Proceedings of the 5th WSEAS Int. Conf. on Instrumentation, Measurement, Circuits and Systems, Hangzhou, China, April 16-18, 2006 (pp166-169)

Low Frequency Passive RFID Transponder with Non-revivable Privacy Protection Circuit

M. F. Lu, S. Y. Chang, C. M. Ni, J. S. Deng, and C. Y. Chung
Institute and Department of Electronic Engineering
Ming Hsin University of Science and Technology
No. 1, Hsin Hsin Rd., Hsinfeng, Hsinchu, Taiwan
http://www.et.must.edu.tw/menu/teacher/LMF/index.htm

Abstract: -A non-revivable Privacy Protection Circuit is proposed and designed in a low frequency passive Radio Frequency Identification (RFID) transponder. The main component of the non-revivable Privacy Protection Circuit is a poly fuse. The fuse acts as a switch and will be burn out when the function of transponder must be disabled. The broken fuse can not be repaired and prohibit the power required for the internal circuits. Thus, the transponder is non-revivable and personal privacy can be fully protected. The carrier frequency of this passive transponder is 125 kHz and the working voltage is 5V. Power and data are transmitted from a reader to the transponder by inductive coupling. The circuits in the transponder including rectifier, clock generator, sequencer, memory, and ASK modulator. The whole chip is designed and verified based on the 0.35 μm semiconductor process provided by the Taiwan Semiconductor Manufacturing Company.

Key-Words: - Radio frequency identification (RFID), Poly fuse, Privacy protection, Transponder

1 Introduction

As compared to the conventional technology of magnetic cards or IC cards, radio frequency identification (RFID) has the following advantages: such as wireless communication, hard to wear out, compact size, etc. RFID system consists of a reader and a transponder (also called a tag), information transmits and receives wirelessly between them through radio frequency. Energy can also transfer from a reader to a tag through electromagnetic wave to supply the power required in a passive transponder. With the rapid growth in applications, global companies invest in RFID and their products are ubiquitous in the market.

While the usage of RFID is pervasive, security and privacy concerns become the major issue that we must face [1-3]. Someone may collect information contained in RFID chips; this is an aggression to customer's right to privacy. So, consumers request that the tags should be removed or the data contained in tags should be erased after the products left the store. There are some researchers focus on this issue and use EEPROM or Flash to register the data of locking bit [4-9]. But as we known, the information reserved in nonvolatile memory can be overridden easily by electrical signal. Therefore, we propose the "Low frequency passive RFID transponder with non-revivable privacy protection circuit" to solve the problem of privacy concern. The main component of the Privacy Protection Circuit (PPC) is a poly fuse. After check-out, the card reader will send a pulse signal to notify the PPC to burn the poly fuse out. The broken fuse acts as a switch and prohibits the energy required for the internal circuits. It can not be repaired, thus this RFID is non-revivable, and personal privacy can be fully protected.

This study is aiming at the design of a passive RFID tag, its carrier frequency is 125 kHz and working voltage is 5V. The data and power are transmitted through inductive coupling between a reader and this tag. Meanwhile, the power is provided to the internal circuits through rectification and voltage stabilization. The other circuits include sequencer, clock generator, memory, ASK (Amplitude Shift Keying) modulator, and a non-revivable privacy protection circuit designed by the fuse mechanism.

In the following sections, we show the architecture of a low-frequency passive RFID. The functions of poly fuse and each block will be discussed. The circuit design and simulation, especially the non-revivable Privacy Protection Circuit, will be presented. Finally, the main features of this transponder will be listed in table.

2 The RFID with PPC

The block diagram of the low-frequency passive RFID with Privacy Protection Circuit is shown in Fig. 1. The architecture and functional descriptions of each block are as following:

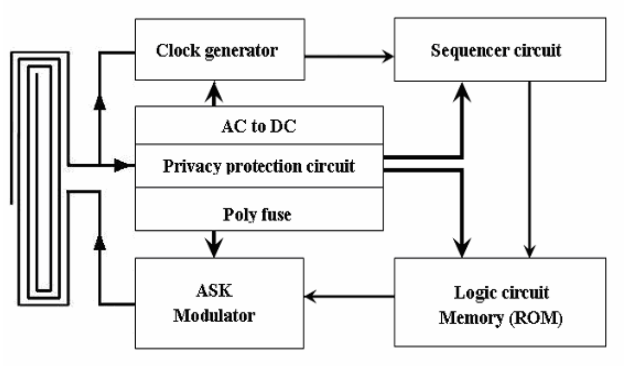


Fig.1. Architecture of the low-frequency passive RFID with Privacy Protection Circuit.

2.1 AC to DC converter

Active or semi-active tags have embedded battery as the energy source but passive tags do not have an embedded power. The energy required for a low frequency passive RFID is coupled from a reader through an inductive coil. After rectifying, filtering, and stabilizing, the AC electromagnetic wave is converted to DC source, and then is provided to each block. The rectifier may be replaced by a voltage multiplier to get a high enough voltage.

2.2 Clock Generator

The AC 125 kHz electromagnetic wave coupled from the inductive coil is also sent to the clock generator. The sense amplifier in clock generator transforms the sinusoidal wave to 125 kHz square wave, which is the synchronous pulse of digital circuits.

2.3 Sequencer and Memory

For simplicity, the memory embedded in this RFID is a 16bits read only memory (ROM), which is partitioned to 4 word lines by 4 bit lines. A sequencer constructed by counters generates 00, 01, 10, and 11 to drive the word lines and bit lines sequentially. Then the information stored in the memory will output in series.

2.4 Modulator

PWM, FSK, and ASK are the general modulation used in RFID system [10]. In our tag, the data stored in the memory are sent to the ASK modulator in series. The amplitude modulated signals are fed to the inductive coil and transmitted to the reader.

2.5 Privacy Protection Circuit

The main component of the Privacy Protection Circuit is a poly fuse as shown in Fig. 2. Poly fuse uses the minimum line width of polycrystalline silicon to connect two metal contacts. When the current through the fuse exceeds the power density it can hold, the polycrystalline silicon will evaporate and the fuse will burn out. Note that a window must open on the top nitride passivation layer, let the evaporated silicon volatilize through it. Otherwise the silicon may accumulate and the broken fuse may reform. While needed, the card reader will send a high power pulse to notify the PPC to burn the poly fuse out, that prohibits the energy required for the RFID.

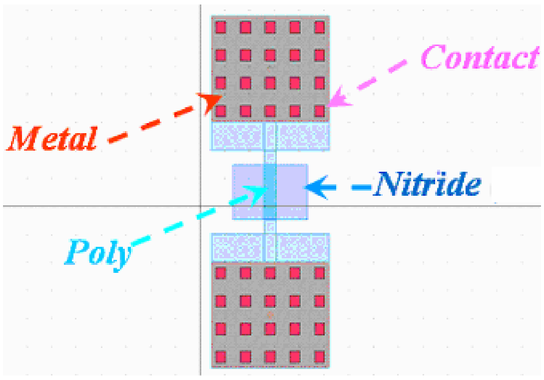


Fig.2. The structure of a poly fuse.

3 Circuit Design and Simulation

3.1 AC to DC converter and PPC

The front end circuit of the RFID including AC to DC converter and Privacy Protection Circuit is shown in Fig. 3. The AC power coupled from the inductive coil is converted to DC energy through the full-wave rectifier D_1~D_4. The ripple is filtered by the off chip capacitor C_1. The final output voltage V_{DD} is limited and stabilized by the Zener diode D_Z and the active loads M_7~M_{10}. The poly fuse and the current mirror M_1~M_6 build the Privacy Protection Circuit.

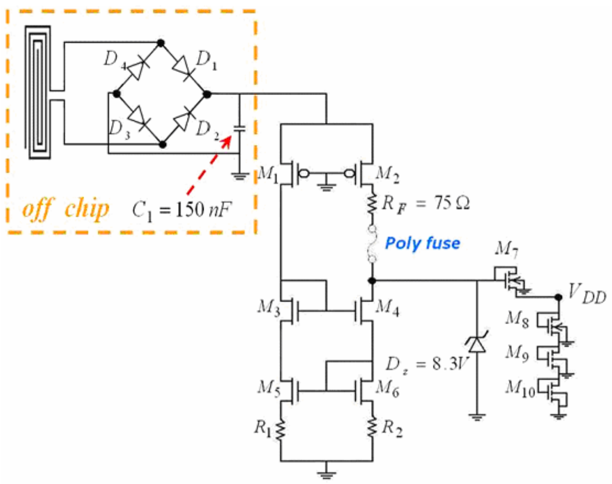


Fig.3. The AC to DC converter and Privacy Protection Circuit.

Table 1 shows the current and pulse width required to burn the poly fuse out [11]. We can see that the minimum line width of polycrystalline silicon will evaporate if the current through it is greater than 50 mA or the power density is larger than 0.9375 W/μm^2.

When the coil inductive power V_{P-P} = 32 V, the current through the poly fuse is less than 46 mA, the final voltage V_{DD} = 5V. The tag is in normal operation and the information of transponder will feed back to the reader.

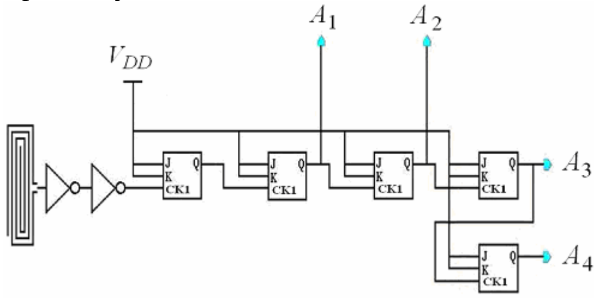
If the card reader sends a pulse signal and the coil inductive power V_{P-P} is larger than 48 V, the current through the poly fuse is greater than 77 mA. Then the fuse will be broken and no energy can be delivered to the internal circuits. The tag is in disable condition and is non-revivable.

Table 1 The current and pulse width required to burn the poly fuse out [11].

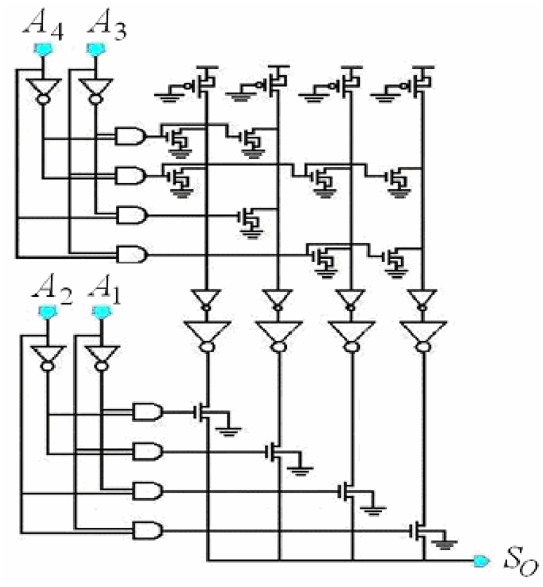
Width x Length (µm) / Pulse Width (ms)	0.4×1	0.4×2	0.4×3	0.4×5	0.4×10
1	75mA	50mA	50mA	50mA	50mA
10	75mA	75mA	100mA	75mA	50mA
100	75mA	75mA	75mA	75mA	75mA

3.2 Digital Circuits

Fig. 4 shows the digital circuits in the RFID including clock generator, sequencer and memory. The clock generator and sequencer shown in Fig. 4(a) consist of two inverters and five J-K flip-flops. The AC signals coupled from the inductive coil are converted to 125 kHz square wave through the clock generator. The clock drives the sequencer to generate A_1, A_2, A_3, and A_4 sequentially. A_1 and A_2 address the word lines, and A_3 and A_4 address the bit lines of 4×4 ROM, respectively.



(a)



(b)

Fig.4. The digital circuits in the RFID, (a) the clock generator and the sequencer, and (b) the memory.

3.3 Analog Circuits

The Amplitude Shift Keying modulator in the RFID is shown in Fig. 5. S_O is the series output of memory. When S_O = 1, the upper transmission gate is enabled, M_{Out} is equals to the AC signal coupled from the inductive coil. If S_O = 0, the lower transmission gate is enabled, M_{Out} is equals to ground. The amplitude modulated data is then transmitted to the reader through the inductive coil.

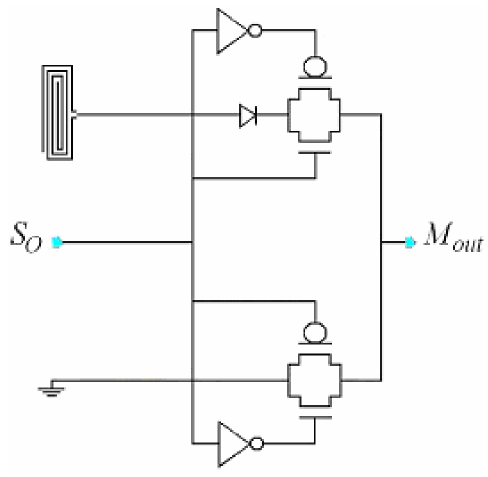


Fig.5. The ASK modulator.

3.4 Parameters Variation

The features of transistors may vary with the variation of semiconductor process. According to the deviation of process, there are three models, i.e. Slow, Typical, and Fast, for NMOS and PMOS. In order to make sure the circuit can work under any process variation, we must consider the performance of circuit under the condition of SS, SF, TT, FS, and FF model. Besides that, we must also consider the circuit stabilization under different temperature or the working voltage has +/-10% variation.

We monitor the output voltage levels of sequencer (A_1、A_2、A_3、A_4) and ASK modulator (S_O、M_{out}). Either in the condition of SS, SF, TT, FS, and FF model, or the working voltage has +/-10% variation, or the temperature is 0 ℃~ 85 ℃, the variations of monitor parameters are less than +/-10%. Mean that our chip is a solid design. Finally, the correctness of circuit is verified by DRC (Design Rule Check) and LVS (Layout vs. Schematic Check). Table 2 lists the main specifications of this low frequency passive RFID transponder.

Table 2 The main specifications of the RFID transponder.

Condition	Specification
Process	TSMC 0.35μm 2P4M
Working voltage	5V
Consuming power	17.25 mW
Frequency	125 kHz
Modulation	ASK
Power source	Passive
Range	10cm
Privacy protection	Yes

4 Conclusion

In this paper, a low-frequency passive RFID transponder with Privacy Protection Circuit is presented. The poly fuse in PPC can be burn out when the function of transponder must be disabled. The broken fuse can not be repaired, thus the transponder is non-revivable and personal privacy can be fully protected. Based on the 0.35 μm 2P4M process provided by the TSMC and Chip Implementation Center (CIC), the whole chip area is 1390 μm × 750 μm.

Acknowledgments

The authors would like to thank the National Science Council for financial support under grants NSC 94-2213-E-159-007.

References:

[1] S. Srinivasan, Akshai Aggarwai, and Anup Kumar, "RFID security and privacy concerns," *WSEAS Transactions on Communication*, Vol. 5, Issue 2, 2006, pp. 296 - 301.

[2] Xingxin Gao, Zhe Xiang, Hao Wang, Jun Shen, Jian Huang, and Song Song, "An approach to security and privacy of RFID system for supply chain," *IEEE International Conference on E-Commerce Technology for Dynamic E-Business*, 2004, pp. 164 - 168.

[3] T. Phillips, T. Karygiannis, and R. Huhn, "Security standards for the RFID market," *IEEE Security & Privacy Magazine*, Vol. 3, Issue 6, 2005, pp. 85 - 89.

[4] Ulrich Kaiser and Wolfgang Steinhagen, "A low power transponder IC for high performance identification systems," *IEEE Journal of Solid-State Circuits*, Vol. 30, No. 3, 1995, pp. 306-310.

[5] Jari-Pascal Curty, Norbert Joehl, Catherine, and Michel J. Declercq, **"**Remotely powered addressable UHF RFID integrated system,**"** *IEEE Journal of Solid-State Circuits*, Vol. 40, No. 11, 2005, pp. 2193-2202.

[6] Qiuting Huang and M. Oberle, "A 0.5-mW passive telemetry IC for biomedical applications," *IEEE Journal of Solid-State Circuits*, Vol. 33, 1998, pp. 937-946.

[7] Steve C. Q. Chen and Valerie Thomas, "Optimization of inductive RFID technology," *IEEE Electronics and Environment Proceeding*, 2001, pp. 82-87.

[8] W. Jeon, J. Meingailis, and R. W. Newcomb, "CMOS passive rfid transponder with read-only memory for low cost fabrciation," *IEEE International SOC Conference*, 2005, pp179-184.

[9] U. Karthaus and M. Fischer, "Fully integrated passive UHF RFID transponder IC with 16.7μW minimum RF input power," *IEEE Journal of Solid-State Circuits*, Vol. 38, No. 10, 2003, pp. 1602-1608.

[10] Jung-Hyun Cho, Suk-Byung Chai, Chung-Gi Song, Kyung-Won Min, and Shiho Kim, **"**An analog front-end IP for 13.56MHz RFID interrogators,**"** *IEEE Design Automation Conference*, Vol. 2, 2005, pp. 1208-1211.

[11] M. C. Cheng, "Design of 8-bit thermal-to-digital converter in CMOS technology," *Thesis of National Chiao Tung University*, 2005.