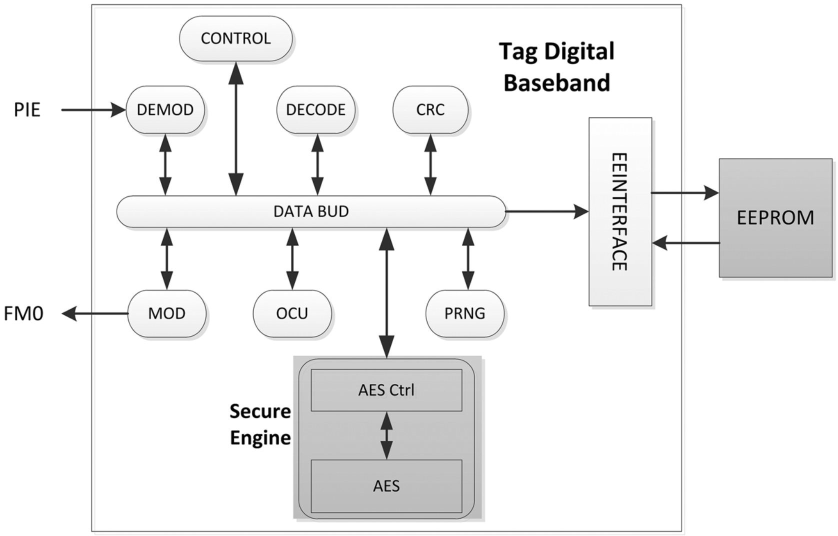


Figure 6. Inversion operation on $GF(2^4)^2$.

from the analog front end. The PIE is demoded by DEMOD module and processed to get the command and parameters from the reader. The CONTROL module conducts the related action according to the command, such as accessing register, updating random number, sending EPC, and security authentication. Cyclic redundancy check and PRGN modules work together with CONTROL to fulfill the process. The message to the reader is modemed by MOD into FM0 or Miller code, and sent to the analog front end.

The data inside the digital baseband is transmitted in DATA BUS and stored in EEPROM storage with EEINTERFACE.

An AES-secure engine is designed for security-related data processing, which will be introduced in detail later.

4.3. Implementation of AES engine

The SubBytes function or S-box is the most difficult part. In this work, the S-box is implemented by turning operation on GF(2^8) to GF(2^4)^2, and the hardware cost is reduced.

In S-box replacing, the 8 bit of a byte can be considered as the coefficient of polynomial on GF(2^8). The conversion from GF(2^8) to GF(2^4) is to turn the coefficient of an eight-times polynomial $a_{0\sim8}$ to that of two quartic polynomials $ah_{0\sim3}$ and $al_{0\sim3}$. The conversion equation and the reverse equation are Equations (7) and (8).

$$\begin{bmatrix} ah3 \\ ah2 \\ ah1 \\ ah0 \\ al3 \\ al2 \\ al1 \\ al0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} a7 \\ a6 \\ a5 \\ a4 \\ a3 \\ a2 \\ a1 \\ a0 \end{bmatrix} \tag{7}$$

$$\begin{bmatrix} a7 \\ a6 \\ a5 \\ a4 \\ a3 \\ a2 \\ a1 \\ a0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} ah3 \\ ah2 \\ ah1 \\ ah0 \\ al3 \\ al2 \\ al1 \\ al0 \end{bmatrix} \tag{8}$$

After the conversion, inversion operation is conducted on GF(2^4)^2, as shown in Figure 6.

$$\begin{cases} q3 = a1 \oplus a2 \oplus a3 \oplus a1a2a3 \oplus a0a3 \oplus a1a3 \oplus a2a3 \\ q2 = a0a1 \oplus a2 \oplus a0a2 \oplus a3 \oplus a0a3 \oplus a0a2a3 \\ q1 = a0a1 \oplus a0a2 \oplus a1a2 \oplus a3 \oplus a1a3 \oplus a0a1a3 \\ q0 = a1 \oplus a2 \oplus a3 \oplus a1a2a3 \oplus a0 \oplus a0a2 \oplus a1a2 \oplus a0a1a2 \end{cases} \tag{9}$$

The result of inversion ah_1 and al_1 is converted to GF(2^8), and the inversion of GF(2^8) is achieved. With affine transformation in Equation (1), the result of S-box is fulfilled. In hardware implementation, the finite transformation matrix A and affine transformation matrix T can be combined to save area. Similar combination can be applied on the decryption process. The GF(2^4)^2 module can be reused. The hardware structure of S-box is shown in Figure 7(a).

MixColumns operation is 4-bit fixed-coefficient finite-field multiplication. The coefficients of encryption and decryption are shown in Equations (4) and (5), and the variation of the coefficients is too large and requires a large hardware cost. If the $d(x)$ is subtracted by $c(x)$ as in (10), only two additional coefficients 08 and 0C are needed to fulfill the encryption and decryption to save area.

$$d(x) - c(x) = \{08\}x3 + \{0C\}x2 + \{0C\}x \tag{10}$$

In SubBytes operation, the data are processed by bit, and the MixColumns requires 4 bits, so the latter block has to wait for four clock cycles to get the data. In [13], a serial input parallel output MixColumns hardware structure is proposed to promote the efficiency. The

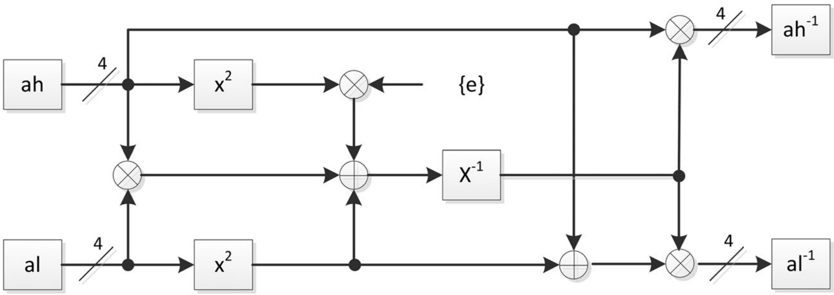


Figure 7. Hardware structure.

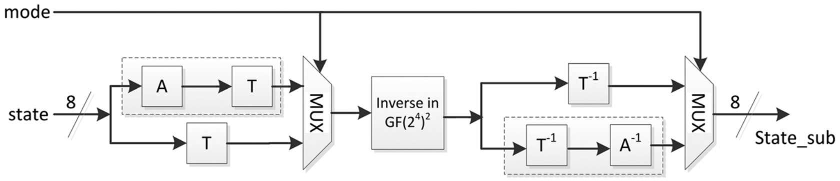


Figure 8. Module structure of AES core.

structure in this paper is shown in Figure 7(b). After the S-box, d_in is a 1-bit input, decry is a mode selection signal, in which high level indicates decryption mode, and D0 ~ D3 are four 8-bit D flip-flops. On the positive edge of each clock, d_in is updated, and after four clock cycles, the result is outputted in d3_out ~ d0_out.

The encryption and decryption of AES are different, and an additional InvMixColumns module is required, which increase the hardware cost.

Because the SubBytes and ShiftRows are based on byte, the order of operation does not influence the result [14]. With this conclusion, a different key length solution is proposed.

In encryption process, the key extension module outputs a 32-bit Key_en, and it is in the XOR operation with the output of MixColumns. In a clock cycle, the operation width of AddRoundKey is 32 bits.

In decryption process, the key extension module outputs an 8-bit Key_de, and it is in the XOR operation with the output of S-box. The operation width of a clock cycle is 8 bits.

The number of S-box is a trade-off among area, power consumption and speed. The AES state contains 16 bits, and the round key extension requires the replacement of 4 bits, so 20 bits are required to be processed in S-box in one round. One S-box can process 1 bit, so more S-boxes will increase the parallelism and speed, but takes more cost. In passive RFID tag, only one S-box is applied in the circuit to reduce cost.

The module structure of AES core is shown in Figure 8, and the data path is shown in Figure 9.

4.4. Implementation result

The design is synthesized with Design Complier with SMIC 0.13-μm EEPROM process. The circuit area of AES module is 27403.3 μm^2. A two input NAND gate covers 5.53 μm^2, so the area of the circuit equals 4952 gates.

By synthesizing each submodule separately, the area and percentage of the area of each submodule can be counted, as shown in Table I. It can be seen that the Key-expansion module and State_schedule module takes 3/4 of the total area in the circuit.

The power consumption of the circuit is analyzed by NanoSim. The power consumption varies significantly with different voltage and clock frequency. The circuit can work at the voltage of no lower than 0.6 V. The

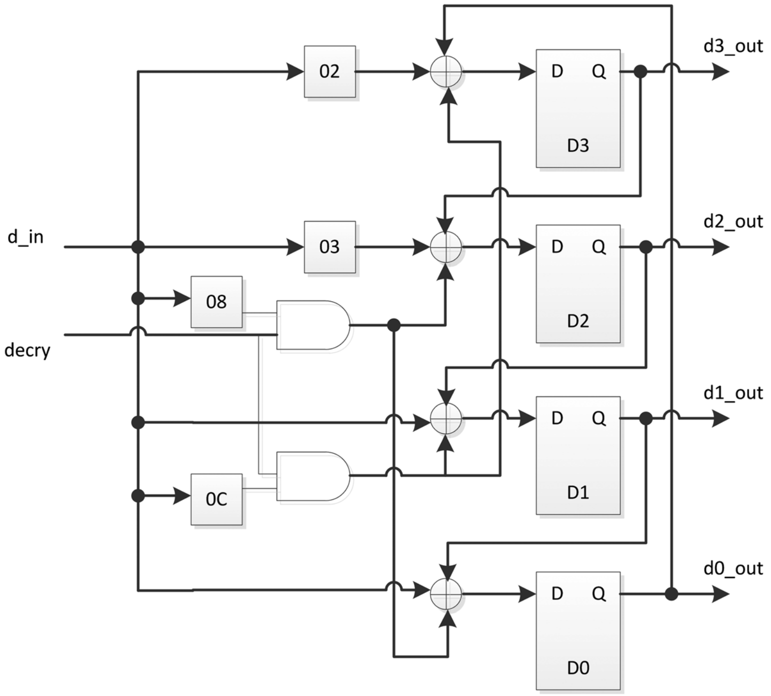


Figure 9. Data path of AES engine.

Table I. Circuit area of AES.

Module name	Gates	Percentage (%)
Controller	142	2.9
S-Box	391	7.9
Mixcolumns	647	13.0
Keyexpansion	1756	35.5
State_schedule	2017	40.7
Total	4952	100.0

Table II. Power consumption with different supply voltage at 100-kHz clock frequency.

Voltage (V)	Currency (μA)	Power (μW)
1.8	2.25	4.05
1.2	1.26	1.51
1.0	1.01	1.01
0.8	0.81	0.65
0.6	0.56	0.34

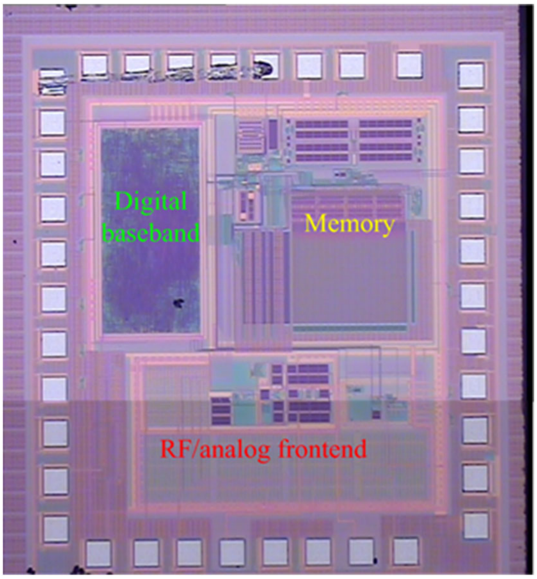


Figure 10. Photo of the SoC tag chip.

power consumption with voltage from 0.6 to 1.8 V under 100-KHz clock frequency is listed in Table II. The power consumption almost increase linearly as the clock frequency increase.

Figure 10 shows the photo of the entire SoC tag chip.

5. SIMULATION AND VERIFICATION RESULTS

5.1. Logic verification of digital baseband with Modelsim

A verification platform is established to verify the function of digital baseband in RTL level, and the structure is shown in Figure 11. The entire platform runs in Modelsim.

In the platform, the reader is modeled in behavior level, and it conducts the functions according to ISO 18000-6C protocol (Test Vector Generator in Figure 11), such as sending commands, processing data replied from the tag, and authenticating the tag.

A reference AES model is established with C and the result of C-model and our design is compared. If the output of the design agrees with that of C-model, the test case is judged as PASS.

The simulation results show that the design in this paper works appropriately under standard mode and security mode.

5.2. Power simulation

The design of digital baseband is synthesized by Design Complier and the power consumption of the digital baseband is analyzed with NanoSim. NanoSim can conduct power analyzing for large-scale circuits at the accuracy of transistor level and high speed.

The supply voltage is 1.2 V, and the average currency during the simulation is 11.4 μA. Thus, the average power consumption is 13.68 μW, which is acceptable for RFID security tag.

5.3. Real-scenario measurement

The design of the secure tag is measured in real communication between the reader and the tag. The entire platform

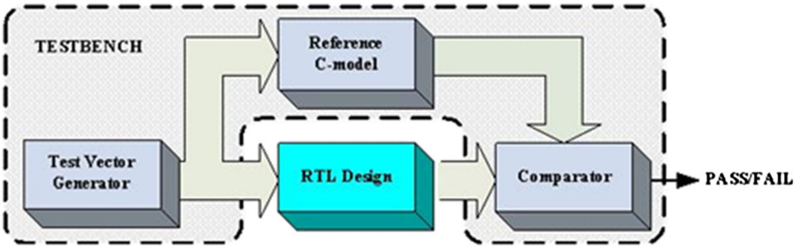


Figure 11. Structure of verification platform.

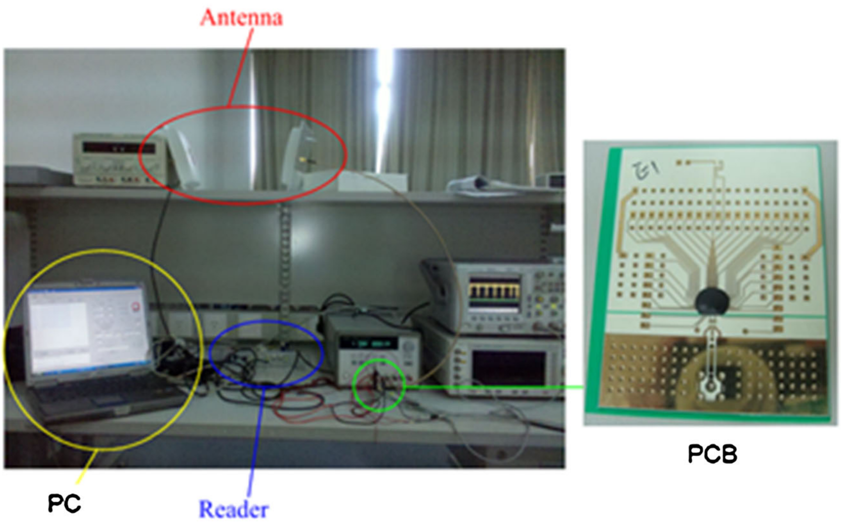
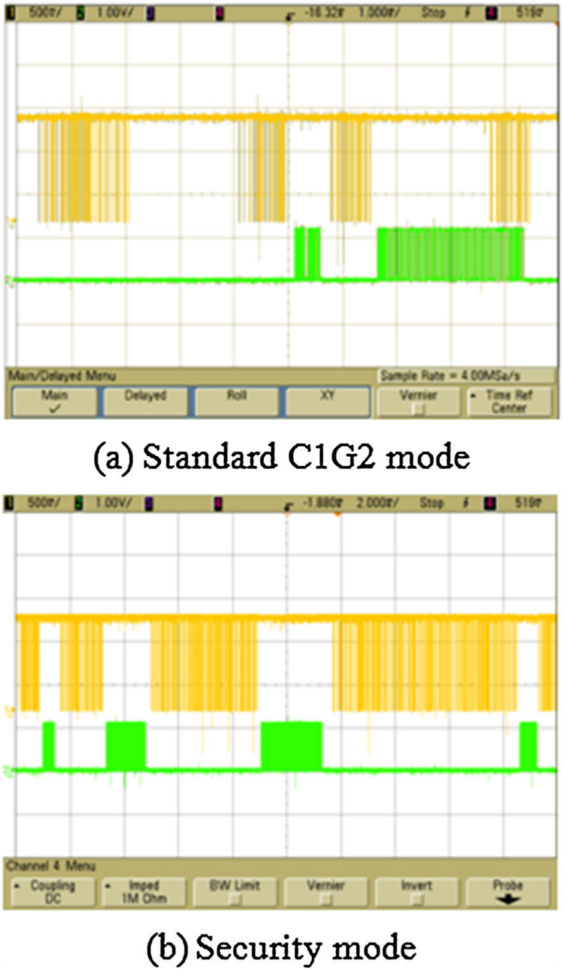


Figure 12. Measurement platform.

consists of a printed circuit board with the tag chip, a commercial ISO 18000-6C reader by Quanray, antennas for the reader and the tag, a PC, and related equipment. The platform is shown in Figure 12.

Figure 13(a) and (b) shows the signal waves between the reader and the tag. The aforementioned is the PIE sent by the reader, including Select, Query, and ACK.



(a) Standard C1G2 mode

(b) Security mode

Figure 13. Waves of security mode in measurement.

5.4. Comparison

The result of this work is compared with that of other AES circuit in references. Table III shows the comparison of baseband design with AES, and Table IV shows the results of ASIC AES design results in the references.

The result shows that the design of AES engine in this work has the lowest power consumption, and the power consumption of the entire digital baseband is competitive.

6. CONCLUSION

In this paper, an authenticating protocol for ISO 18000-6C is proposed. The architecture of AES cryptographic engine is studied and the engine is implemented in the baseband of a tag chip. The design of AES engine can achieve the required operation with low cost. A digital baseband with the AES engine is implemented in hardware and measured in real scenario. The whole tag chip with RF and analog frontend is taped out on SMIC 0.13μm EEPROM process. The results show that the design can work on both the standard ISO 18000-6C mode and the security enhanced ISO 18000-6C mode.The design of this work is competitive in the application of passive RFID security tags with low cost and low power.

Table III. Result of tag baseband designs containing AES alogorithm.

	Chip/Syn	Tech (μm)	Chip Area (mm^2)	Clock frequency	Volts (V)	Power consumed (μw)
A. Ricci [15]	Syn	0.18	0.205	2 MHz	0.6	3.600
Qi.YZ [16]	Syn	0.18	0.247	N/A	1.0	6.900
Xiao.x [17]	Chip	0.18	0.700	N/A	0.9	15.000
Jong.w [18]	Chip	0.18	1.100	N/A	1.8	360.000
Adam [19]	Syn	0.18	0.446	3.55 MHz	1.8	4.695
This work	Chip	0.18	0.149	1.28 MHz	1.2	13.680

Table IV. Result of AES ASIC design.

	Chip/Syn	Tech (μm)	Equivalent gates	Clock frequency	Volts (V)	Power consumed (μW)	Cycles
A. Ricci [15]	Syn	0.18	6k	2 MHz	0.6	2.5	N/A
Lin [20]	Syn	0.13	86.2k	N/A	1.2	40 900	10
Hsai [21]	Syn	0.18	11.277k	N/A	1.2	5.3	N/A
Tim.G [22]	Chip	0.18	4.7k	100 kHz	1.8	2.76	356
This work	Chip	0.18	4952	1.28 MHz	1.2v	1.51	204

ACKNOWLEDGEMENTS

This work was sponsored by the National Natural Science Funds of China (61076022 and 61211140046), the National High Technology Research and Development Program (“863” Program) of China (2011AA100701), and the Shanghai Pujiang Program.

REFERENCES

1. Weis SA, Sarma SE, Rivest RL, Engels DW. Security and privacy aspects of low-cost radiofrequency identification systems. *Proceedings of the 1st International Conference on Security in Pervasive computing*, 2004; 201–212.
2. Henrici D, Müller P. Hash-based enhancement of location privacy for radiofrequency identification devices using varying identifiers. *International Workshop on Pervasive Computing and Communication Security—Per-Sec 2004*, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer Society; 149–153.
3. Lehtonen M, Staake T, Michahelles F, Fleisch E. From identification to authentication—a review of RFID product authentication techniques. Printed handout of *Workshop on RFID Security—RFIDSec 2006*, 2006.
4. Syamsuddin I, Dillon T, Chang E, Han S. A survey of RFID authentication protocols based on hash-chain method. *Third International Conference on Convergence and Hybrid Information Technology*, 2008; 559–564.
5. Godor G, Giczi N, Imre S. Elliptic curve cryptography based mutual authentication protocol for low computational complexity environment. *5th IEEE International Symposium on Wireless Pervasive Computing*, 2010; 331–336.
6. Kim C-J, Yun S-Y, Park S-C. A lightweight ECC algorithm for mobile RFID service. *Proceedings of the 5th International Conference on Ubiquitous Information Technologies and Applications (CUTE)*, 2010; 1–6.
7. Guihao B, Minggao Z, Jiuwen L, Yin L. The design of an RFID security protocol based on RSA signature for e-ticket. *The 2nd IEEE International Conference on Information Management and Engineering (ICIME)*, 2010; 636–639.
8. Dang Nguyen Duc, Hyunrok Lee, and Kwangjo Kim, Enhancing security of EPCglobal Gen2 RFID tag against traceability and cloning. *Proc. Third Conf. Soft Computing and Intelligent Systems (SCIS ’06)*, Jan. 2006.
9. Sun H-M, Ting W-C. A Gen2-based RFID authentication protocol for security and privacy. *IEEE Transactions on Mobile Computing*, 2009; **8**(8):1052–1062.
10. Engels D, Fan X, Gong G, *et al*. Ultra-lightweight cryptography for low-cost RFID tags: hummingbird algorithm and protocol. CACR, 2009.
11. Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm. *Cryptographic Hardware and Embedded Systems—CHES 2004*, Volume 3156 of LNCS. Springer, August 2004; 357–370.

12. Kim K, Chung K, Shin J, *et al*. A lightweight RFID Authentication protocol using step by step symmetric key change. *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2009; 853–854.
13. Wolkerstorfer J, Oswald E, Lamberger M. *An ASIC implementation of the AES SBox [C]*. Lecture Notes in Computer Science, Volume 2271. Springer, 2002; 67–78.
14. Hamalainen P, Alho T, Hannikainen M, Hamalainen T.D. Design and implementation of low-area and low-power AES encryption hardware core. *Digital System Design: Architectures, Methods and Tools, 2006. DSD 2006. 9th EUROMICRO Conference*, 2006; 577–583.
15. Ricci A, Grisanti M, De Munari I, Ciampolini P. Design of a 2uW RFID baseband processor featuring an AES cryptography primitive. *IEEE ICECS*, 31 Aug 3 Sept, Malta, 2008, 376–379.
16. Yongzhen Q, Xin'an* W, Xiaoxing F, Weqing G. Design and implementation of a security-enhanced baseband system for UHF RFID tag. *ASIC, 2009. ASICON '09. IEEE 8th International Conference on Year*, 2009; 999–1002.
17. Xiaoxing F, Xin A, Xing Z, Yongzhen Q, Binjie G, Jinpeng S, Shan L. An UHF RFID transponder with novel demodulator and security algorithm. *Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on Digital Publication Year*, 2009; 254–257.
18. Lee J-W, Vo DHT, Huynh Q-H, Sang HHG. A fully integrated HF-band passive RFID tag ICUsing 0.18-μm CMOS technology for low-cost security applications. *IEEE Transactions on Industrial Electronics* June 2011; **58**(6):2531–2540.
19. Man ASW, Zhang ES, Lau VKN, Tsui CY. Luong HC. Low power VLSI design for a RFID passive tag baseband system enhanced with an AES cryptography engine. *1st Annual RFID Eurasia Conf.*, 5–6 Sept. 2007; 1–6.
20. Lin S-Y, Huang C-T. A high-throughput low-power AES cipher for network applications. *Proc. ASP-DAC 07*, 23–26 Jan, Yokohama, Japan, 2007; 595–600.
21. Hsai ML,Chen OT. Passive RFID transponder with power-aware encryption. *Midwest Symposium on Circuits and Systems*, Knoxville USA, 10–13 Aug 2008; 838–841.
22. Good T, Benaissa M. A low-frequency RFID to challenge security and privacy concerns. *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on Digital Object, Year*, 2009; 856–863, IEEE Conference Publications.
23. Nohl K, Evans D, Starbug S, Plötz H. Reverse-Engineering a Cryptographic RFID Tag. *17th USENIX Security Symposium*, Dec. 2007; Page(s): 185–193.
24. de Koning Gans G, Hoepman J H, Garcia F. *A practical attack on the MIFARE Classic [J]*. Smart Card Research and Advanced Applications, 2008: 267–282.
25. Courtois N T, Nohl K, O'Neil S. *Algebraic attacks on the crypto-1 stream cipher in mifare classic and oyster cards [J]*. Early announcement of a research in progress, 2008: **14**.
26. Ryan R, Anderson Z, Chiesa A. *Anatomy of a subway hack [J]*. tech. mit. edu V, 2008: **128**.
27. Sarma S.E, Weis S.A, Engels D.W. RFID systems and security and privacy implications. Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems, 2003Page(s): 454–469.
28. Tuan A. P, Mohammad S. H, Hongnian Y. A RFID mutual authentication protocol based on AES, UKACC International Conference on Control, 2012.
29. Adam S.W. Man, Edward S. Zhang, Vincent K.N. Lau, C.Y. Tsui, Howard C. Luong, Low Power VLSI Design for a RFID Passive Tag baseband System Enhanced with an AES Cryptography Engine, RFID Eurasia, 2007.
30. A. Ricci, M. Grisanti, I. De Munar, P. Ciampolini, Design of a 2 μW RFID Baseband Processor Featuring an AES Cryptography Primitive, 15th IEEE International Conference on Electronics, Circuits and Systems (ICECS), 2008.