原 ID卡复制教程(使用T5577卡复制4100卡)

2017年07月16日 12:58:14 TonnyBrown 阅读数：29778 标签： RFID ID卡 ID卡复制 T5577 EM4100

1 ID卡的常见类型与区别

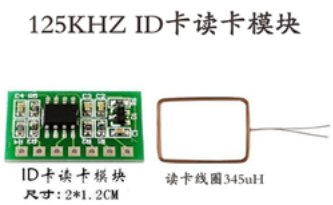
国内常见的普通ID卡多为EM 4100 或 EM 4102卡，其特点是不可修改ID号。为了复制普通ID卡，通常采用T5577 或 EM4305卡（俗称ID白卡），其特点是内EEPROM可读可写，修改卡内EEPROM的内容即可修改卡片对外的ID号，达到复制普通ID卡的目的。

本文以**T5577**卡复制普通**EM4100**卡。读者需具备基本的电子DIY能力。

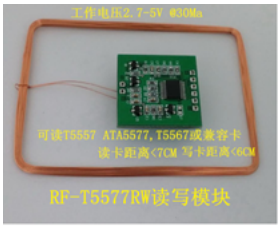
多说一句，ID卡和IC卡是不一样的哦，本文只针对ID卡，绝大多数ID卡卡面会有一串数字，如果没有数字可能是IC卡哦，本文就不适用了。

2 硬件准备

A. ID卡读卡模块，用于读取待复制ID卡的卡号，某宝售价10元左右。



B. T5577卡读写模块，用于读取或写入ID号到T5577卡，某宝低于20元。



C.T5577空白卡

D.USB转串口TTL模块（10元以下）（懒得放图了）

3 ID卡号介绍

标准EM ID卡号（曼彻斯特内码）由10位16进制数组成，例如：

7200944C78

其中**7**为版本代码，**2**为客户代码，**00944C78**为**ID代码**

曼彻斯特内码 **不在卡面标注**，卡面常见标注为以下两种形式：

而此卡面所标注的卡号分别为**ABA**码（0009718904） 和 **wiegand26**码（148，19576）：

如图所示的**ABA**码由**ID代码**转换为10进制所得，即：

（**00944C78**）16 → （**0009718904**）10

如图所示的**wiegand26**码由ID代码倒数5、6位和后4位分别换算成10进制组成，即：

（**94，4C78**）16 → （**148，19576**）10

综上所述：只有曼彻斯特内码（**7200944C78**）包含了完整的ID卡号信息，因此下文中所述的卡号、ID号如无特别说明均为10位16进制**曼彻斯特内码**。

4 使用ID卡读卡模块读取ID号

由第3节可知：虽然ID卡卡面会包含"ID号"，但其信息并不完整，只有通过ID读卡器才能读出完整的曼彻斯特内码。

通过USB转串口TTL模块连接电脑和ID卡读卡模块，注意连接TXD和RXD交叉，使用**串口调试助手**读取ID号。读取ID的过程比较简单，详情可以参考模块手

（这里如果有时间的话会放一张硬件连接图）

5 向T5577空白卡写入ID号（原创内容）

ID号码只是一串16进制数，而T5577卡可以储存大量的数据，只有将ID号码按照指定格式写入T5577后，T5577才能起到原卡的作用。

5.1普通ID卡中的ID号

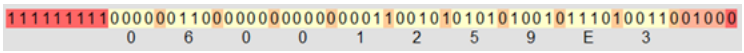
EM4100卡能够存储64bits数据，只可读**不可写**，其数据格式如下：

1	1	1	1	1	1	1	1	1	9 bit header bits, all 1's
8 bit version number or customer ID.				D00	D01	D02	D03	P0	
				D04	D05	D06	D07	P1	
32 Data Bits				D08	D09	D10	D11	P2	Each group of 4 bits is followed by an Even parity bit
				D12	D13	D14	D15	P3	
				D16	D17	D18	D19	P4	
				D20	D21	D22	D23	P5	
				D24	D25	D26	D27	P6	
				D28	D29	D30	D31	P7	
				D32	D33	D34	D35	P8	
				D36	D37	D38	D39	P9	
4 column Parity bits				PC0	PC1	PC2	PC3	S0	1 stop bit (0)

EM4100卡与RFID读卡器的交互过程中，按照以上数据格式循环传输，连续9个1表示一次传输的开始，每组5位中最后一位（P0~P9）是偶校验（每组5位中为偶数个），在进行数据校验的同时，确保了不会出现连续9个1与传输开始标志冲突。PC0~PC3位为列校验位，S0位停止位。

以下为一次传输的数据情况，该卡的卡号（曼彻斯特内码）为：

06001259E3



如果我们能像4100卡一样向读卡器发送上面64bit数据，即可达到复制ID卡的目的。

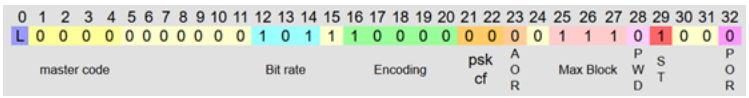
5.2 T5577空白卡

英文原文：http://www.priority1design.com.au/t5557_rfid_transponder.html

T5577能够储存330bits的数据，可读可写，其数据格式如下：

page	lock bit	data	block address
page 0	L	Configuration Data	Block 0
	L	32 bits Read / Write data	Block 1
	L	32 bits Read / Write data	Block 2
	L	32 bits Read / Write data	Block 3
	L	32 bits Read / Write data	Block 4
	L	32 bits Read / Write data	Block 5
	L	32 bits Read / Write data	Block 6
	L	User Data or password.	Block 7
page 1	1	Traceability Data	Block 1
	1	Traceability Data	Block 2

Block 0为配置块：



The configuration block bits are described in detail in Atmel's T5557 datasheet, see T5557 datasheet. Here is a description of some of the more important configuration bit details.

Bits 16 - 20: Determine the Encoding protocol upon start up. A bit pattern of 10000 selects Manchester Encoding. When data is transmitted from tag to rea data is encoding using this selected scheme. See Data modulation

Bits 12 - 14: Determine the Bit rate of the data transmitted by the transponder to the reader. A bit pattern of 101 selects a bit rate of 64 Field Cycles per bit

Bits 25 - 27: Determine the maximum block address transmitted in standard read mode. For the T5557 RFID transponder this value can be from 0 to 7.

Bit 28: When Set this bit activates the Password mode. In Password mode all blocks need a password to be sent before they can be read or written. The p required is stored in block 7.

这部分就是说"配置块"每一位的含义，有点类似于51单片机配置寄存器的感觉……

当卡片被放入读卡器时，卡片会读取保存在配置块的数据按照配置要求发送数据。然后进入标准读模式。在标准读模式中，卡片从Block1开始发送数据到配到27位定义的Max Block结束，整个发送过程重复进行。

配置块Block 0的默认配置为：000880E8

比特率：RF/32 调制方式：Manchester 最大块：7　PSKCF：RF/2　ST：1

这个默认配置是**不正确**的，EM4100卡的比特率是RF/64，且不使用ST（ST：0）

因此，Page0 Block0应当配置为:**001480E0**（有同学配置成 **00148041**成功了，懒得分析了，只要能用就OK，感谢评论区@hahahwokao）

5.3 T5577写入ID号（核心+原创）

普通ID卡（4100卡）在工作时，会循环发送自身全部64bit数据，这些数据中包含引导帧，ID卡号，行校验，列校验。以ID号：**06001259E3**写入4100卡为例（4100卡不可写，这里只是分析ID号在卡内的储存形式，进而推出应该写入T5577卡的数据）

第一步：写入引导序列和ID卡号

0→0000　6→0110　E→1110　1→0001

1	1	1	1	1	1	1	1	1
				0	0	0	0	
				0	1	1	0	
				0	0	0	0	
				0	0	0	0	
				0	0	0	1	
				0	0	1	0	
				0	1	0	1	
				1	0	0	1	
				1	1	1	0	
				0	0	1	1	
								0

第二步：写入列校验和行校验，最后一个固定为0

1	1	1	1	1	1	1	1	1
				0	0	0	0	0
				0	1	1	0	0
				0	0	0	0	0
				0	0	0	0	0
				0	0	0	1	1
				0	0	1	0	1
				0	1	0	1	0
				1	0	0	1	0
				1	1	1	0	1
				0	0	1	1	0
				0	1	0	0	0

列校验和行校验均为偶校验：每行或每列中"1"的个数为偶数的时候，这个校验位就是"0"，否则这个校验位就是"1"

将上表按数据发送顺序展开，则4100卡最终发送的数据就是：

111111111　000000110000000000000000 （FF818000）

110010101　01010010111010011001000　（CAA974C8）

只要把这64位数据写入T5577的EEPROM中，即可实现ID卡的复制。

page	lock bit	data	block address
	L	Configuration Data	Block 0
	L	32 bits Read / Write data	Block 1
page 0	L	32 bits Read / Write data	Block 2

使用T5577读写模块和配套软件，首先在Block1中写入**FF818000**，在Block2中写入**CAA974C8**即完成了ID号的写入，**最后**在配置块Block0中写入**001480E0**学配置成 **00148041**成功了，懒得分析了，只要能用就OK，感谢评论区@hahahwokao）。此时，T5577卡即可替代原ID卡。