Encrypted Tag Design for RFID Systems

Shida Yu
Department of Electrical Engineering and Automation
Luoyang Institute of Science and Technology
Luoyang, China
8617603872355
857940118@163.com

ABSTRACT: The wireless implantable RFID tag combines wireless communication technology, medical sensor technology, and data conversion technology to achieve continuous detection of body indicators. The implantable tag system includes a small signal detection circuit, a readout circuit to complete sensor data acquisition and conversion, and a digital baseband and RF front end to perform communication with an external reader. The digital baseband processor handles communication protocols, controls communication flow, configures the RF front end, and controls the sampling of human body data by the ADC, which is a key component of the implantable tag system.

Based on the 13.56MHz ISO15693 radio frequency identification protocol, this paper designs and implements an encrypted tag baseband. Through the analysis of the protocol and the application requirements of the tag, the system architecture of the digital baseband is formulated. Subsequently, the functional logic was verified using Cadence’s Incisive EDA tool and synthesized using Synopsys’ EDA synthesis tool Design Compiler. The simulation results show that the logic function is correct. The synthesis tool report shows that under the 0.13um process, timing closures. The setup time and hold time meet the requirements.

1. INTRODUCTION

1.1 RFID system security issues.
RFID systems are composed of three key components:
• The RFID tag, or transponder, carries object identifying data.
• The RFID tag reader, or transceiver, reads and writes tag data.
• The back-end database stores records associated with tag contents

1.1.1 Tags
Every object to be identified in an RFID system is physically labeled with a tag. Tags are typically composed of a microchip for storage and computation, and a coupling element, such as an antenna coil for communication. Tags may also contain a contact pad, as found in smart cards. Tag memory may be read-only, write-once read-many or fully rewritable.

1.1.2 Readers
Tag readers interrogate tags for their data through an RF interface. To provide additional functionality, readers may contain internal storage, processing power or connections to back-end databases. Computations, such as cryptographic calculations, may be carried out by the reader on behalf of a tag.
1.1.3 Back-End Database

Readers may use tag contents as a look-up key into a back-end database. The back-end database may associate product information, tracking logs or key management information with a particular tag. Independent databases may be built by anyone with access to tag.[1]

As you can see from the above introduction, each electronic tag usually contains an integrated circuit, which is essentially a microchip with memory. The security of data on electronic tags and the security of data on computers are also threatened. When an unauthorized party enters an authorized reader, it still sets a reader to communicate with a particular electronic tag, and the data of the tag is attacked. In this case, an unauthorized user can read the data on the electronic tag like a legitimate reader. On writable tags, data may even be modified or even deleted by illegal users.

1.2 Development status of RFID technology at home and abroad

The development of RFID technology abroad is also relatively early. Especially in the United States, the United Kingdom, Germany, Sweden, Switzerland, Japan, and South Africa, there are relatively mature and advanced RFID systems. According to different operating frequencies, RFID tags can be classified into low frequency (LF), high frequency (HF), ultra-high frequency (UHF) and ultra-high frequency (SHF). Among them, the low-frequency close-range RFID system is mainly concentrated in the 125KHz and 13.56MHz systems; the high-frequency long-distance RFID system is mainly concentrated in the UHF band (902MHz-928MHz) 915MHz, 2.45GHz, 5.8GHz. Long-range RFID systems in the UHF band have been well developed in North America; European applications have gained more applications with active 2.45 GHz systems. The 5.8 GHz system has mature active RFID systems in Japan and Europe[2].

China's research on RFID technology has also developed rapidly, and market cultivation has begun to bear fruit. More typical is the introduction of a remote automatic identification system with independent intellectual property rights in the construction of automatic identification system for railway numbers in China. After years of on-site operation test, the railway number automatic identification system project was fully invested in construction in 1999. After two years of construction and trial operation, the current railway number automatic identification system project has played a system design function, which has fulfilled the dream of railway people, and its role in radiation and penetration into other applications has become increasingly apparent. In the field of close-range RFID applications, many cities have implemented bus RF cards as prepaid electronic tickets, prepaid electronic rice cards and other applications. In terms of RFID technology research and product development, China has already developed the technical capabilities and system integration capabilities of self-developed low-frequency, high-frequency and microwave RFID electronic tags and readers. The gap between advanced RFID technologies and foreign RFID technology is mainly reflected in the technology of RFID chips. Despite this, in the design and development of tag chips, there have been many successful low-frequency RFID system tag chips available in China. However, there is still much room for development based on the function and research of the baseband control circuit of the RFID chip.

1.3 The research of this paper

This paper mainly deals with the tag of high frequency passive HF RFID system based on ISO15693 protocol. A new set of encrypted 13.56MHz high frequency RFID tag chip system is proposed for the security problem of RFID tag system. The system supports the tag part of the RFID system with encryption function based on the ISO 15693 international standard protocol, using advanced RF circuit design and embedded microcontroller, combined with efficient data processing technology[3].

2. DESIGN INTRODUCTION

The tag portion of the RFID system designed in this paper mainly includes a baseband module and an encryption module.
2.1 Baseband Module
The digital baseband is mainly responsible for the processing of digital signals, and its functions are summarized into three functions: decoding, instruction processing and encoding. Introduced below:

2.1.1 Decoding
After receiving the instruction from the reader (electromagnetic wave signal), the tag converts the demodulated signal into a digital signal and transmits it to the baseband through the analog front end. At this time, the signal is recognized by the tag, that is, it is determined what instruction it is, What kind of operation is performed, what data is included, etc., and decoding is required first. Therefore, the signal first enters the decoding module when it enters the digital baseband.

2.1.2 CRC Check
The signal received by the tag from the reader may be erroneous due to various factors during the transmission. In order to verify the correctness of the instruction, the decoded data in the baseband is checked for correctness.

2.1.3 Instruction Analysis
After the CRC check is correct, the baseband will analyze it. First, according to the first byte of the instruction, the relevant format of the tag to return instruction is analyzed, such as single/double load wave, data transfer rate and the like. Then, according to the second byte of the instruction, the type of the instruction is resolved, and the corresponding operation module is entered according to different instruction types.

2.1.4 Anti-collision Handling
When a reader communicates with an electronic tag, it is prone to a situation where multiple tags enter the active field of the reader at the same time, when the reader sends a query command to the tag, if multiple tags return to the reader at the same time The unique identifier (UID), due to the superposition and interference of the electromagnetic wave signal, the reader cannot get the correct return signal. The anti-collision module in the tag is to solve the problem that when the reader interrogates multiple tags, the tag also returns signals at the same time. The anti-collision module is responsible for calculating the order in which the tags of different UIDs are returned to the reader, so that the plurality of tags can sequentially return signals to the reader in an orderly manner, so that the reader receives and processes the signals one by one.[4]

2.1.5 Access EEPROM
After the baseband analyzes the instructions, different operations are performed according to different types of instructions, such as reading data blocks, writing data blocks, etc., essentially performing read/write operations on the EEPROM. According to the instruction, after the corresponding read/write operation of the EEPROM is successful, the corresponding information will be returned.

2.1.6 State transition
The baseband switches the tag to the corresponding working state according to different types of state transition instructions.

2.1.7 Coding
After the instruction in the baseband is executed, the corresponding information will be returned to the reader, and the completion or error information of the reader instruction will be fed back, thereby realizing the interaction of information once. In the encoding module, the baseband encodes the instructions that return the tag to the reader, and then passes it to the analog front end, which is sent through the antenna. Each tag needs to store certain information to be recognized as a specific object to be recognized by the reader. Currently, more non-volatile memory EEPROMs are used. It not only stores
the user’s information, such as the origin, price, etc. of a certain product, but also stores the information of the tag itself, such as the unique identifier (UID) of the tag. When the corresponding read/write instruction arrives, the tag baseband reads and writes the EEPROM as needed.

2.2 Cryptographic Module
In order to prevent the tag from being read by an illegal user, we added the operating mode of this module. In this mode, tags cannot make predictable responses to queries from unauthorized users. The implementation of this module is divided into hash lock and hash unlock.

2.2.1 Hash lock protocol:
A tag owner locks tags by first selecting a key at random, then computing the hash value of the key. The hash output is designated as the metaID.

The tag owner will then store the metaID on the tag and toggle it into a locked state. Writing the metaID may occur either over the RF interface or over a physical contact channel for added security. Upon receipt of a metaID value, the tag enters its locked state. While locked, a tag responds to all queries with only its metaID and offers no other functionality.

Finally, the tag owner will store the key and metaID in a back-end database, indexed on the metaID.

2.2.2 Hash unlock protocol:
To unlock a tag, the owner first queries the metaID from the tag and uses this value to look up the key in a back-end database. The owner transmits this key value to the tag, which hashes the received value and compares it to the stored metaID. If the values match, then the tag unlocks itself and offers its full functionality to any nearby readers.

To prevent hijacking of unlocked tags, they should only be unlocked briefly to perform a function before being locked again.

This unlocking protocol is summarized and illustrated in Figure 1.

![Figure 1 A reader unlocks a hash-locked tag](image)

3. SIMULATION AND DESIGN COMPILE

3.1 Simulation
Anti-collision handling is an essential feature of RFID systems. When there are multiple tags entering the effective field of the reader at the same time, and the reader sends a query command to the tag, if multiple tags return a unique identifier (UID) to the reader at the same time, due to the superposition and interference of the electromagnetic wave signals, the reader cannot get the correct return signal. It is a key feature so that we must verify it. So in our testbench, we instantiate five tag modules to ensure the necessary conditions for conflicts. At the same time, in our test and test platform, a Reader was also instantiated. It randomly reads one of the five tags.

The hierarchy of the testbench is as follow:
The wave of the simulation is as follow:

In the text file, the “?” means that there is a collision. But it only appears in the head or tail and the data is not interrupted. According to the above analysis, the collision has been avoided.

3.2 Design Compile
After we finished the RTL, we use the Design Compiler of Synopsys to compile our RTL. The tag in this paper is composed with eight blocks: ClkBck, InBlcok, MainBlcok, MemBlock, RndBlock, HashBlock, RWMBlock and OutputBlock. The MainBlock is the control block, which provide all the control of the tag. And RndBlock is the randomize block, which make up the cryptographic module with the HashBlock.
4. CONCLUSION AND FUTURE WORK
In this paper, we designed an encrypted tag design for RFID systems according to the hash-lock protocol. The tag design is compatible with ISO15693. After finishing the RTL, we use the EDA tools to simulate the function and compile the design to check out that the logic function is correct and the timing is closure.

In the future work, we will optimize the design, which includes less area and lower power. In addition, we will add some feature. For example, we will make our tag design be able to control the ADC to simple voltage, which can be used in the human implantable chip.

References
[1] OHTA H, IZUMI S, YOSHIMOTO M. A more acceptable endoluminal implantation for remotely monitoring ingestible sensors anchored to the stomach wall[J]. Conference proceedings: ... Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual Conference, 2015, 2015: 4089–4092.
[2] XIAO Z, TAN X, CHEN X et. al. An Implantable RFID Sensor Tag toward Continuous Glucose Monitoring[J]. IEEE journal of biomedical and health informatics, 2015, 19(3): 910–919.
[3] DEHENNIS A D, MAILAND M, GRICE D et.al. A near-field-communication (NFC) enabled wireless fluorimeter for fully implantable biosensing applications[C]//2013 IEEE International Solid-State Circuits Conference Digest of Technical Papers. 2013: 298–299.
[4] DEHENNIS A, GETZLAFF S, GRICE D et.al. An NFC-Enabled CMOS IC for a Wireless Fully Implantable Glucose Sensor[J]. IEEE journal of biomedical and health informatics, 2016, 20(1): 18–28.
[5] WEIS S A. Security and Privacy in Radio-Frequency Identification Devices[J]. : 79.