IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 7, 2019, accepted May 27, 2019, date of publication June 3, 2019, date of current version June 18, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920437

A Fully Integrated HF RFID Tag Chip With LFSR-based Light-weight Tripling Mutual Authentication Protocol

JIAHAO LU, DONGSHENG LIU, (Senior Member, IEEE), HAO LI, CONG ZHANG, AND XUECHENG ZOU

School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China

Corresponding author: Hao Li (hli@hust.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61874163, in part by the National Science and Technology Major Project under Grant 2017ZX01032-101, in part by the Introduced Innovative Research and Development Team of Dongguan under Grant 201760712600139, and in part by the Fundamental Research Funds for the Central Universities under Grant HUST: 2018KFYYXJJ056.

ABSTRACT Radio frequency identification (RFID) is widely used in various areas such as logistics, supply-chain management, and access control. The new challenge for designing an RFID tag is how to embed a low-cost and low-power consumption algorithm into a compact RFID tag chip. This paper presents a passive HF-band tag chip supporting ISO/IEC 14443 type A/B protocol with low-cost and low-power consumption. In the Analog Front End, a bridge rectifier with 73.76% power conversion efficiency is presented to accomplish RF-dc conversion. A robust demodulator with both 10% and 100% ASK demodulation capabilities and a subcarrier-based modulator are designed to complete the data transfer process. Moreover, a burr-eliminating power ON/OFF reset circuit is proposed to provide a reset signal for the system. In the digital baseband controller, a linear feedback shift register-based light-weight authentication protocol is presented to ensure data security while reducing resource overhead. The embedded 8-Kb EEPROM contains eight independent keys for eight different application fields. The tag chip is fabricated in HJ025 2P4M CMOS process with an area of 1.1mm $\times$ 1.18mm and total static power consumption of 116.45μW. The low cost and low-power consumption ensure the tag chip, especially suitable for smart cards.

INDEX TERMS RFID tag chip, AFE, authentication protocol, LFSR, light-weight.

I. INTRODUCTION

Radio Frequency Identification (RFID) is a technology that enables information communication between readers and tags. With the rapid development of IoT, RFID system is being widely used in mobile payment [1], [2], medical fields [3], [4] and logistics [5], [6] with its inherited advantages including incomparable flexibility [7], security [8] and low cost [9].

Nowadays, the wide use of Internet and wireless communication technology have stimulated the growth of RFID technology. There are some presented RFID researches with High Frequency(HF) band. Reference [10] presents a passive electronic tag for smart cards with high-security. Using the HHNEC 0.13 μm process, the chip area is 8.08mm^2. The security algorithm used is DES/3DES. The work in [11] uses 0.6 μm CMOS technology and its area is 2.8mm $\times$ 2.9mm with a power consumption more than 2mW and it uses DES for security. The chip in [1] is fabricated in 0.35 μm process with the area of 11.24 mm^2 and it utilizes AES to ensure security. They all have some common characteristics including large chip area, complex security algorithm, high power consumption and high cost.

In this paper a fully integrated passive HF chip is presented which is compatible with ISO/IEC 14443 A/B protocol. The chip is fabricated in HJ025 2P4M CMOS process with an area of 1.1mm $\times$ 1.18mm. Its static power consumption is as low as 116.45μW. A bridge rectifier, a 10% ASK demodulator and a power on/off reset circuit are designed in Analog Front End(AFE) and a Linear Feedback Shift Register(LFSR) based light-weight authentication protocol in Digital Baseband Controller(DBC). The paper is organized as follows.

The associate editor coordinating the review of this manuscript and approving it for publication was Vyasa Sai.

Section II describes the design of AFE. The design procedure of DBC and a LFSR based light-weight authentication protocol is proposed in Section III. Measurement results are presented in section IV and followed by conclusion in Section V.

II. ANALOG FRONT END

Fig. 1 shows the structure of AFE. Receiving the signals of reader, AFE generates VDD, VCC, CLK, Ring Oscillator and demodulated signal, named Data_in_ana. The power supply VDD is provided for DBC and EEPROM, and VCC for AFE respectively. VDD and VCC are separated to avoid the noise from DBC transmitting back to AFE although the same structure is used for the signals' generation. AFE also includes a burr-eliminating power-on and power-off RST block and a modulator using the 847KHz subcarrier for the wave separation. Ring Oscillator in the structure is a random seed generator, and make up a True Random Number Generator(TRNG) together with the post digital processor mentioned in DBC.

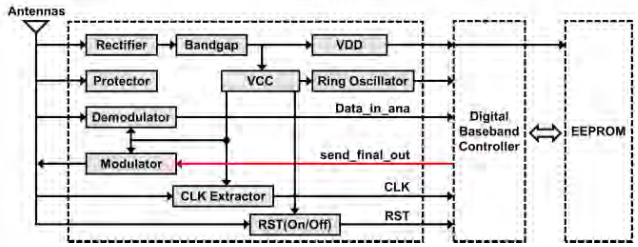


FIGURE 1. The block diagram of AFE.

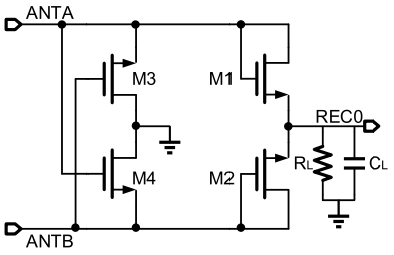


FIGURE 2. The structure NMOS gate-crossed rectifier.

A. RECTIFIER AND RF LIMITER

As shown in Fig. 2, a full-wave NMOS gate-crossed bridge rectifier is designed to generate the raw power supply REC0 for its higher driving capability than half-wave rectifier [12]. Schottky diodes are not used in the design due to cost and compatibility with standard CMOS process. ANTA and ATNB are connected to the tag's two antenna terminals and REC0 is the output. Large W/L of diode-connected MOSFETs are required to achieve higher driving capability and small W/L of switching MOSFETs for lower power consumption. The W/L of two switching MOSFETs is 16u/2u and W/L of two diode-connected MOSFETs is 140u/2u. Moreover, the Power Conversion Efficiency(PCE), which is defined as Pout/Pin$\times$100%, is a crucial parameter in estimating the performance of the rectifier. During the calculation, the integration of Vin$\times$Iin and Vout$\times$Iout in the stable stage are used, and a high PCE of 73.76% is achieved by adjusting the parameter of the MOSFETs at the estimating input of 8Vpp sine wave and load of 40KΩ(REC0's average voltage is about 6V and its drive capability should be about 150uA for driving DBC and AFE itself, so the load of 40KΩ is roughly estimated).

The RF limiter is necessary as the tag chip could be affected by both high RF power and static electricity [14]. In the reported research, many different kinds of limiter circuits are used. The design in [13] connects the drain and source of an NMOS to two antenna terminals as a RF limiter. Reference [10] uses a voltage clamping circuit to ensure the safety of the rectifier and the subsequent circuits. But none of them considers the effect of the signals transmitting back from DBC. Considering the feedback signals, a more robust RF limiter is designed. Fig. 3 shows the structure.

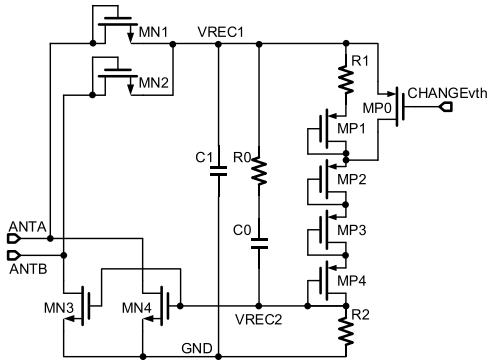


FIGURE 3. The circuit design of the robust RF limiter.

ANTA and ANTB link to the two terminals of the antenna. MN1, MN2 and C1 make up a simple full-wave regulator. R0 and C0 provide a fast AC way from VREC1 to the gate of MN3 and MN4. After powering on, VREC1 is established quickly. Divided by R1, MP1, MP2, MP3, MP4 and R2, a judge voltage VREC2 is generated, and if it is higher than the threshold voltage of MN3 and MN4, the path ANTA-MN4-MN3-ANTB will be formed. Because of the large W/L of MN3 and MN4, the impedance between two antennas will be very small, so its quality factor Q will be decreased and such a RF power will not damage the tag. CHANGEvth is derived from DBC, when the tag receives signal from reader, CHANGEvth is equal to VREC1, and when the tag responses to the reader, CHANGEvth is a Manchester signal modulated by subcarrier. It controls the involvement of R1 and MP1 to decide the amplitude of voltage of two antennas.

As for the statics protection, ANTA and ANTB will be connected to GND from MN4 and MN3 when too much statics stores in the tag.

B. VDD GENERATOR

The normal chosen structure of regulator is LDO, but it has a big power tube which costs a lot of area. As for RFID Tag ICs, the premise is small area and low cost. Fig. 4 shows

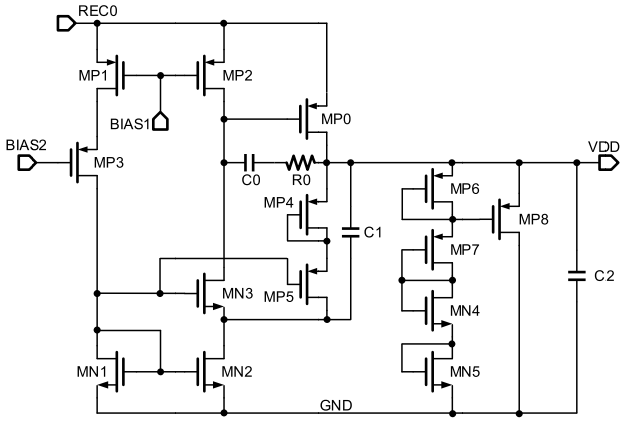


FIGURE 4. The circuit design of VDD generator.

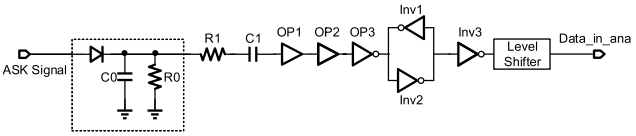


FIGURE 5. The structure of 10% ASK demodulator.

the designed circuit. It is a simple regulator to provide a stable 1.8V output. After powering on, REC0, BIAS1 and BIAS2 set up quickly, so MP1, MP2, MP3 and then MN1 turn on. VDD goes up because the path REC0-MP2-C0-R0-C2-GND forms and VDD is the plus terminal voltage of C2. The drain of MN2 will be charged by VDD through C1 and then MN2 turns on, after which, MN3 and MP0 turn on in order, so all the path to set up VDD turns on and a stable VDD generates which can be expressed by:

$$VDD=V_{SGMP4}+V_{SGMP5}+V_{GSMN1} \tag{1}$$

C. ASK DEMODULATOR AND MODULATOR

The ISO/IEC 14443 A protocol uses 100% and ISO/IEC 14443 B protocol uses 10% ASK modulation for the reader-to-tag communication. Fig. 5 shows the structure of 10% ASK demodulator which can also support the demodulation of 100% modulated signals. Inside the dotted box is a RC envelope extractor. Connecting to it, R1 and C1 provide AC path for the envelope to detect its edge. OP1 and OP2 are low gain amplifier and OP3 is an inverter. Inverter 1 and 2 make up a cross-coupled memory cell, and Level Shifter shapes the wave to meet the requirements of DBC.

During the use, the extracting result has ripple due to the RC sampling accuracy, so OP1 and OP2 are designed to smooth the ripple. The structure is shown in Fig. 6. It has a low gain region which means when the bias voltage of this circuit changes within the low gain region, the circuit's output is relatively stable. So the low gain structure helps in improving the anti-jamming capability of the demodulator.

Fig. 7 illustrates the simulation results of the structure in Fig. 6. The structure has two conversion voltage, the lower one is the input for the subthreshold conduction of MN2,

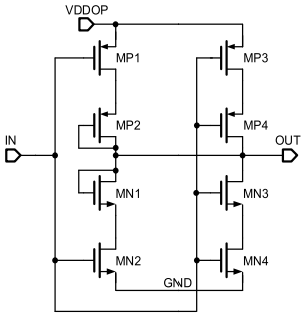


FIGURE 6. The circuit design of low gain amplifiers OP1 and OP2.

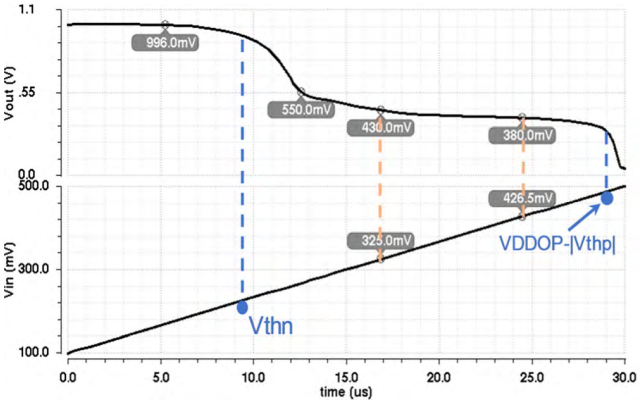


FIGURE 7. The transmission characteristics of OP1 and OP2.

approximately to Vthn, and the higher one is the input for the subthreshold conduction of MP1, approximately to VDDOP-|Vthp|. When IN rises and reaches the subthreshold conduction voltage of MN2, MN2 turns on, and MP3, MP4, MN1, MN2 form a path to GND so OUT goes down quickly from 1.0V to 550mV. Then IN continuing to rise, the output impedance of MP3 and MP4 increases quickly, but the output impedance of MN1 and MN2 decreases slowly so that the output voltage also decreases slowly from 550mV to 380mV. When output voltage falls into the region turning on MP2 in subthreshold stage, MP2 turns on so that the output voltage goes down quickly to GND. As is illustrated in Fig.7, when Vin varies from 325mV to 426.5mV, the corresponding Vout from 430mV to 380mV, so the improving ratio(IR) can be calculated by

$$IR = \left|\frac{\Delta Vin}{\Delta Vout}\right| = \left|\frac{325-426.5}{430-380}\right| = 2.04 \tag{2}$$

So during the application, the bias voltage should be set in the period during which the output is stable enough to improve immunity of the circuit.

The subcarrier modulation theory is used in the modulator design. Detecting the change of the resistance of two antennas during the signals' feedback period from DBC to AFE, the reader reaches voltages of different amplitude with signals attached. During the modulation process, 847KHz subcarrier is used. The structure of modulator is shown in Fig. 8. ANTA and ANTB connect to the terminals of antennas, and

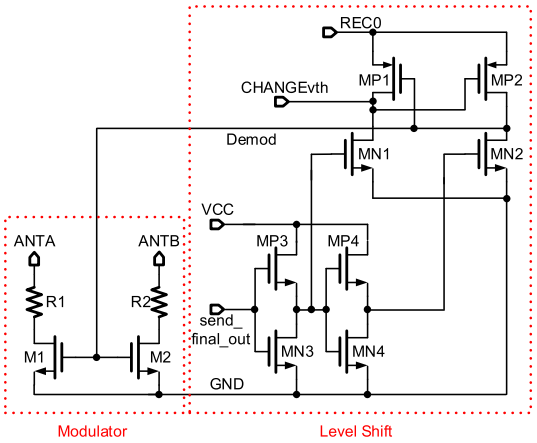


FIGURE 8. The structure of modulator.

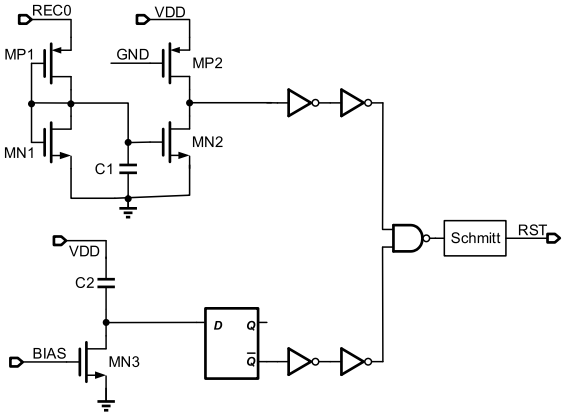


FIGURE 9. The structure of RST block.

Demod controls M1 and M2 so the antennas' resistance will be modified when these two MOSFETs open or close. According to ISO/IEC 14443 protocol, the amplitude of two sidebands(13.56MHz±847KHz) should be both larger than 10mV for the reader to distinguish the signals from the tag [14] to complete the process of feedback signals.

D. RST

DBC and EEPROM contained in the tag both need reset signal to start, and if the voltage turns down abruptly, AFE should be able to inform DBC and EEPROM to protect their data, so a circuit with power-on and power-off reset capability is designed. Fig. 9 shows the structure.

After powering on, REC0 and VDD set up quickly, and MN2 turns on so its drain voltage drops, that is to say, the upper half provides "0" to NAND. As for the lower half part in Fig. 9, the voltage of C2's lower plate is pulled up fast by VDD so MN3 turns on. Then the input of D-trigger is "0" so /Q outputs "1", namely the lower half provides "1" to NAND. So RST jump from the initial "0" into "1", namely power-on reset is generated.

When the antennas' voltage drops accidently, REC0 turns down but VDD stands still, and when REC0 is close to VDD, they go down together, so the charge of C1 leaks in the meantime. MP2 and MN2 make up a simple comparator whose conversion voltage is approximately VthMN2, and when the voltage of C1 is lower than the conversion voltage, the upper half outputs "1". When the voltage of the C2's bottom plate is lower than the turning voltage of D-trigger, /Q equals to "1". So RST turns "0", namely, a power-off reset is generated.

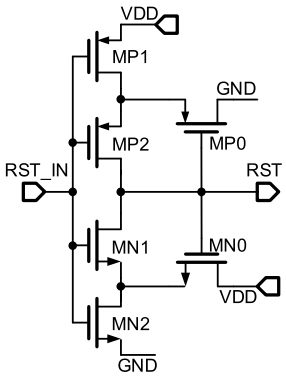


FIGURE 10. The Schmitt circuit used in RST block.

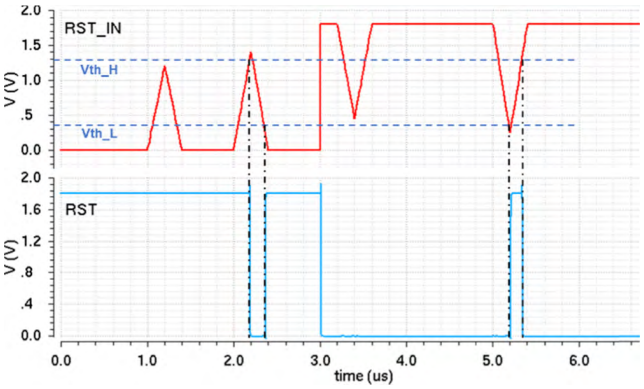


FIGURE 11. The performance of the designed Schmitt circuit.

The spotlight of this circuit is the Schmitt circuit, as shown in Fig. 10, which can filter the burrs caused by noise efficiently. Its performance is shown in Fig. 11, in which Vth_H and Vth_L are the upper and the lower threshold voltages of the Schmitt circuit. When RST_IN is "0", MP1 turns on so its drain voltage is pulled up, then MP2 turns on, whose drain is also pulled up and RST is "1". As is illustrated in Fig. 11, when RST_IN is lower than the upper threshold voltage Vth_H, RST remains "1", and RST changes from "1" to "0" only when RST_IN is higher than Vth_H. Conversely, when RST_IN drops, RST changes from "0" to "1" only when RST_IN is lower than Vth_L. So when RST_IN is "0" originally, the burrs with a magnitude below Vth_H will be filtered and when RST_IN is "1" originally, the burrs with a magnitude over Vth_L will be filtered.

III. DIGITAL BASEBAND CONTROLLER

A. ARCHITECTURE OF DBC

The proposed Digital Baseband Controller(DBC), which is compatible with the ISO14443 type A/B protocol, consists

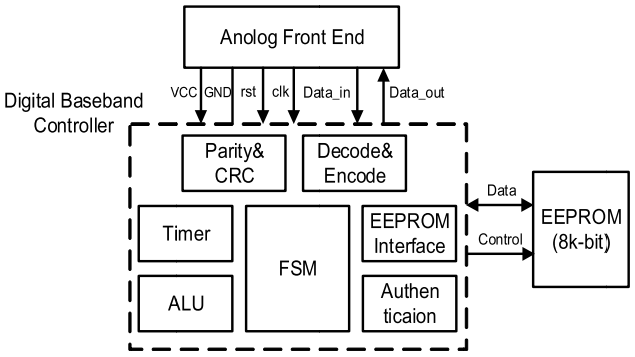


FIGURE 12. The architecture of digital baseband controller.

of seven modules, as illustrated in Fig. 12. And in Fig. 12, we also present the other two parts, AFE mentioned above and Electrically Erasable Programmable Read-only Memory(EEPROM). These two parts together with DBC make up the entire RFID tag chip.

In the mutual communication between reader and tag, the AFE provides demodulated data, RST and CLK signal to the DBC. The Timer module deals with the incoming CLK signal and divides it into appropriate frequency. The ALU module accomplishes all the arithmetic operation. The Decoder module coordinated with the Parity & CRC module checks the validity of the incoming frame and extracts useful command data. As long as the frame is valid, the finite-state machine(FSM) module will control the classification and execution of the extracted command data and cooperate with the ALU module to get the specific response. When the command is authentication related, the authentication module will use LFSR structure to generate true-random numbers and realize encryption. The Encoder module coordinated with the Parity & CRC module encodes data and generates the valid response frame. When the DBC needs to get access to EEPROM, the EEPROM Interface will provide the required signals obeying the time diagrams of the EEPROM.

The EEPROM is a total of 8K-bit or 1K-Byte memory which is organized as 64 blocks×16 Bytes. The 64 blocks consist of one only Tag ID block, 6 access condition blocks, 9 key blocks and 48 data blocks. The 9 key blocks are numbered from key[0] to key[8] and key[8] is only for Kill command which is to deactivate the tag for destruction. The remaining 8 independent keys can be used in eight different applications for authentication. That means the tag IC can be applied to eight different fields simultaneously. The 16 Bytes register can be written simultaneously during a write cycle with serial in/out interface. Using CMOS technology to manufacture the device makes the access time lower down to 90ns at low power dissipation.

B. LIGHT-WEIGHT TRIPLING MUTUAL AUTHENTICATION PROTOCOL

The designed tripling mutual authentication protocol is proposed in Fig. 13. It can satisfy the security requirement of the ISO 14443 type A/B protocol. According to the protocol, after sending the authentication command to tag from reader, the communication between tag and reader is performed three times to insure the protocol's security. The proposed mutual authentication protocol is based on Linear Feedback Shift Register (LFSR) function which is a lightweight encryption function. The function has 64-bit shift register and will shift one bit each CLK cycle. It uses secret key to control the shift step and determine the next shift bit to complete the lightweight encryption process.

TABLE 1. Notation of the used characters.

Characters	Notations
Auth	Authentication command
$Rb_{(1)}$*	The 32-bits true-random number generated by tag, subscript 1 stands for the true-random number received in reader from tag
$Ra_{(1)}$*	The 32-bits true-random number generated by reader, subscript 1 stands for the true-random number received in tag from reader
$LFSR_{1or2}$ (A,B)	LFSR function, A and B are two input signals of the function, subscript means the number of execution
||	Bit series connection
M_i	The key block key[i] in the memory
tLFSR, tLFSR', wLFSR, wLFSR'	The result of LFSR function

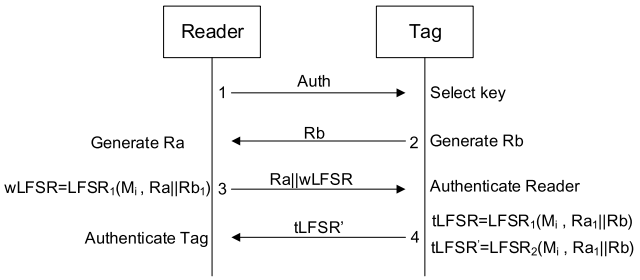


FIGURE 13. The proposed light-weight authentication protocol.

We assume that the tag and reader have stored the same key blocks in advance and the communication between reader and back-end server is definite secure. The notations used are showed in TABLE 1. Fig. 13 shows the whole process of the authentication protocol. The detailed procedures for each step is described as followed:

Step 1: The reader sends Auth command to the tag, and the used secret key block address is embedded in the command frame.

Step 2: When the tag receives the Auth command, it will generate a true-random number Rb and transmit it to the reader.

Step 3: The reader receives Rb1 and then generates Ra. The reader then utilizes the secret key Mi and the connected random number Ra||Rb1 to get the result of wLFSR by function LFSR:

$$\text{wLFSR}=\text{LFSR}_1(M_i, \text{Ra}||\text{Rb}_1) \tag{3}$$

After that the reader transmits Ra||wLFSR to the tag.

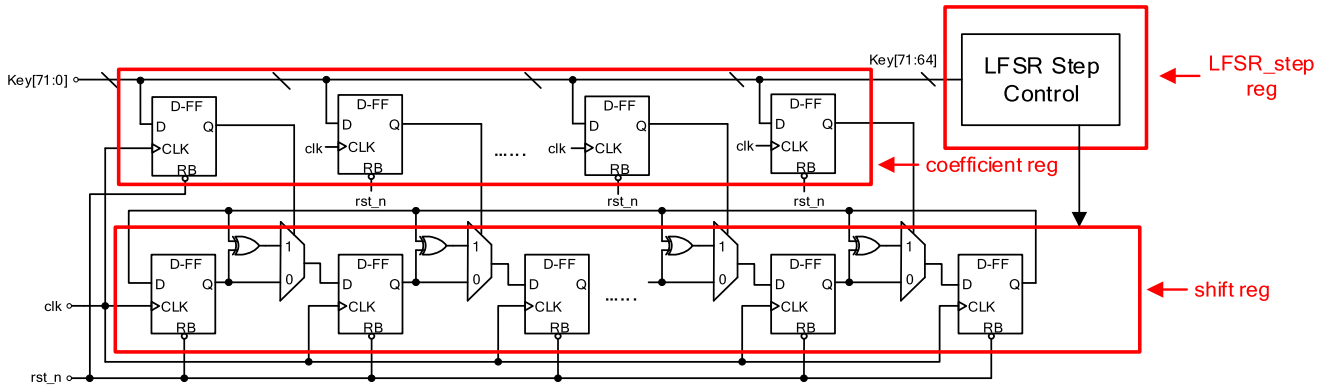


FIGURE 14. The structure of LFSR encryption function.

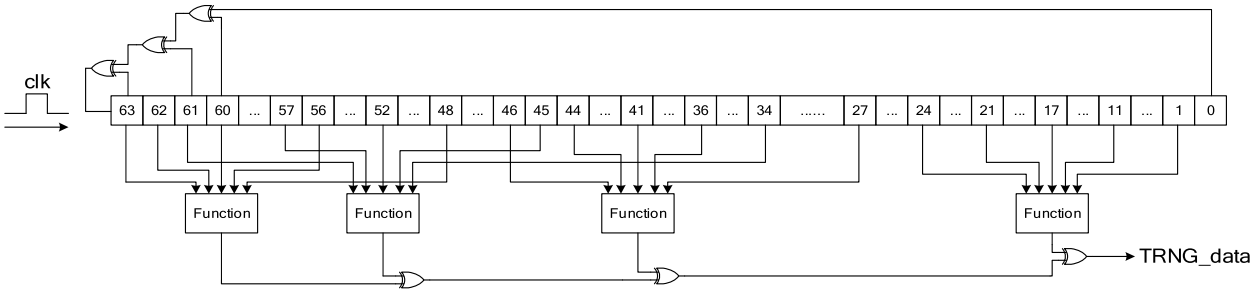


FIGURE 15. The structure of post digital processor of TRNG.

Step 4: This is the tag authentication phase. In this phase, the tag authenticates the reader.

1) The tag extracts Ra_1 and $wLFSR_1$ from the received data.
2) Regarding $Ra_1||Rb$ and Mi as two inputs of the function LFSR and get the result of $tLFSR=LFSR_1(Mi, Ra_1||Rb)$
3) If $tLFSR = wLFSR_1$, it means the tag successfully authenticates the reader. If $tLFSR \neq wLFSR_1$, the state machine will return to an error state.
4) Continue to execute function LFSR, and calculate the result of $tLFSR'=LFSR_2(Mi, Ra_1||Rb)$.Then send it to reader, prepare for the authentication in reader.

Step 5: This is the reader authentication phase. In this phase, reader authenticates the tag.

1) The reader takes over $tLFSR_1'$
2) Continue to execute function LFSR, calculate the result of $wLFSR'=LFSR_2(Mi, Ra||Rb_1)$
3) If $tLFSR_1'=wLFSR'$, it means the reader successfully authenticates tag and the whole authentication procedure is done. If not, the state machine will return to an error state.

C. DESIGN AND IMPLEMENTATION OF LFSR

1) LINER FEEDBACK SHIFT REGISTER FUNCTION

In this paper, we design a light-weight encryption function based on LFSR. As shown in Fig. 14, this structure, which is Galois type, is constituted of three parts: shift register(SR), LFSR_step register(LR) and coefficient register(CR).

To the light-weight encryption function LFSR(Mi,random), Mi = {mb, ma}, random = Ra||Rb. The bit length of mb is usually set to 8 bits. The random and ma have the same 64 bit length. Before the start of encryption, SR should be initialized with random number Ra||Rb generated by TRNG. And the used key will be divided into two parts ma and mb, they will be used to load in CR and LR respectively in the beginning. LR decides the shift step of LFSR in each execution, and it cannot be fulfilled with all logic zero bits. CR initialized data should at least include three logic "1" bits.

CR is regarded as the control signal of multiplexer which is to select the next shift bit. When every effective CLK edge comes, the SR will shift right 1-bit according to the structure. The last bit will fill in the vacant highest bit and it will also become one of the parameters of XOR operation. In each execution, the LFSR will shift mb clock cycles to generate the 32 bits value wLFSR(or tLFSR) = LFSR(Mi, random).

2) TRUE-RANDOM NUMBERS GENERATOR

In this design, the True Random Numbers Generator is realized by Ring Oscillator in Fig.1 and post digital processor which is designed to improve the unpredictability and randomness. The structure of the post digital processor is shown in Fig. 15.

TABLE 2. Results of NIST randomness test.

NIST random tests	The average of P-value	Pass rate
Frequency	0.44705969	98%
Block Frequency	0.49227702	98%
Cumulative Sums	0.50759657	98%
Runs	0.5020036	98%
Longest Run	0.45973381	99%
Rank	0.55228669	100%
FFT	0.50860565	100%
Overlapping Template	0.50375037	100%
Approximate Entropy	0.4660371	100%
Serial	0.53784511	99%
Linear Complexity	0.51136779	99%
Non Overlapping Template	0.37379925	100%
Universal Statistical	0.43895337	98%
Random Excursions	0.42190871	97%
Random Excursions Variant	0.38952846	98%

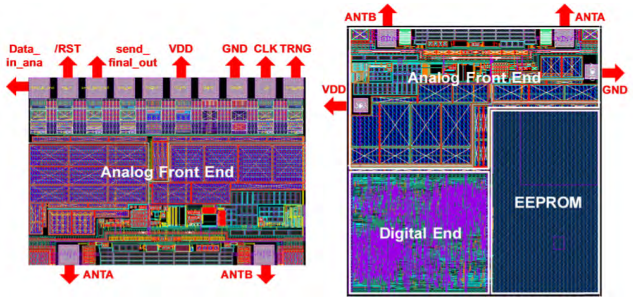


FIGURE 16. (a) The layout of AFE. (b) The layout of tag IC.

The 64 bits LFSR registers shift right at every rising edge of CLK. And the highest bit(D_{63}) will be reloaded as $D_{63} \oplus D_{61} \oplus D_{60} \oplus D_0$. The detailed operation is described as follows:

Step 1: The analog oscillator structure is used for TRNG to generate initial 32-bit seed.

Step 2: The shift register is loaded as seed connected to its reversal data at first. And then TRNG will run for 64 CLK cycles to initialize the whole structure.

Step 3: Continue to execute TRNG for another 64 CLK cycles. During each cycle, 20 bits are extracted and divided into 4 groups averagely. The 5 bits in each group then become the 5 inputs of the defined filter function and get one bit out marked as $wt_{1,2,3,4}$. Then the four output bits XOR each other to get the final one bit out as the result of this cycle. And the 64 bits random number is serial generated after TRNG runs for 64 CLK cycles. The filter function is defined as:

$$\begin{aligned} &\text{Function\_fir}(x1, x2, x3, x4, x5) \\ &\quad = x1 \oplus x3 \oplus x4 \oplus x5 \oplus (x2\&x4) \\ &\qquad \oplus((x1 \oplus x2 \oplus x3)\&(x3 \oplus x4 \oplus x5)) \quad (4) \\ &wt_1 = \text{Function\_fir}(D_{63}, D_{62}, D_{60}, D_{56}, D_{48}) \quad (5) \\ &wt_2\, wt_2 = \text{Function\_fir}(D_{46}, D_{44}, D_{41}, D_{36}, D_{27}) \quad (6) \\ &wt_3\, wt_3 = \text{Function\_fir}(D_{61}, D_{57}, D_{52}, D_{45}, D_{34}) \quad (7) \\ &wt_4 wt_4 = \text{Function\_fir}(D_{24}, D_{21}, D_{17}, D_{11}, D_1) \quad (8) \end{aligned}$$

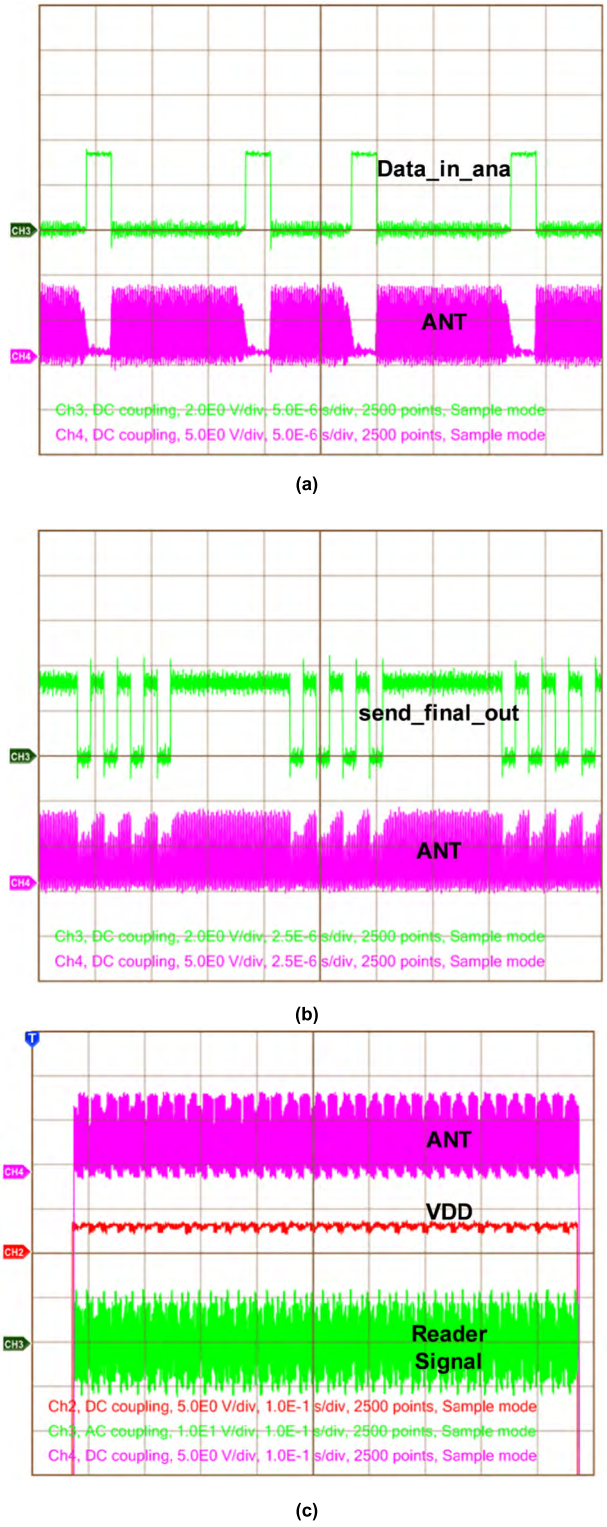


FIGURE 17. (a) The demodulation test result of AFE. (b) The modulation test result of AFE. (c) The test of the integrated tag IC.

The bit length of shift register of TRNG and LFSR function are the same. So, the 64 bits registers can be reused in the two structure which greatly reduce the hardware resource consumption. The designed TRNG has successfully passed the NIST randomness test. Results of the test are shown in

TABLE 3. Comparison with previous researches.

Design	[1] *	[2]	[10]	[11]	[13]	This Work
Process	0.35μm	0.18μm	0.13μm	0.6μm	0.18μm	**0.25μm**
Power Consumption	990μW	NA	NA	2.5mW	360μW	**116.45μW**
Protocol	14443A	14443A	14443A	14443B	14443B	**14443A/B**
Memory	4Kb EEPROM ROM(CU constants) RAM macro (128 × 16-b)	8Kb EEPROM 32Kb ROM	32Kb EEPROM	8Kb EEPROM	4Kb EEPROM	**8Kb EEPROM**
Security Algorithm	AES	3DES	DES/3DES	DES	AES	**LFSR**
Schottky diode	NA	NA	NO	NO	YES	**NO**
Size(mm^2)	11.24	3	8.08	8.1	1.1	**1.298**

* The size of [1] is presented by 49999GEs under 0.35μm process, and it is converted to unit in mm^2 for comparison

TABLE 2. The pass rate of Random Excursions reaches 97%, which is the lowest one among all the 15 test items. There are 5 test items with a pass rate of 100%.

D. SECURITY ANALYSIS

The presented authentication protocol is based on ISO/IEC 9798-2 and the security of the design is analyzed in this part. And the protocol is secure against these attacks mentioned below:

Eavesdropping: During the forward and backward channel, attacker can only acquire the data of Rb, $wLFSR_1$, Ra_1, $tLFSR_1$. None of these data has privacy information included directly though they are all related to the key M_i except Ra_1 and Rb. The secret keys are protected in the chip so that simple eavesdropping cannot help attackers get the information.

Location Tracking: As the true random number is used in every transformation between the reader and tag, no matter what step the authentication protocol runs to, the data in the air is always different. So it's impossible for attackers to track the tag by intercepting information exposed in air.

Replay Attack: The initial seed used to generate random number is produced by analog oscillator. So in each round of authentication, the seed is random and unpredictable, which means the transferred random number changes between each two rounds. Obviously, the secret key used in the tag cannot be obtained by simply replaying the information tapped in last round of authentication.

Man-in-the-middle Attack: The man-in-the-middle attack won't work because this design possesses strong integrity in the authentication. Any attempt to replace the data will make the authentication stop.

IV. MEASUREMENT RESULTS

The chip is fabricated in HJ025 2P4M CMOS process with an area of 1.1mm × 1.18mm. Fig. 16 shows the layout of

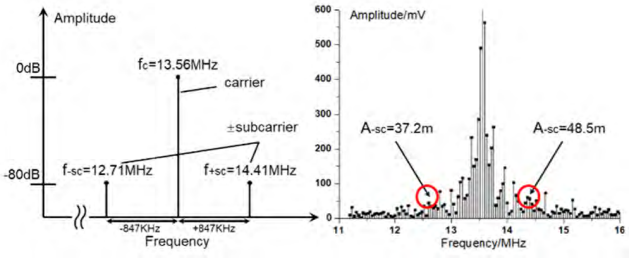


FIGURE 18. (a) The principle of subcarrier modulation. (b) The spectrum of the reader's receiving signal.

separated AFE and the fully integrated tag IC. Some pins for test its functionality are located separately around.

Self-designed PC software and reader supporting ISO14443 type A/B protocol are used during the measurement. Pins of chip for measurement are respectively connected to an oscilloscope with a probe containing 10MΩ impedance and 16pF capacitor.

Fig. 17 shows the results of measurement when PC software sends REQA command [8]. Fig. 17(a) illustrates the command can be demodulated successfully and Fig.17 (b) shows DBC's feedback signal send_final_out can modulate the carrier wave obviously. Fig. 17 (c) illustrates that VDD is 2.5V with ripple and ANT is modulated. We can also see signals attached in the reader's receiving signal, meaning the DBC is processing the data. As Fig. 18 (a) shows, ISO/IEC 14443 protocol stipulates that the amplitude of two sidebands should be higher than −80dB, namely 10mV. Fig. 18(b) shows the spectrum of the reader's receiving signal, and the amplitudes of two sidebands (13.56±847KHz) are much larger than 10mV so the signals are easy to be detected by the PC software, which means the success of modulating process.

Table 3 gives a performance comparison of recently reported research. Although 0.25μm process is used, a smaller area is achieved, which means lower cost. And our design can support both ISO14443 type A and B

TABLE 4. The performance of the tag IC.

Item	Performance
Carrier Frequency	13.56MHz±7KHz
Power	2.5V±10%
Demodulation Type	10% ASK/100% ASK
Data Rate	106Kbps
Security Algorithm	LFSR
Anti-collision capability	YES
Subcarrier Frequency	847.5KHz
Recognition distance	0.3cm-3.1cm

protocol simultaneously. Table 4 shows the performance of the designed chip.

V. CONCLUSION

A fully integrated RFID chip with mutual triple authentication protocol is presented in this paper. The chip is fabricated in HJ025 2P4M CMOS process and the area of chip is 1.1mm × 1.18mm with a total power consumption as low as 116.45μW. In AFE, an NMOS gate-crossed bridge rectifier is designed with a high PCE of 73.76% and the RF limiter designed can prevent the chip from the over-high RF power and over accumulated statics. Moreover, a power on/off reset circuit is designed. The digital part has an on-chip 8-Kb EEPROM to support the normal data processing. The tag IC can be applied to multiple application fields simultaneously with the stored eight independent keys. In order to simplify circuit structure while ensuring security, a LFSR structure is used to the light-weight authentication protocol for true random data generation and data encryption. The whole measurement and analysis of the designed RFID tag with HF-band reader and PC measurement software reveal success in all designed specifications. The main advantages of our design are the unique security algorithm, low cost and low power consumption. These merits ensure the chip's suitability for smart cards, access control and supply-chain management.

REFERENCES

[1] T. Plos, M. Hutter, M. Feldhofer, M. Stiglic, and F. Cavaliere, "Security-enabled near-field communication tag with flexible architecture supporting asymmetric cryptography," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 21, no. 11, pp. 1965–1974, Nov. 2013.

[2] D. Wang, J. Hu, and H.-Z. Tan, "A highly stable and reliable 13.56-MHz RFID tag IC for contactless payment," *IEEE Trans. Ind. Electron.*, vol. 62, no. 1, pp. 545–554, Jan. 2015.

[3] S. Jisha and M. Philip, "RFID based security platform for Internet of Things in health care environment," in *Proc. Int. Conf. Green Eng. Technol.*, Nov. 2016, pp. 1–3.

[4] D. Jayawardana, S. Kharkovsky, R. Liyanapathirana, and X. Zhu, "Measurement system with accelerometer integrated RFID tag for infrastructure health monitoring," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 5, pp. 1163–1171, May 2016.

[5] B. Skowron-Grabowska and T. Szczepanik, "Application of RFID technologies in logistics centres to improving operations of courier firms," in *Proc. IEEE Int. Conf. RFID Technol. Appl.*, Sep. 2017, pp. 140–145.

[6] R. Caso, A. Michel, M. Rodriguez-Pino, and P. Nepa, "Dual-band UHF-RFID/WLAN circularly polarized antenna for portable RFID readers," *IEEE Trans. Antennas Propag.*, vol. 62, no. 5, pp. 2822–2826, May 2014.

[7] J. Lechner, W. A. Günthner, S. Nosovic, and A. Ascher, "Context-based monitoring of logistic process events using passive UHF RFID technology," in *Proc. IEEE Int. Symp. Robot. Intell. Sensors (IRIS)*, Oct. 2017, pp. 260–265.

[8] Z. Liu, D. Liu, and X. Zou, "An efficient and flexible hardware implementation of the dual-field elliptic curve cryptographic processor," *IEEE Trans. Ind. Electron.*, vol. 64, no. 3, pp. 2353–2362, Mar. 2017.

[9] M. Y. Ahmad and A. S. Mohan, "Novel bridge-loop reader for positioning with HF RFID under sparse tag grid," *IEEE Trans. Ind. Electron.*, vol. 61, no. 1, pp. 555–566, Jan. 2014.

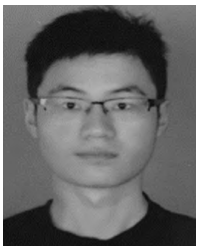
[10] K. Chen, D. Zhao, H. Zhang, Y. Wang, and L. Liu, "13.56 MHz passive electron tag for smart card application with high-security," in *Proc. IEEE Int. Conf. RFID-Technol. Appl.*, Sep. 2013, pp. 1–6.

[11] P. Rakers, L. Connell, T. Collins, and D. Russell, "Secure contactless smartcard ASIC with DPA protection," *IEEE J. Solid-State Circuits*, vol. 36, no. 3, pp. 559–565, Mar. 2001.

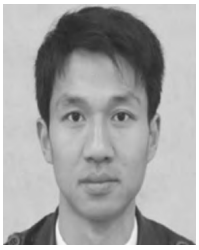
[12] J. Lim, B. Lee, and M. Ghovanloo, "Optimal design of a resonance-based voltage boosting rectifier for wireless power transmission," *IEEE Trans. Ind. Electron.*, vol. 65, no. 2, pp. 1645–1654, Feb. 2018.

[13] J. W. Lee, D. H. T. Vo, Q. H. Huynh, and S. H. Hong, "A fully integrated HF-band passive RFID tag IC Using 0.18-*mum* CMOS technology for low-cost security applications," *IEEE Trans. Ind. Electron.*, vol. 58, no. 6, pp. 2531–2540, Aug. 2010.

[14] L. Dongsheng, L. Huan, Z. Xuecheng, G. Liang, Y. Ke, and L. Zilong, "A high sensitivity analog front-end circuit for semi-passive HF RFID tag applied to implantable devices," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 8, pp. 1991–2002, Aug. 2015.



JIAHAO LU received the B.S. degree in integrated circuit design and integrated systems from the Huazhong University of Science and Technology, Wuhan, China, in 2018, where he is currently pursuing the Ph.D. degree with the School of Optical and Electronic Information. His current research interests include digital integrated circuits and artificial intelligence algorithms for implantable medical.



DONGSHENG LIU received the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, China, in 2007. In 2013, he was selected to Wuhan Chenguang Youth Talent Support Program. He is currently a Full Professor with the School of Optical and Electronic Information, Huazhong University of Science and Technology. His main research interests include VLSI design, RFID tag chip, RF transceiver, and cryptographic processor. He was served as the Team Leader of at least six important projects in last five years, including a subproject of the National Science and Technology Major Project, two National Natural Science Foundation of China, a Wuhan Fundamental Research Project, and three enterprise cooperation projects. He has authored or coauthored over 50 technical papers. He holds eight Chinese patents. Many of them have been published in flagship transactions of several IEEE societies, including TCAS I and TIE. Furthermore, his long-term dedication on the field of RFID is well recognized by the industry community.

HAO LI received the B.S. degree in microelectronics science and engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2018, where he is currently pursuing the M.S. degree with the School of Optical and Electronic Information. His current research interests include analog front end design for SoC and RF front end design for implantable medical.

CONG ZHANG was born in Hubei, China, in 1994. He received the B.S. degree in integrated circuit design and integrated system from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2016. He is currently pursuing the Ph.D. degree with the School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan, China. His current research interests include digital integrated circuits and cryptographic processor design.

XUECHENG ZOU received the Ph.D. degree in electronic science and technology from the Huazhong University of Science and Technology, Wuhan, China, in 1993, where he is currently a Professor with the School of Optical and Electronic Information. His research interest include IC design and the Internet of Things.