

第 3 章 RFID 基础实验

实验 3.1 近距离 ID 卡读取实验

【实验目的】

- (1) 了解 ID 卡的基本原理。
- (2) 熟悉 125kHz 读卡模块的使用方法。

【实验设备】

- (1) 计算机一台。
- (2) RFID 读写器辅助教学工具 RFID_Tool 软件一套。
- (3) 物联网多网技术综合教学开发设计平台一套。

【实验要求】

- (1) 要求：了解 ID 卡的基本原理。
- (2) 实现功能：利用 RFID_Tool, 测试 ID 卡的读取。
- (3) 实验现象：刷卡后, RFID_Tool 显示 ID 卡的卡号。

【实验原理】

ID 卡全称为身份识别卡 (Identification Card), 是一种不可写入的感应卡, 含固定的编号, 主要有中国台湾 SYRIS 的 EM 格式、美国 HID、MOTOROLA 等各类 ID 卡。ID 卡与磁卡一样, 都仅仅使用了“卡的号码”而已, 卡内除了卡号外, 无任何保密功能, 其“卡号”是公开、裸露的。所以说 ID 卡就是“感应式磁卡”。ISO 标准 ID 卡的规格为: $85.6 \times 54 \times 0.80 \pm 0.04\text{mm}$ (高 $\times$ 宽 $\times$ 厚), 市场上也存在一些厚卡、薄卡或异型卡。

ID 卡的工作系统由卡、读卡器和后台控制器组成。工作过程如下:

- (1) 读卡器将载波信号经天线向外发送, 载波频率为 125kHz (THRC12)。
- (2) ID 卡进入读卡器的工作区域后, 由卡中电感线圈和电容组成的谐振回路接收读卡器发射的载波信号, 卡中芯片的射频接口模块由此信号产生出电源电压、复位信号及系统时钟, 使芯片“激活”。
- (3) 芯片读取控制模块将存储器中的数据经调相编码后调制在载波上经卡内天线回送给读卡器。

- (4) 读卡器对接收到的卡回送信号进行解调、解码后送至后台计算机。
- (5) 后台计算机根据卡号的合法性,针对不同应用做出相应的处理和控制。

本实验箱配置 125kHz 读卡模块。读卡模块接口为 UART 接口(19200 波特率),当有卡靠近模块天线时,模块会以 UART 方式输出 ID 卡的卡号,用户仅需简单地读取即可,该读卡模块完全支持 EM、TK 及其兼容卡片的操作,125kHz 读卡模块和 ID 卡如图 3.1 所示。

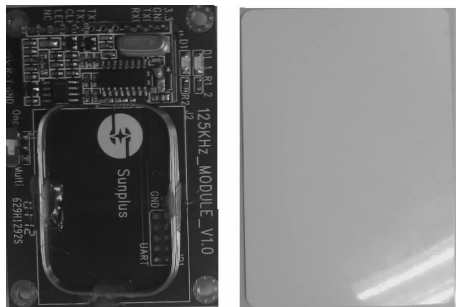


图 3.1 125kHz 读卡模块和 ID 卡

数据通信协议如下:

- UART 接口一帧的数据格式为 1 个起始位、8 个数据位、无奇偶校验位、1 个停止位。
- 输出波特率为 19 200bps。
- 数据格式: 5 字节数据,高位在前,格式为 4 字节数据+1 字节校验(异或和)。例如,卡号数据为 12345678,则输出 0x12 0x34 0x56 0x78 0x08(异或和计算: $0x12 \oplus 0x34 \oplus 0x56 \oplus 0x78 = 0x08$),当有卡进入该射频区域内时,主动发出以上格式的卡号数据。

【实验步骤】

- (1) 将计算机串口通过串口线连接到开发板的串口 VB1,将实验箱“ARM 选通”开关选择到“计算机”端,如图 3.2 所示。
- (2) 双击打开 RFID_Tool 软件(可在清华大学出版社网站下载,路径为物联网基础实践教学\Tools\RFID 调试助手),打开的界面如图 3.3 所示。



图 3.2 选择串口和计算机相连



图 3.3 RFID_Tool 主界面

- (3) 选择当前计算机的串口号(默认为 COM1),RFID 读写器类型选 125kHz,然后单击“打开”按钮,打开该串口,如图 3.4 所示。
- (4) 刷一下 125kHz 卡片,则 RFID_Tool 界面将会显示该卡的卡号,如图 3.5 所示。



图 3.4 125kHz 测试界面



图 3.5 刷卡后显示的卡号

【范例路径】

本书提供了本实验的参考程序,可在清华大学出版社网站下载,下载后文件路径如下:
物联网基础实践技术\TOOLS\RFID 调试助手

实验 3.2 IEEE 14443 寻卡实验

【实验目的】

- (1) 了解 IC 卡的基本原理。

- (2) 了解 IEEE 14443 标准。
- (3) 熟悉 13.56MHz 读卡模块的使用方法。
- (4) 熟悉 IEEE 14443 寻卡的方法。

【实验设备】

- (1) 计算机一台。
- (2) RFID 读写器辅助教学工具 RFID_Tool 软件一套。
- (3) 物联网多网技术综合教学开发设计平台一套。

【实验要求】

- (1) 要求：了解 IC 卡的基本原理。
- (2) 实现功能：利用 RFID_Tool, 测试 IC 读卡模块的寻卡功能。
- (3) 实验现象：刷卡后, RFID_Tool 应显示 IC 卡的卡号。

【实验原理】

1. IC 卡简介

IC 卡全称集成电路卡(Integrated Circuit Card), 又称智能卡(Smart Card)。可读写容量大, 有加密功能, 数据记录可靠, 使用更方便, 如一卡通系统、消费系统等, 目前主要有 PHILIPS 的 Mifare 系列卡。IC 卡是继磁卡之后出现的又一种新型信息工具。IC 卡是指集成电路卡, 一般用的公交车卡就是 IC 卡的一种, 一般常见的 IC 卡采用射频技术与 IC 卡的读卡器进行通信。IC 卡与磁卡是有区别的, IC 卡是通过卡里的集成电路存储信息, 而磁卡是通过卡内的磁力记录信息。IC 卡的成本一般比磁卡高, 但保密性更好。主要用于公交、轮渡、地铁的自动收费系统, 也应用在门禁管理、身份证明和电子钱包。

2. IEEE 14443 标准简介

目前我国常用的 RFID 标准为用于非接触智能卡的两个 ISO 标准: ISO 14443 和 ISO 15693。ISO 14443 和 ISO 15693 标准在 1995 年开始操作, 其完成则是在 2000 年之后, 二者皆以 13.56MHz 交变信号为载波频率。ISO 15693 读写距离较远, 而 ISO 14443 读写距离稍近, 但应用较广泛。目前的第二代电子身份证采用的标准是 ISO 14443 TYPE B 协议。ISO 14443 定义了 TYPE A、TYPE B 两种类型协议, 通信速率为 106kbps, 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)的曼切斯特编码, TYPE B 采用 NRZ-L 的 BPSK 编码。TYPE B 与 TYPE A 相比, 具有传输能量不中断、速率更高、抗干扰能力强的优点。RFID 的核心是防冲撞技术, 这也是和接触式 IC 卡的主要区别。ISO 14443-3 规定了 TYPE A 和 TYPE B 的防冲撞机制。二者防冲撞机制的原理不同, 前者是基于位冲撞检测协议, 而 TYPE B 通信系列命令序列完成防冲撞。ISO 15693 采用轮寻机制、分时查询的方式完成防冲撞机制。防冲撞机制使得同时处于读写区

内的多张卡的正确操作成为可能,既方便了操作,也提高了操作的速度。

3. IC 卡的工作原理

射频读写器向 IC 卡发一组固定频率的电磁波,卡片内有一个 LC 串联谐振电路,其频率与读写器发射的频率相同,这样在电磁波激励下,LC 谐振电路产生共振,从而使电容内有了电荷。在这个电荷的另一端,接有一个单向导通的电子泵,将电容内的电荷送到另一个电容内存储,当所积累的电荷电压达到 2V 时,此电容可作为电源为其他电路提供工作电压,将卡内数据发射出去或接受读写器的数据。

4. 本实验箱配置的 13.56MHz 读卡模块简介

读写模块采用 13.56MHz 非接触射频技术,内嵌低功耗射频基站 MFRC522。用户不必关心射频基站的复杂控制方法,只需通过简单地选定 UART 接口发送命令就可以实现对卡片完全的操作。该系列读写模块支持 Mifare One S50、S70、FM11RF08 及其兼容卡片,该模块及相应的 IC 卡片如图 3.6 所示。

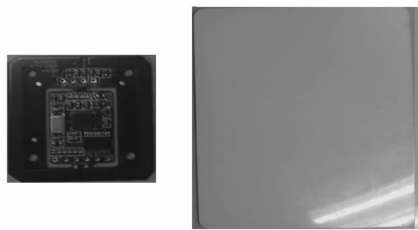


图 3.6 13.56MHz 读卡模块和 IC 卡

5. 数据通信协议

异步半双工 UART 格式:一帧的数据格式为 1 个起始位,8 个数据位,无奇偶校验位,1 个停止位。

波特率为 19 200bps。

(1) 发送数据封包格式如下所示。

数据包帧头 02	数据包内容	数据包帧尾 03
----------	-------	----------

注意: 0x02、0x03 被使用为起始字符、结束字符,0x10 被使用为 0x02、0x03 的辨识字符。因此在通信的传输数据之中(起始字符 0x02,至结束字符 0x03 之中)的 0x02、0x03、0x10 字符之前,皆必须补插入 0x10 作为数据辨识之用。例如起始字符 0x02,至结束字符 0x03 之中有一原始数据为 0x020310,补插入辨识字符之后,将变更为 0x100210031010。

数据包内容:

模块地址	长度字	命令字	数据域	校验字
------	-----	-----	-----	-----

- 模块地址:对于单独使用的模块来说固定为 0x0000。对网络版模块来说为 0x0001~0xFFFE。0xFFFF 为广播。
- 长度字:指明从长度字到校验字的字节数。
- 命令字:本条命令的含义。
- 数据域:该条命令的内容,此项可以为空。
- 校验字:从模块地址到数据域最后一字节的逐字节累加值(最后一字节)。

(2) 返回数据封包格式与发送数据封包格式相同。

数据包内容：

模块地址	长度字	接收到的命令字	执行结果	数据域	校验字
------	-----	---------	------	-----	-----

- 模块地址：对于单独使用的模块来说固定为 0x0000；对网络版模块来说为本身的地址。
- 长度字：指明从长度字到数据域最后一字节的字节数。
- 命令字：本条命令的含义。
- 执行结果：0x00 表示执行正确；0x01—0xFF 表示执行错误。
- 数据域：该条命令的内容，返回执行状态和命令内容。
- 校验字：从模块地址到数据域最后一字节的逐字节累加值（最后一字节）。

6. 寻卡实验所需的命令

(1) 寻卡指令如表 3.1 所示。

表 3.1 寻卡指令

命令字	发送数据域	正 确 返 回	错误返回
0x46	1 字节寻卡模式 model=0x26 为寻未进入休眠状态的卡 model=0x52 寻所有状态的卡	2 字节 TagType(返回卡类型值) pTagType:0x0400=Mifare_One(S50) 0x0200=Mifare_One(S70)	非 0

(2) 防冲突指令如表 3.2 所示。

表 3.2 防冲突指令

命令字	发送数据域	正确返回	错误返回
0x47	1 字节 bcnt(说明：bcnt=0x04)	4 字节卡序列号	非 0

(3) 选卡指令如表 3.3 所示。

表 3.3 选卡指令

命令字	发送数据域	正确返回	错误返回
0x48	4 字节卡序列号	1 字节卡容量	非 0

(4) 密钥验证指令如表 3.4 所示。

表 3.4 密钥验证指令

命令字	发送数据域	正确返回	错误返回
0x4A	1 字节密钥验证 model+1 字节绝对块号+6 字节密钥 说明：1 字节密钥验证模式：model=0x60 为验证 A 密钥，model=0x61 为验证 B 密钥	0x00	非 0

【实验步骤】

(1) 计算机串口通过串口线连接到开发板的串口 VB2,注意实验箱“ARM 选通”开关选

- 择到“计算机”端,如图 3.2 所示。
- (2) 双击打开 RFID_Tool 软件(见本书配套资料“物联网基础实践技术\TOOLS\RFID 调试助手”),如图 3.3 所示。
- (3) 选择当前计算机的串口号(默认为 COM1),RFID 读写器类型选 13.56MHz,然后单击“打开”按钮,打开该串口,如图 3.7 所示。



图 3.7 13.56MHz 测试界面

- (4) 将 13.56MHz 卡片放置到 13.56MHz 读卡模块的上方。
- (5) 依次单击“13.56M 控制”下的“1. 寻卡”、“2. 防冲突”、“3. 选卡”、“4. 密钥验证”按钮,结合通信协议观察“数据包监视器”中的数据以及相应的操作是否成功,如图 3.8 所示。

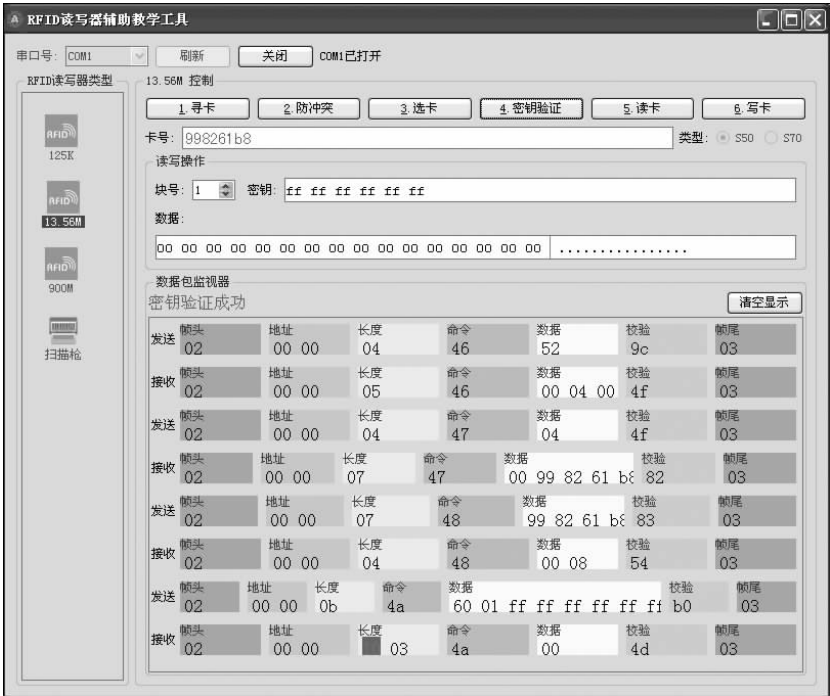


图 3.8 RFID_Tool 寻卡实验

【范例路径】

本书提供了本实验的参考程序,可在清华大学出版社网站下载,下载后文件路径如下:

物联网基础实践技术\TOOLS\RFID 调试助手

实验 3.3 IEEE 14443 写入标签数据实验

【实验目的】

- (1) 熟悉 S50 卡的存储结构。
- (2) 熟悉 13.56MHz 读卡模块的使用方法。
- (3) 熟悉 IEEE 14443 写数据的方法。

【实验设备】

- (1) 计算机一台。
- (2) RFID 读写器辅助教学工具 RFID_Tool 软件一套。
- (3) 物联网多网技术综合教学开发设计平台一套。

【实验要求】

- (1) 要求:了解 IEEE 14443 写数据的方法。
- (2) 实现功能:利用 RFID_Tool,测试 IC 读卡模块的写数据功能。
- (3) 实验现象:写数据后,RFID_Tool 显示“写入数据成功”。

【实验原理】

1. S50 卡存储结构

S50 非接触式卡符合 MIFARE I 的国际标准,容量为 8Kb,数据保存期为 10 年,可改写 10 万次,读无限次。S50 卡不带电源,自带天线,内含加密控制逻辑电路和通信逻辑电路,卡与读写器之间的通信采用国际通用的 DES 和 RES 保密交叉算法,具有极高的保密性能。

M1 卡分为 16 个扇区,每个扇区由 4 块(块 0、块 1、块 2、块 3)组成,16 个扇区的 64 个块通常按绝对地址编号为 0~63,S50 卡存储结构如图 3.9 所示。

第 0 扇区的块 0(即绝对地址 0 块),它用于存放厂商代码,已经固化,不可更改。

每个扇区的块 0、块 1、块 2 为数据块,可用于存储数据。

每个扇区的块 3 为控制块,包括了密码 A、存取控制、密码 B。



图 3.9 S50 卡存储结构

2. 写标签数据命令

写标签数据命令如表 3.5 所示。

表 3.5 写标签数据命令

命令字	发送数据域	正确返回	错误返回
0x4C	1 字节绝对块号+16 字节要写入的数据说明： S50 块号(0~63) S70 块号(0~255)	0x00	非 0

【实验步骤】

- (1) 将计算机串口通过串口线连接到开发板的串口 VB2,注意实验箱“ARM 选通”开关选择到“计算机”端如图 3.2 所示。
- (2) 双击打开 RFID_Tool 软件,如图 3.3 所示。
- (3) 选择当前计算机的串口号(默认为 COM1),RFID 读写器类型选“13.56M”,然后单击“打开”按钮,打开该串口,如图 3.7 所示。
- (4) 将 13.56MHz 卡片放置到 13.56MHz 读卡模块的上方。
- (5) 依次单击“13.56M 控制”下的“1. 寻卡”、“2. 防冲突”、“3. 选卡”、“4. 密钥验证”按钮,观察“数据包监视器”下方显示“密钥验证成功”,密钥验证成功后便可对 IC 卡进行写操作,如图 3.8 所示。
- (6) 在软件“读写操作”下选择块号,填入卡的 6 字节密钥(默认全为 0xFF),单击“13.56M 控制”下的“6. 写卡”按钮,结合通信协议观察“数据包监视器”中的数据。

【范例路径】

本书提供了本实验的参考程序,可在清华大学出版社网站下载,下载后文件路径如下:

物联网基础实践技术\TOOLS\RFID 调试助手

实验 3.4 IEEE 14443 读取标签数据实验

【实验目的】

- (1) 熟悉 S50 卡的存储结构。
- (2) 熟悉 13.56MHz 读卡模块的使用方法。
- (3) 熟悉 IEEE 14443 读取标签数据的方法。

【实验设备】

- (1) 计算机一台。
- (2) RFID 读写器辅助教学工具 RFID_Tool 软件一套。
- (3) 物联网多网技术综合教学开发设计平台一套。

【实验要求】

- (1) 要求:了解 IEEE 14443 读取标签数据的方法。
- (2) 实现功能:利用 RFID_Tool,测试 IC 读卡模块的读数据功能。
- (3) 实验现象:写数据后,RFID_Tool 显示“读取数据成功”。

【实验原理】

1. S50 卡存储结构

存储结构请参照实验 3.3。

2. 读标签数据命令

读标签数据命令如表 3.6 所示。

表 3.6 读标签命令

命令字	发送数据域	正确返回	错误返回
0x4B	1 字节绝对块号 说明: S50 块号(0~63);S70 块号(0~255)	16 字节读出的数据	非 0

【实验步骤】

(1) 将计算机串口通过串口线连接到开发板的串口 VB2,注意实验箱“ARM 选通”开关选择到“计算机”端如图 3.2 所示。

(2) 双击打开 RFID_Tool 软件(见本书配套资料“Tools\RFID 调试助手”),如图 3.3 所示。

(3) 选择当前计算机的串口号(默认为 COM1),RFID 读写器类型选“13.56M”,然后单击“打开”按钮,打开该串口,如图 3.7 所示。

(4) 将 13.56MHz 卡片放置到 13.56MHz 读卡模块的上方。

(5) 依次单击“13.56M 控制”下的“1. 寻卡”、“2. 防冲突”、“3. 选卡”、“4. 密钥验证”按钮,观察“数据包监视器”下方显示“密钥验证成功”,密钥验证成功后便可对 IC 卡进行写操作,如图 3.8 所示。

(6) 在软件“读写操作”下选择块号,填入卡的 6 字节密钥(默认全为 0xFF),单击“13.56M 控制”下的“5. 读卡”按钮,读取成功后,软件“数据”一栏会显示读取到的 16 字节数据。

(7) 结合通信协议观察“数据包监视器”中的数据。

【范例路径】

本书提供了本实验的参考程序,可在清华大学出版社网站下载,下载后文件路径如下:

物联网基础实践技术\TOOLS\RFID 调试助手

实验 3.5 UHF 900M 识别单个标签实验

【实验目的】

- (1) 了解 UHF 900M 的基本概念。
- (2) 了解 UHF 900M 读写器的通信协议。
- (3) 熟悉 UHF 900M 读写器读取单标签的方法。

【实验设备】

- (1) 计算机一台。
- (2) RFID 读写器辅助教学工具 RFID_Tool 软件一套。
- (3) 物联网多网技术综合教学开发设计平台一套。

【实验要求】

- (1) 要求:了解 UHF 900M 的基本概念及单标签识别的方法。

(2) 实现功能：利用 RFID_Tool,测试 900MHz 模块的单标签识别功能。

(3) 实验现象：刷卡后,RFID_Tool 显示 900MHz 标签的 12 字节卡号。

【实验原理】

1. UHF 900M 读写器简介

UHF (Ultra High Frequency) 是指超高频。UHF 900M 读写器指工作在 902 ~ 928MHz 频段的一类远距离读卡设备。本实验箱配置的 900MHz 读写器读取距离为 0 ~ 2m,最大功耗 5W,支持 ISO-18000-6C(EPC G2)或 ISO-18000-6B 协议,支持单卡读取和多卡读取,具备 Wiegand26\34\42、RS-232、RS-485 数据接口。

2. 通信帧格式介绍

(1) 命令帧格式(数据流通方向：主机→读写器)如表 3.7 所示。

表 3.7 命令帧格式

Packet Type	Length	Command Code	Device Number	Command Data	Checksum
0xA0	N+3	1 byte	1 byte	N byte	1 byte

- Packet Type 是包类型域,命令帧包类型固定为 0xA0。
- Length 是包长域,表示 Length 域后帧中字节数。
- Command Code 是命令码域。
- Device Number 是设备号域。当设备号为 00 时,表示群发。
- Command Data 是命令帧中的参数域。
- Checksum 是校验和域,规定校验范围是从包类型域到参数域最后一个字节为止所有字节的校验和。读写器接收到命令帧后需要计算校验和来检错。

(2) 读写器命令完成响应帧格式(数据流通方向：读写器→主机)如表 3.8 所示。

表 3.8 响应帧格式

Packet Type	Length	Command Code	Device Number	Status	Checksum
0xE4	0x04	1 byte	1 byte	1 byte	1 byte

Status 是状态域。状态域表明读写器完成计算机命令后读写器的状态或执行命令后的结果,其规定如表 3.9 所示。

表 3.9 状态域

序号	值	名称	描述
1	0x00	ERR_NONE	命令成功完成
2	0x02	CRC_ERROR	CRC 校验错误
3	0x10	COMMAND_ERROR	非法命令
4	0x01	OTHER_ERROR	其他错误

(3) 读写器发送的信息帧格式(数据流通方向: 读写器→主机)如表 3.10 所示。

表 3.10 信息帧格式

Packet Type	Length	Response Code	Device Number	Response Data	Checksum
0xE0	N+3	1 byte	1 byte	N byte	1 byte

3. 单标签读取命令

单标签读取命令如表 3.11 所示。

主机发送命令。

表 3.11 单标签读取命令

Packet Type	Length	Command Code	Device Number	Checksum
A0	03	82	00	DB

例如,主机发送命令 A0 03 82 00 DB 后,识别失败回:

(E4 04 82)头,(00)usercode,(05)Status ,(91)Checksum

识别成功回:

(E0 10 82)头,(00)usercode ,(01)天线号(12 34 00 00 00 00 00 00 00 00 10)ID,

(37)Checksum

【实验步骤】

(1) 将计算机串口通过串口线连接到开发板的串口 VB3,注意实验箱“ARM 选通”开关选择“计算机”端,如图 3.2 所示。

(2) 双击打开 RFID_Tool 软件(见本书配套资料“TOOLS\RFID 调试助手”),如图 3.3 所示。

(3) 选择当前计算机的串口号(默认为 COM1),RFID 读写器类型选“900M”,然后单击“打开”按钮,打开该串口,如图 3.10 所示。



图 3.10 “900M” 测试界面

(4) 单击“读写器设置”选项卡,如图 3.11 所示,依次选中读卡模式下面的“EPC 读单卡”以及工作模式下面的“主从模式”,然后单击“应用设置”按钮。



图 3.11 “读写器设置”选项卡

(5) 切换到“标签识别”选项卡,将 900MHz 卡片放置到天线的上方。

(6) 单击“EPC 标签识别”按钮,则卡片的 12 字节卡号就会显示在“卡号列表”一栏,如图 3.12 所示。



图 3.12 卡片识别成功

(7) 对照通信协议,查看软件“记录”一栏的发送和接收的数据。

【范例路径】

本书提供了本实验的参考程序,可在清华大学出版社网站下载,下载后文件路径如下:

物联网基础实践技术\TOOLS\RFID 调试助手

实验 3.6 UHF 900M 识别多个标签实验

【实验目的】

- (1) 了解 UHF 900M 的基本概念。
- (2) 熟悉 UHF 900M 读写器多标签识别的方法。

【实验设备】

- (1) 计算机一台。
- (2) RFID 读写器辅助教学工具 RFID_Tool 软件一套。
- (3) 物联网多网技术综合教学开发设计平台一套。

【实验要求】

- (1) 要求：了解多标签识别的方法。
- (2) 实现功能：利用 RFID_Tool,测试 900MHz 模块的多标签识别功能。
- (3) 实验现象：多张卡放入 900MHz 读卡模块的天线区域内,RFID_Tool 会读取到这些卡的卡号。

【实验原理】

- (1) 复位命令
复位命令如表 3.12 所示。

表 3.12 复位命令

Packet Type	Length	Command Code	Device Number	Checksum
A0	03	65	00	F8

- Packet Type 是包类型域,命令帧包类型固定为 0xA0。
- Length 是包长域,表示 Length 域后帧中字节数。
- Command Code 是命令码域,多标签读取命令码为 0x65。
- Device Number 是设备号域。当设备号为 00 时,表示群发。
- Checksum 是校验和域,规定校验范围是从包类型域到 Device Number 为止所有字节的校验和。读写器接收到命令帧后需要计算校验和来检错。

读写器收到此命令帧后,先返回命令完成帧,然后读写器复位。

例如,主机发送命令 A0 03 65 00 F8 后,从机返回:

E4 04 65 usercode Status Checksum。

当 Status 为 00 时表示成功;Status 为其他值时表示失败。

(2) 多标签读取命令

主机发送命令格式如表 3.13 所示。

表 3.13 读取多标签命令(主机发送)

Packet Type	Length	Command Code	Device Number	Checksum
A0	03	FC	00	61

- Packet Type 是包类型域,命令帧包类型固定为 0xA0。
- Length 是包长域,表示 Length 域后帧中字节数。
- Command Code 是命令码域,多标签读取命令码为 0xFC。
- Device Number 是设备号域。当设备号为 00 时,表示群发。
- Checksum 是校验和域,规定校验范围是从包类型域到 Device Number 为止所有字节的校验和。读写器接收到命令帧后需要计算校验和来检错。

例如,主机发送命令 A0 03 FF 00 5 后,成功则返回:

E0 04 FC 00 00 20 00 00 66 66 53 82 82 13 00 51 06 00 00 13 01 5F FF 00 00 99 99 99 99 99 99 99 00 00 29 9F 01 6F FF

其中: 66 66 53 82 82 13 00 51 06 00 00 13、99 99 99 99 99 99 99 99 00 00 29 9F 为 ID 号。

(3) 设置单个读写器参数

主机发送命令如表 3.14 所示。

表 3.14 设置单个读写器参数命令(主机发送)

Packet Type	Length	Command Code	Device Number	Parameter address(MSB)	Parameter address(LSB)	Parameter value	Checksum
A0	06	60	00	1 byte	1 byte	1 byte	1 byte

- Packet Type 是包类型域,命令帧包类型固定为 0xA0。
- Length 是包长域,表示 Length 域后帧中字节数。
- Command Code 是命令码域,设置单个读写器参数的命令码为 0x60。
- Device Number 是设备号域。当设备号为 00 时,表示群发。
- Parameter address(MSB) 参数地址高字节。
- Parameter address(LSB) 参数地址低字节。
- Parameter value 要设置的参数值。
- Checksum 是校验和域,规定校验范围是从包类型域到 Parameter value 为止所有字节的校验和。读写器接收到命令帧后需要计算校验和来检错。

读写器接收到此命令帧后,将需要设置的参数写入 EEPROM 中,并返回命令完成帧。

例如,主机发送命令 A0 06 60 00 00 65 96 FF(设置功率)后。从机返回:

(E4 04 60)头,(00)usercode(00)Status,(B8)Checksum。

当 Status 为 00 时表示成功,为其他值时表示失败。

(4) 读写器 EEPROM 参数,如表 3.15 所示。

表 3.15 EEPROM 参数

参数在 EEPROM 中地址(十六进制)	参数含义	设置操作的有效值	数值含义解释	其 他
0x65	发射功率	0~150	功率模拟量	
0x70	读写器读卡操作发生模式	1,2,3	1: 主从工作模式 2: 定时工作模式 3: 触发工作模式	注意: 工作在模式 2、3 时, 主从模式仍然有效
0x71	读卡时间间隔	N 为 10~100	读卡时间间隔(N×10)ms	读写器读卡操作发生模式为 2、3 时有效
0x72	读卡器读取到数据后主动发送数据的链路选择	1,2,3	1: RS485 链路 2: wiegand 链路 3: RS232 链路	
0x87	单标签和多标签标别	0,1	0: EPC 单标签识别 1: EPC 多标签识别	

注: 上述地址在命令中使用两个字节, 由于上述字节仅一个字节范围, 所以在实际使用时, 命令中的高位字节填写 0。在上述命令完成后, 需要使得读写器使用新的参数工作必须重启读卡器(使用复位命令)。

【实验步骤】

- (1) 将计算机串口通过串口线连接到开发板的串口 VB3, 注意实验箱“ARM 选通”开关选择“计算机”端, 如图 3.2 所示。
- (2) 双击打开 RFID_Tool 软件(见本书配套资料“Tools\RFID 调试助手”), 如图 3.3 所示。
- (3) 选择当前计算机的串口号(默认为 COM1), RFID 读写器类型选“900M”, 然后单击“打开”按钮, 打开该串口, 如图 3.10 所示。
- (4) 单击“读写器设置”选项卡, 如图 3.13 所示。依次选中读卡模式下面的“EPC 读多卡”和工作模式下面的“定时模式”, 数据报告接口选择“默认串口”, 然后单击“应用设置”按钮。

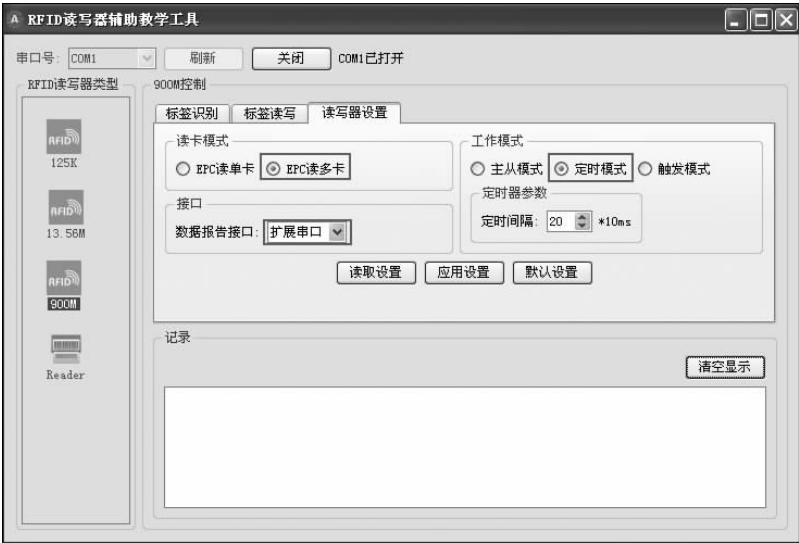


图 3.13 “读写器设置”选项卡

(5) 切换到“标签识别”选项卡,将多个 900MHz 卡片放置到天线的上方则“卡号列表”一栏,将会显示识别到的 900MHz 卡片的卡号,如图 3.14 所示。



图 3.14 多卡识别

(6) 单击“EPC 标签识别”按钮,则卡片的 12 字节卡号就会显示在“卡号列表”一栏,如图 3.15 所示。



图 3.15 卡片识别成功

(7) 读写器配成“EPC 读多卡”及“定时模式”后,按钮“复位”和“重新识别”具有相同的作用,即读取天线区域内的 900MHz 卡片的卡号。单击“重新获取数据”按钮,可将读卡器缓冲区中的所有数据再次发送到串口。

(8) 对照通信协议,查看软件“记录”一栏的发送和接收的数据。

【范例路径】

本书提供了本实验的参考程序,可在清华大学出版社网站下载,下载后文件路径如下:

物联网基础实践技术\TOOLS\RFID 调试助手

实验 3.7 IEEE 18000 读取标签数据实验

【实验目的】

- (1) 了解 900MHz 标签内部数据区域。
- (2) 熟悉读取 900MHz 标签数据的方法。

【实验设备】

- (1) 计算机一台。
- (2) RFID 读写器辅助教学工具 RFID_Tool 软件一套。
- (3) 物联网多网技术综合教学开发设计平台一套。

【实验要求】

- (1) 要求: 读取标签数据。
- (2) 实现功能: 利用 RFID_Tool,测试 900MHz 模块的读取标签数据功能。
- (3) 实验现象: 读取成功后,显示读取的数据。

【实验原理】

1. 900MHz 标签内部数据区域简介

- 数据区域: 有保留区(保留)、EPC 区(电子产品代码)、TID 区(标签识别号)、用户区。4 个独立的存储区块用途如表 3.16 所示。

表 3.16 数据区域

MemBank	区块名称	用 途
00	保留区	存储 Kill Password(灭活口令)和 Access Password(访问口令)
01	EPC	存储 EPC 号码
10	TID	存储标签识别号码,每个 TID 号码应该是唯一的
11	用户区	存储用户定义的数据

- 地址：当选择“保留区”时，范围为 0~3。当选择 EPC 区时，范围为 2~7。当选择用户区时，范围为 0~31。
- 长度：保留区地址从 0~3。EPC 区地址从 2 至 7，单位是字（1 字=2 字节）。

2. 标签读取命令

标签读取命令如表 3.17 所示。

表 3.17 标签读取命令

Packet Type	Length	Command Code	Device Number	MemBank	Addr	Read Length	Checksum
A0	06	80	00	1 字节	1 字节	1 字节	1 字节

- Packet Type 是包类型域，命令帧包类型固定为 0xA0。
- Length 是包长域，表示 Length 域后帧中字节数。
- Command Code 是命令码域，标签读取命令码为 0x80。
- Device Number 是设备号域。当设备号为 00 时，表示群发。
- MemBank 是当前要读取的数据区域。
- Addr 是要读取的数据地址。
- Read Length 是要读取的数据长度。
- Checksum 是校验和域，规定校验范围是从包类型域到 Read Length 为止所有字节的校验和。读写器接收到命令帧后需要计算校验和来检错。

例如：主机发送命令：A0 06 80 00 01 02 01 D6；表示从 0x02 地址开始起，读取 1 个字（两个 BYTE）的数据。

【实验步骤】

- （1）将计算机串口通过串口线连接到开发板的串口 VB3，注意，实验箱“ARM 选通”开关应选择“计算机”端，如图 3.2 所示。
- （2）双击打开 RFID_Tool 软件，如图 3.3 所示。
- （3）选择当前计算机的串口号（默认为 COM1），RFID 读写器类型选“900M”，然后单击“打开”按钮，打开该串口，如图 3.10 所示。
- （4）单击“标签读写”选项卡，如图 3.16 所示。
- （5）将 900MHz 卡片放置到天线的上方。
- （6）单击“读卡”按钮，则读取的数据会显示在“数据”一栏中，如图 3.17 所示。
- （7）更改要读取的卡的“区号”、“地址”以及“长度”，观察现象。
- （8）对照通信协议查看软件“记录”一栏的发送和接收的数据。

【范例路径】

本书提供了本实验的参考程序，可在清华大学出版社网站下载，下载后文件路径如下：

物联网基础实践技术\TOOLS\RFID 调试助手