江南大学

JIANGNAN UNIVERSITY

物联网工程学院

无线射频识别技术课程作业

高频 RFID 标签和读写器芯片的结构与功能分析

——以复旦微电子 FM13HS02 芯片和 FM17550 芯片为例

班　　级：物联 1601

组　　长：纪港

组　　员：尹达恒、郭星宇、孙硕、孙瑜博、王雷

指导老师：孙子文

2018~2019 第二学期

2019 年 3 月 27 日

目录

1 高频 RFID 射频识别系统硬件结构简介

一个完整的 RFID 系统通常由标签 (Tag or Transponder) 、阅读器 (Interrogator or Reader) 和数据管理系统组成。标签一般包含天线、调制/解调器、编码/解码器以及储存器或微控制器等单元；阅读器由天线、射频收发模块和控制单元组成, 其中控制模块通常包含放大器、解码和纠错电路、微处理器、时钟电路、标准接口以及电源电路等 [1]。

1.1 电子标签的硬件结构简介

电子标签的硬件结构按照功能可以划分为三个主要部分：天线、模拟前端（射频前端）和控制电路（如图 1）。电子标签中的射频信号调制器和解调器包含于模拟前端中，编码/解码器、储存器或微控制器等单元包含于控制电路中。电子标签工作时，其天线接收由读写器发出的信号，该信号通过射频前端电路中的解调器和解码器等部件的处理，进入电子标签的控制电路，由控制电路对数据流做各种逻辑处理，再经过射频前端的编码和调制发送到读写器。依照控制电路的结构，电子标签可分为不可编程电子标签和可编程电子标签。

不可编程电子标签的控制电路硬件结构包括地址和安全逻辑形成电路、IO 寄存器和存储器等部分。其中地址和安全逻辑电路是控制电路的主要部分，它控制整个芯片的处理进程，并且和专用 IO 寄存器互相配合完成数据交换、授权、加密及密匙管理等功能。存储器主要包括 ROM、EEPROM 或 FRAM，ROM 主要存放永久数据，EEPROM 或 FRAM 连接芯片内部逻辑电路的地址线和数据线进行数据交换。电子标签的工作受存储器中的程序控制，控制程序一旦确定就被固定在芯片存储器中，不能改变 [2]。

可编程电子标签的控制电路硬件结构除存储器外还包括一个微控制器。微控制器可以运行微操作系统程序，控制电子标签的数据转换、接收、发送、命令控制、文件管理及加密算法等。在芯片的制作阶段操作系统程序写在 ROM 存储器中，成为芯片的一部分。可编程电子标签可以按照读写器的指令对标签中的非易失性存储器进行读写，改变标签的发回读写器的输出从而达到可编程的目的 [3]。一些可编程标签还能对电子标签中的存储信息进行散列 (Hash) 等加密算法计算后存储，以防止标签伪造。

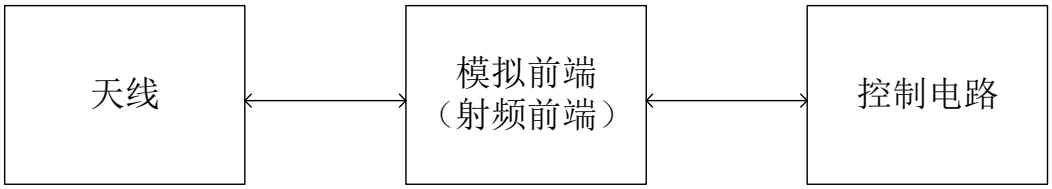

图 1. 电子标签的硬件结构（按功能划分）

1.2 读写器的硬件结构简介

读写器的硬件结构包括射频电路模块和基带电路模块。射频电路模块除了产生高频信号激活电子标签，给电子标签提供能量外，还包括两个独立的收发通道，其中发射通道将按照协议编好的基带信号进行调制并通过天线发送给电子标签，接收通道接收和解调电子标签反馈的微弱的反向散射高频信号并将高频信号还原成基带信号。基带电路由微处理器专用集成电路 (Application Specific Integrated Circuit,ASIC) 模块构成。ASIC 模块专门处理信号的调制和解调等任务。基带电路实现与应用软件通信，完成信号采集处理、运算、编码、解码和校验，执行反碰撞协议算法，对读写器与电子标签之间收发数据进行认证、加密和解密等。应用软件与基带电路之间数据交换可通过 USB、RS232、485 和以太网等接口，基带电路输出到射频接口的信号是二进制数字信号，而经过射频电路的调制，输出到天线的信号一般是二进制数字信号经过 ASK 或 PSK 调制的模拟信号。

2 高频 RFID 射频识别标签芯片分析——复旦微电子 FM13HS02

2.1 芯片简介

FM13HS02 是复旦微电子公司开发的符合 ISO/IEC15693 协议的 ITAG 系列高频安全电子标签芯片之一，具较好的射频性能和射频兼容性，保证了更远的操作距离和更可靠的读写。FM13HS02 芯片提供了较大容量数据存储空间，内置国家商用密码算法 SM7，支持安全鉴别和安全通信。FM13HS02 芯片具有物理不可克隆功能 (PUF)，并创新性的将 PUF 与 SM7 算法相结合，显著提升了算法实现的安全性。FM13HS02 芯片具有物理唯一性和高安全性的特点，可广泛应用于高值物资管理、防伪溯源、证件、会议通行证等领域。

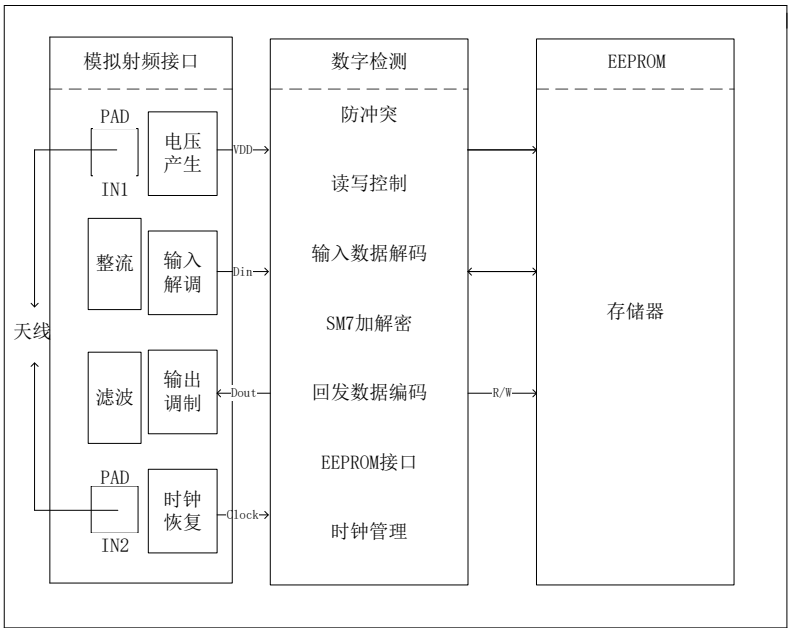

图 2. 复旦微电子 FM13HS02 芯片结构图

2.2 硬件结构

FM13HS02 芯片由模拟射频电路、数字逻辑电路和存储器三部分组成，属于不可编程电子标签，读写器与芯片间的射频接口符合 ISO/IEC 15693-2 和 ISO/IEC 15693-3，其整体结构框图如图 2所示：

- 模拟射频接口：模拟射频接口即该标签芯片的射频前端，负责接收天线中传来的读写器信号、提取能量、解调读写器信号以及激活并维持系统时钟脉冲、接收并调制数字信号通过天线完成数据回发。
- 数字检测电路：数字检测电路是该芯片的主要功能部件。数字逻辑电路负责执行防冲突算法、完成射频前端输入信号的解码、数据的加密和解密、控制对 EEPROM 的读写、对回发数据的编码以及控制系统时钟。
- 非易失性存储器 (EEPROM)：提供高可靠的数据存储。

2.3 关键技术分析

2.3.1 ISO/IEC 15693 标准

ISO/IEC 15693 是一种短距离非接触式 IC 卡数据协议标准，该标准规定了读取距离可达一米的非接触 IC 卡的功能及运作模式，使用的频率为 13.56MHz，数据传输速率的一般上限是 53Kb/s 或者 26.5Kb/s，采用轮寻机制、分时查询的方式完成防冲突过程。

该标准设计简单，生产读取器的成本比 ISO/IEC 14443 低，应用场景多为开放式会议签到、考勤等。

2.3.2 国家商用密码算法

为了保障商用密码的安全性，国家商用密码管理办公室制定了一系列密码标准 [4]，包括 SM1（SCB2）、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法（ZUC) 等。其中 SM1、SM4、SM7、祖冲之密码（ZUC）是对称算法；SM2、SM9 是非对称算法；SM3 是哈希算法。目前，这些算法已广泛应用于各个领域中。其中 SM1、SM7 算法不公开，仅以 IP 核的形式存在于芯片中，使用该算法时，一般通过加密芯片的接口进行调用。

FM13HS02 芯片所使用的 SM7 算法是一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特 [5]。SM7 适用于非接触式 IC 卡，应用包括身份识别类应用 (门禁卡、工作证、参赛证)，票务类应用 (大型赛事门票、展会门票)，支付与通卡类应用（积分消费卡、校园一卡通、企业一卡通等）。

2.3.3 物理不可克隆技术

物理不可克隆技术 (Physical Unclonable Function,PUF) 利用了芯片制造过程中注入和光照等工序的随机工艺偏差，产生芯片的唯一“指纹”信息，经特殊技术提取后，可作为芯片的唯一标识信息。该唯一标识由于是制造过程中自行产生，芯片的设计者、制造者、生产者均无法对其进行控制，保证了防伪芯片的物理不可复制特性。

芯片为保证自身安全性，需内置加密算法，加密算法除了保证数学上的逻辑安全性以外，还需能抵抗暴力破解攻击、侧信道攻击、重放攻击等各种攻击手段，以避免自身存储的密钥被泄露出去。防护手段的强弱与设计复杂度直接相关，而 RFID 防伪芯片由于其应用环境的特殊性，难以启用复杂的抗攻击设计来

保护其内置的密码算法，导致芯片的安全等级下降 [6]。而 FM13HS02 芯片中使用 PUF 技术提取的“指纹”信息，利用了自然环境中普遍存在的物理扰动，具有较好的随机特性，利用该随机特性，可产生随机 PUF KEY [7]，与 SM7 密码算法相结合，可显著提升密码算法的抗攻击性能和安全等级 [8]。

3 高频 RFID 射频读写器芯片分析——复旦微电子 FM17550

3.1 芯片简介

FM17550 是一款高度集成的工作在 13.56MHz 下的非接触通讯芯片，支持以下 3 种不同的工作模式。

- 支持符合 ISO/IEC 14443 TypeA 协议的读写器模式
- 支持符合 ISO/IEC 14443 TypeB 协议的读写器模式
- 支持符合 ISO/IEC 14443A 协议的卡片模拟工作模式

同时提供了低功耗的外部卡片侦测功能，方便电池供电、需要低功耗工作、并且需要实时处理任意时刻会进入射频场的外部卡片的读写器设备。FM17550 具有低电压、低功耗、驱动能力强、多接口支持、多协议支持等特点。适用于低功耗、低电压、低成本要求的非接触读写器应用。

3.2 硬件结构

FM17550 芯片由主机接口控制器、控制寄存器组、FIFO 缓冲器和芯片主控制器组成，其结构整体框图如图 3所示，各部分功能如下：

- 主机接口控制器 (Host Interface Control)：用于控制芯片与主机的数据交换支持 SPI、UART、I2C 三种连接方式，所有的接口在上电硬复位之后自动完成接口方式的侦测。
- 控制寄存器组 (Control Register Bank)：包含用于控制芯片各种功能的寄存器单元。
- 8*64 位 FIFO 缓冲器 (FIFO,codec,Receiver,Transmitter)：用于主控芯片与内部状态机之间的输入输出数据流的缓冲。图中的 codec,Receiver,Transmitter 三者负责缓冲器与该缓冲器与内部状态机之间的数据交换。该缓冲器对于最长 64 字节的数据流控制非常方便，使数据传输时无需考虑交互时序。

- 芯片主控制器 (Control Engine)：芯片主控制器是 FM17550 芯片的核心部件，负责控制和协调芯片的大部分处理过程。主控制器又可以分成下列功能单元：
  - 加密单元 (Encryption Unit)：加密单元在读写器模式下负责数据的 M1 加密；
  - CRC 协处理器 (CRC Co-prosesscer)：用于对数据进行 CRC 校验；
  - 中断控制器 (Interrupt Control)：处理系统中断信号，控制芯片的中断；
  - 时钟和 reset 控制器 (Clock/reset control)：用于维持稳定的系统时钟以及控制芯片重启；
  - 可编程定时器 (Programable timer)：内置的 Timer 计时单元，主控芯片可以利用该计时器进行计时相关的任务，支持超时计数器、看门狗计数器、秒表、可编程脉冲输出、周期性脉冲触发功能；
  - 电源控制器 (Power Manage Unit)：用于控制芯片各组件的电源供应，除支持正常功耗模式外还支持三种低功耗模式，Deep power down 模式 (DPD)、Hard power down 模式 (HPD) 和 Soft power down 模式 (SPD)。其中，SPD 模式下，芯片内部逻辑进入低功耗状态，关闭晶振；HPD 模式关闭大部分数字逻辑的供电、关闭晶振，并使所有双向 IO 引脚都控制为三态输出，输入引脚隔离与内部电路的连接；DPD 模式在 HPD 模式的基础上进一步关闭所有数字逻辑的供电，使系统能耗尽可能降到最低。

FM17550 芯片的 QFN32 封装方式及引脚定义见附录图 4和表 1。

3.3 关键技术分析

3.3.1 ISO/IEC14443 标准

ISO/IEC 14443 标准是一种超短距离非接触式 IC 卡标准，规定了读取距离 7-15 厘米的非接触式 IC 卡的功能及运作方式，使用的频率为 13.56MHz，通信速率为 106kbit/s。

ISO/IEC 14443 定义了 Type A, 和 Type B 两种类型协议，它们的不同主要在于载波的调制深度及位的编码方式：Type A 采用开关键控 (On-Off keying) 的 Manchester 编码，Type B 采用 NRZ-L 的 BPSK 编码。Type B 与 Type A 相比，具

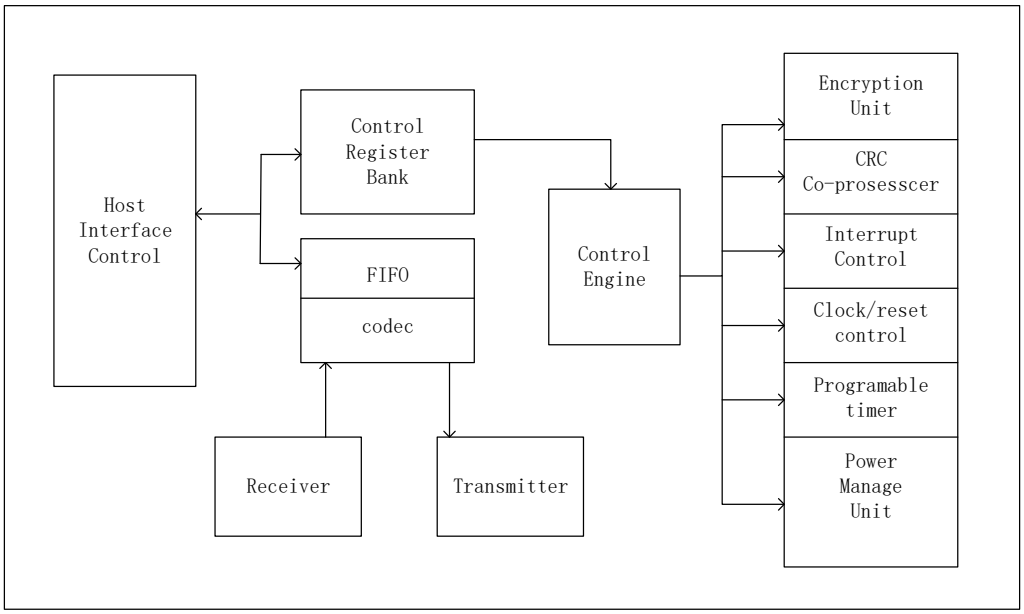

图 3. 复旦微电子 FM17550 芯片结构图

有传输能量不中断、速率更高、抗干扰能力强的优点。Type A 和 Type B 的防冲突机制原理也有所不同：Type A 的防冲突算法基于位冲突检测协议，而 Type B 使用通信系列命令序列完成防冲突过程。

与 ISO/IEC 15693 相比，ISO/IEC 14443 读写距离较近，灵敏度较低，但具有加密功能。ISO/IEC 14443 Type A 协议的应用领域主要有门禁卡、考勤卡、公交卡、一卡通等，而 Type B 协议的加密功能更加完善，主要用于身份证、护照、银联卡等需要高安全性和大容量的场合，目前的第二代电子身份证采用的标准就是 ISO/IEC 14443 Type B 协议。

参考文献

[1] 张晖，王东辉. Rfid 技术及其应用的研究. 微计算机信息, (11):252–254, 2007.

[2] 余雷. 基于 rfid 电子标签的物联网物流管理系统. 微计算机信息, (02):233–235+232, 2006.

[3] 何苏勤，蔡帆. 基于射频无线通信技术的智能车辆出入管理系统设计. 计算机应用研究, (05):208–210, 2005.

[4] 田涛，苏董杰，赫松龄，贾峻，谢文录. 基于国密 sm7 算法的电子标签在防伪中的应用. 中国集成电路, 20(11):70–72, 2011.

[5] 苏董杰. 基于 sm7 国密算法非接触逻辑卡对 mifare 1 门禁系统的升级方案. 中国集成电路, 21(03):80–83, 2012.

[6] 贺章擎，郑朝霞，戴葵，邹雪城. 基于 puf 的高效低成本 rfid 认证协议. 计算机应用, 32(03):683–685+698, 2012.

[7] 郭丽敏，刘丹，王立辉，单伟君，李清. 基于 puf 的 rfid 系统安全密钥协商协议. 微电子学与计算机, 34(07):60–64, 2017.

[8] Srinivas Suh, G Edward，Devadas. Physical unclonable functions for device authentication and secret key generation. In *2007 44th ACM/IEEE Design Automation Conference*, pages 9–14. IEEE.

附录

复旦微电子 FM17550 芯片封装图和引脚定义

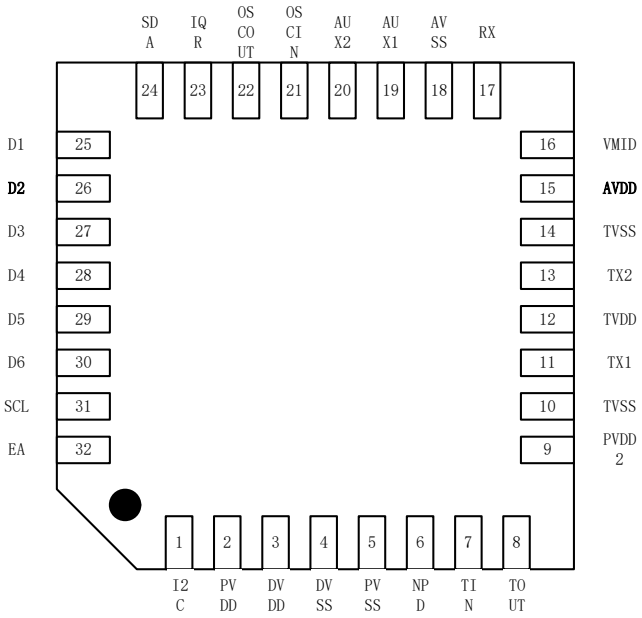

图 4. 复旦微电子 FM17550 芯片封装图

表 1: 复旦微电子 FM17550 芯片引脚定义

引脚序号	引脚名称	类型	引脚说明
1	I2C	I	I2C 总线接口使能
2	PVDD	P	引脚供电
3	DVDD	P	芯片供电
4	DVSS	G	数字地
5	PVSS	G	引脚地
6	NPD	I	复位/休眠（Power Down) 控制脚 电平时内部电路进入 power down 状态 当产生一个上升沿时内部电路复位
7	TIN	I	测试信号输入
8	TOUT	O	测试信号输出
9	PVDD2	P	TIN、TOUT 引脚供电
10	TVSS	G	发射电路地
11	TX1	O	发射输出脚 1
12	TVDD	P	发射电路供电
13	TX2	O	发射输出脚 2
14	TVSS	G	发射电路地
15	AVDD	P	模拟电路供电
16	VMID	P	为部参考电压
17	RX	I	射频输入引脚
18	AVSS	G	模拟地
19	AUX1	O	测试输出 1
20	AUX2	O	测试输出 2
21	OSCIN	I	27.12M 晶振输入，也作外部时钟输入
22	OSCOUT	O	27.12M 晶振输出
23	IRQ	O	中断输出
24	SDA	IO	I2C 总线数据 IO 脚
	NSS	I	SPI 接口使能
	URX	I	UART 接口数据输入
25	D1	IO	测试口
	ADR5	I	12C 总线地址 bit5
26	D2	IO	测试口
	ADR4	I	12C 总线地址 bit4
27	D3	IO	测试口
	ADR3	I	12C 总线地址 bit3
28	D4	IO	测试口
	ADR2	I	12C 总线地址 bit2
29	D5	IO	测试口
	ADR1	I	12C 总线地址 bit1
	SCK	I	SPI 接口时钟输入
	DTRQ	O	UART 请求输出给 mcu
30	D6	IO	测试口
	ADRO	I	12C 总线地址 bit0
	MOSI	I	SPI 接口 master 输出 slave 输入
	MX	O	UART 输出到 mcu
31	SCL	I	12C 总线时钟线
	MISO	O	SPI 接口 master 输入 slave 输出
	UTX	O	UART 接口数据输出
32	EA	I	2C 总线地址模式