实验三 IEEE14443 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 IEEE14443 读取标签内数据的方法

【实验设备】

1. 安装有 RFID_Tool 的 PC 机一台
2. 实验箱一台
3. 公-母串口线一条
4. 14443 协议白卡若干

【实验要求】

1. 要求：了解 IEEE14443 读取数据的方法。
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：读数据后，RFID_Tool 显示“读取数据成功”，同时显示读取到的数据。

【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 8K 位，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讯逻辑电路，卡与读写器之间的通讯采用国际通用的 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，（我们也将 16 个扇区的 64 个块按绝对地址编号为 0~63，S50 卡存储结构如图 7.11所示：

图 7.11 S50 卡存储结构

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，可用于存贮数据。

每个扇区的块 3 为控制块，包括了密码 A、存取控制、密码 B，一般情况下不要修改。

2. 读标签数据命令如表 7.4所示

表 7.4 读卡命令

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. 将实验箱左侧的SW5 开关拨至“PC”一侧，并使用串口线将实验箱左侧标有“13.56MHZ”的VB3 串口座与PC机的串口相连，如图 7.12所示；

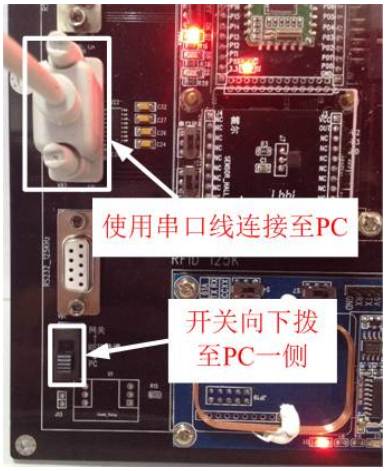

图 7.12 13.56MHz读写器硬件连接

2. 在实验箱配套光盘的“Tools\RFID调试助手”文件夹下找到RFID_Tool.exe软件，并双击打开，如图 7.13所示；

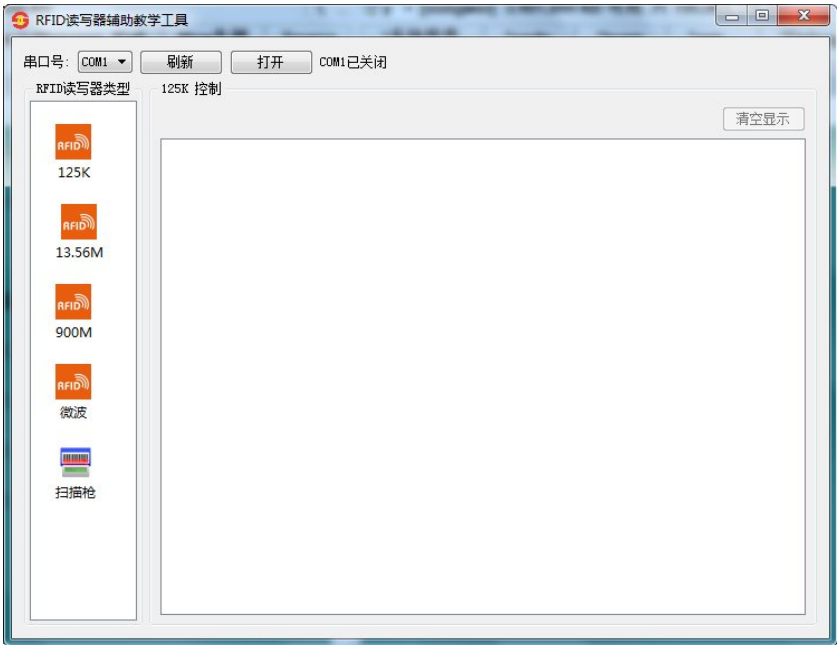

图 7.13 RFID_Tool软件

3. 选择当前电脑的串口号（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 7.14所示：

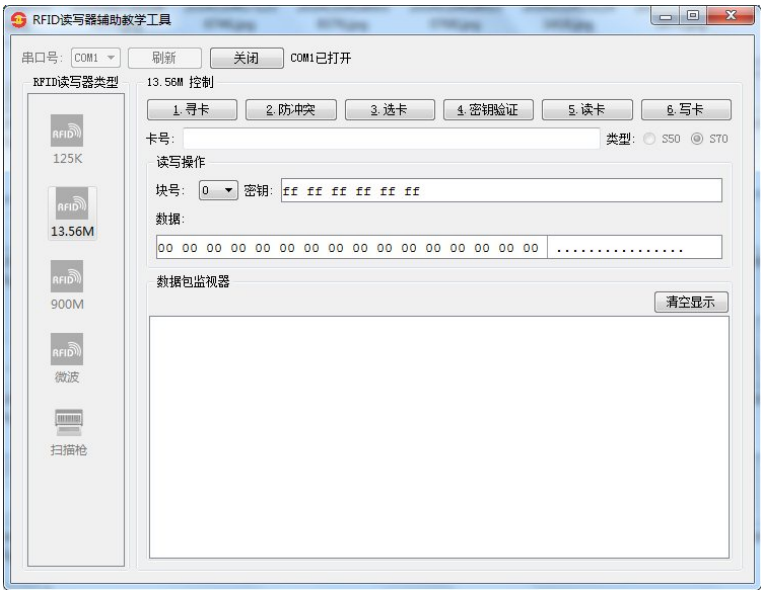

图 7.14 13.56M测试界面

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，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 7.15所示：

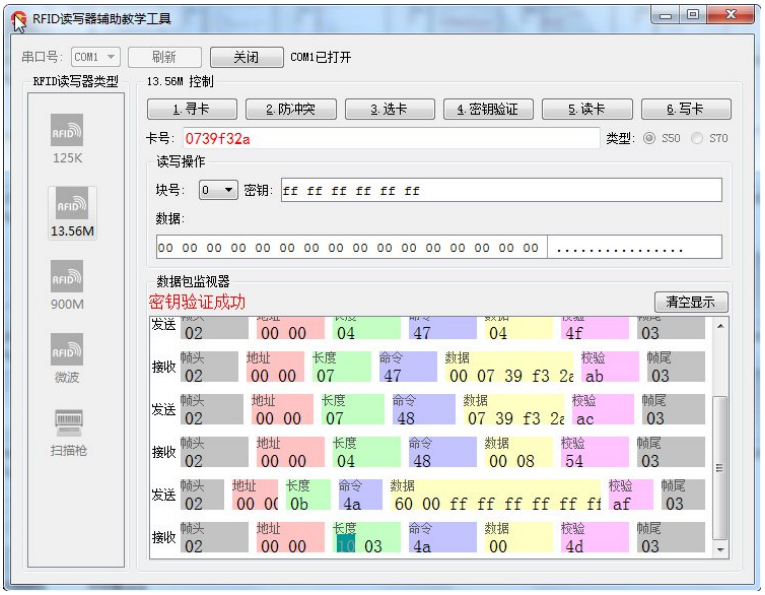

图 7.15 RFID_Tool寻卡实验

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】

本实验用到的软件位于实验箱配套光盘的：

Tools\RFID 调试助手\RFID_Tool V3.0