

手持式 125K 射频卡 密码测试复制器 使用说明书

本装置用于 125KHz 射频卡(包括 T5557、EM4305 及其兼容卡)的密码破解和快速复制，用户可根据需求选择不同功能组合，具有体积小、功能完备、操作简便等特点。



特别注意：

只有卡，无法破解密码。破解 IC 卡密码必须将本装置与用卡设备（发卡器和电脑软件）一起使用才可能破解。

如果一张卡（5557 或 4305）不是密码模式，则该卡无密码可解，也不可以用本装置破解。具体说明请参见“3.2”和技术文档 T5557.pdf/EM4305.pdf。

目录

1. 功能与参数	3
1.1 基本功能	3
1.2 选择开放功能	3
1.3 技术参数	3
2. 使用方法	4
2.1 按键功能说明	4
2.2 卡类型测试	4
2.3 T5557 复制	5
2.4 EM4305 复制	7
2.5 T5557 密码破解	9
2.6 EM4305 密码破解	12
2.7 T5557 数据编辑	13
2.8 EM4305 数据编辑	14
2.9 改写带密码的 T5557 卡	16
2.10 改写带密码的 EM4305 卡	17
2.11 远程升级	18
3. 常见问题	19
3.1 关于“无密码读”和“有密码读”	19
3.2 关于卡的加密方式	20
4. 联系我们	20

1. 功能与参数

1.1 基本功能

- ▼自动识别 T5557/EM4305/EM4100 等 125kHz 射频卡；
- ▼可以编辑设置卡的密码、数据、控制字；
- ▼保存所读数据，掉电数据不会丢失；
- ▼用户可根据需求选择不同功能组合，支持不更换硬件远程升级。

1.2 选择开放功能

特别声明：下列功能，未必全部开放。下列功能是否开放，取决于您购买时的付款情况。

此举的目的在于最大限度地减轻您的投资压力。如果您需要新增功能，请与我们联系，付清新增功能的所需款项之后，使用本机的远程升级（UPGRADE）功能（参见 2.9 远程升级）即可远程升级。

- A T5557/T5567/T5577 等兼容卡复制；
- B T5557/T5567/T5577 等兼容卡密码破解；
- C EM4305/EM4205 等兼容卡复制；
- D EM4305/EM4205 等兼容卡密码破解。

1.3 技术参数

- ♣ 卡密码破解时间：与应用系统写卡时间相同
- ♣ 卡复制时间：1s
- ♣ 供电：4 节 AAA 型（7#）电池；3.3V 电源适配器
- ♣ 外形尺寸：162×80×28mm³（长×宽×高）
- ♣ 密码存储：14 组
- ♣ 数据存储：1 张卡完整数据

2. 使用方法

2.1 按键功能说明

ENT: 确认键。切换至下一级菜单, 密码输入完成后确认密码。

DEL: 取消键。返回至上一级菜单。

RST: 复位键。使本机复位重启; 破解状态下按 RST 可退出并查看密码。

FUN: 功能保留。

◀▶: 左、右移动键。输入密码时调整光标的位置。

▲▼: 上、下移动键。菜单模式下切换菜单; 复制模式下, ▼可清零复制计数值, ▲可切换手动/自动复制模式。

0-F: 16 进制数字键。用于数据输入, 密码列表中可通过按数字键将对应密码存入密码编辑器。

2.2 卡类型测试

第一步: 正确连接电源后, 打开侧面的电源开关, 屏幕被点亮, 出现主菜单界面, 进入“图 2.2.1”所示界面。通过按三次移动键“▼”可切换至菜单第二屏。

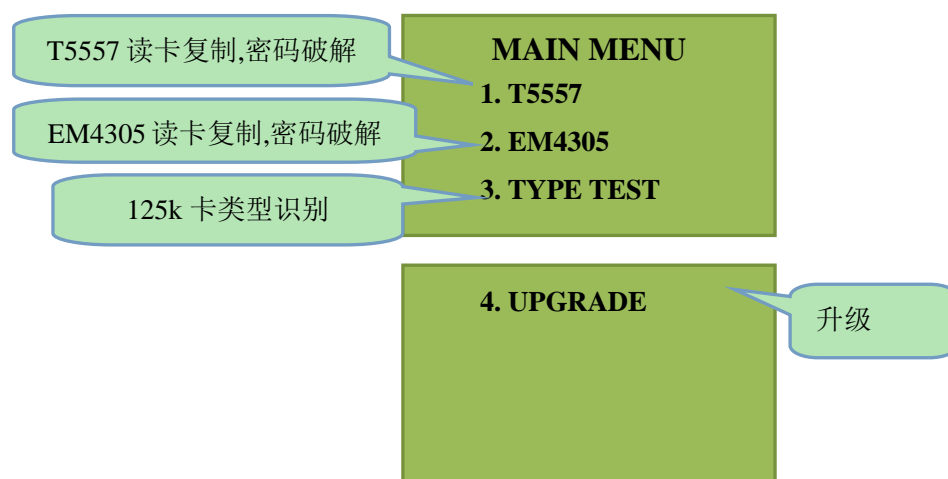


图 2.2.1 主菜单

第二步: 将需要测试的卡片放置于显示屏后面的感应区, 通过▲▼移动键, 移动选单至第三项 **TYPE TEST**, 按 ENT 开始测试。

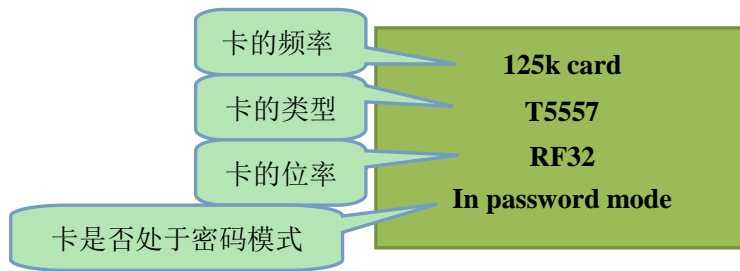


图 2. 2. 2 测试结果

第三步：如图 2. 2. 2 对测试结果进行分析

1. **卡的频率**：被测卡为 125k 低频卡时显示“125k card”，如未放置卡片，或为其他频段的卡（如 s50 卡）时则显示“no 125k card”。
2. **卡的类型**：本装置只支持 T5557，EM4305，EM4100 这三种类型的卡片及其兼容卡。如果不是这三种类型则显示 error。
3. **卡的位率**：被测卡的通信速率，本装置支持 RF32,RF64 两种位率，自动识别无需进行选择。
4. **卡是否有密码**：被测卡处于密码模式显示“**In password mode**”，非密码模式显示“**In no password mode**”。

2.3 T5557 复制

第一步：正确连接电源后，打开侧面的电源开关，屏幕被点亮，出现主菜单界面，进入“图 2. 3. 1”所示界面。通过按三次移动键“▼”可切换至菜单第二屏。

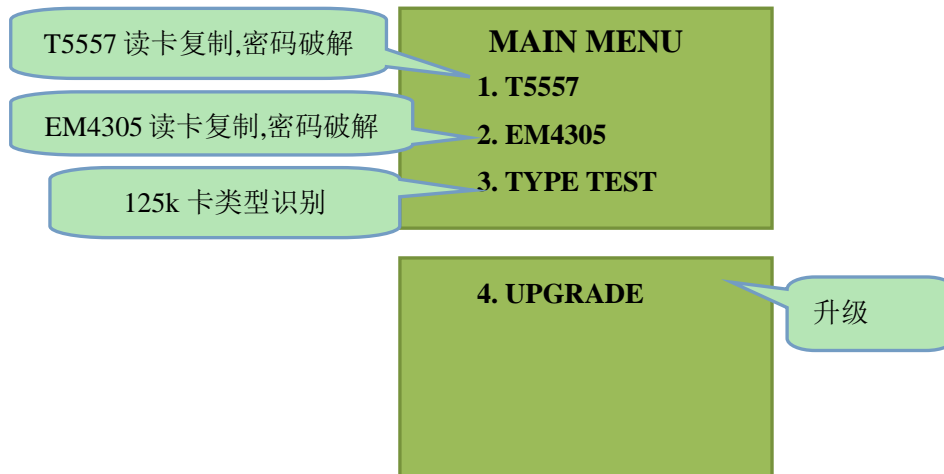


图 2. 3. 1 主菜单

第二步：通过▲▼移动键，移动选单至第一项 T5557，按 ENT 进入“图 2. 3. 2”所示界面。

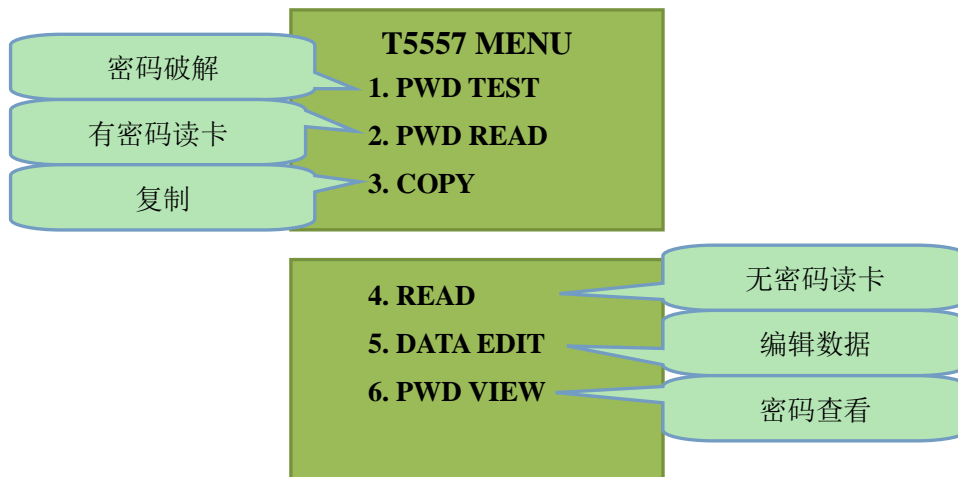


图 2.3.2 T5557 菜单

第三步:

对于无密码卡：选择第四项 **READ** 后直接转到第五步。

对于有密码卡：选择第二项的 **PWD READ** 进入“图 2.3.3”所示界面。

说明：如不能确定该卡有无密码时，请在主菜单界面选择第三项 **TYPE TEST** 进行测试。

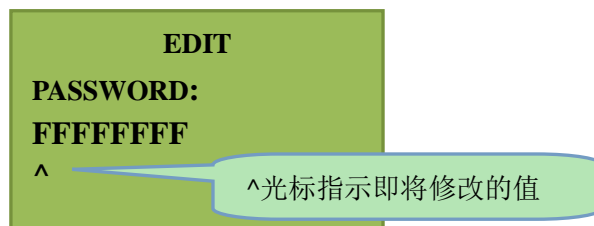


图 2.3.3 密码编辑

第四步: 通过数字按键修改密码数值（移动键：◀ ▶调整光标的位置），输入 8 位密码后将需要复制的 T5557 母卡放到感应区（液晶屏后面），按 **ENT** 开始读卡。

第五步: 读卡成功如图 2.3.4 所示，按 **ENT** 或 **DEL** 退出。数据将会自动保存在主机内掉电不丢失，如需再次浏览或修改请参照“数据编辑/查看”说明。



图 2.3.4 读卡成功



图 2.3.5 读卡失败

第六步: 按 **ENT** 后回到图 2.3.2 所示界面选择第三项 **COPY** 进入图 2.3.6 所示界面。

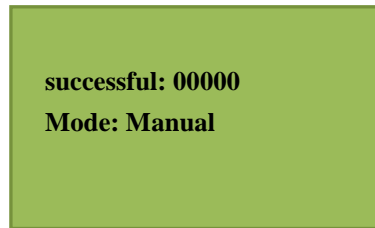


图 2.3.6 复制界面

第七步：将待复制的 T5557 白卡（未使用过）放到感应区（液晶屏背面），按 ENT 即可开始复制。

说明：有手动/自动两种复制模式可供选择，按移动键▲可对两种模式进行切换。Manual 为手动模式；Automatic 为自动模式。

手动模式：每次复制需按 ENT 开始。

自动模式：无需按键控制，自动循环复制。

成功：计数值加一（掉电不丢失，在手动模式下按▼键可清零）。

失败：显示 ERROR。

2.4 EM4305 复制

第一步：正确连接电源后，打开侧面的电源开关。屏幕被点亮，出现主菜单界面。进入“图 2.3.1”所示界面，通过按三次移动键“▼”可切换至菜单第二屏。

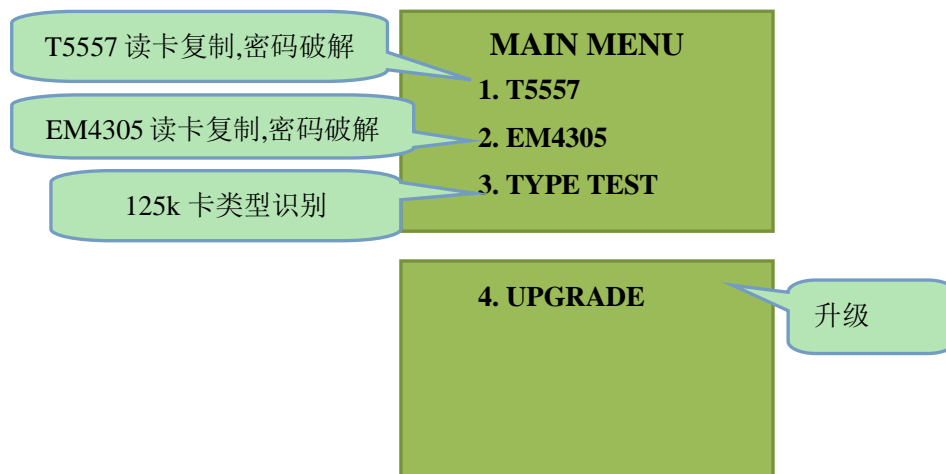


图 2.4.1 主菜单

第二步：通过▲▼移动键，移动选单至第二项 EM4305，按 ENT 进入“图 2.4.2”所示界面。

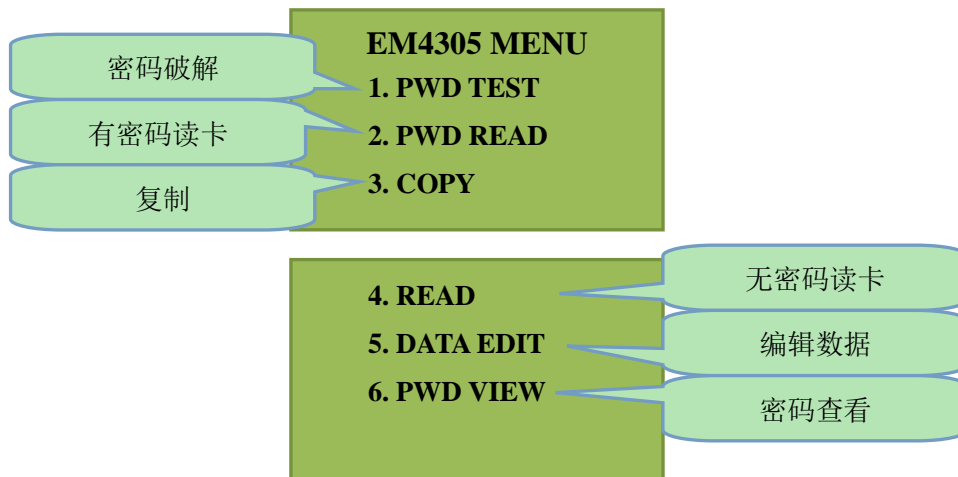


图 2. 4. 2 EM4305 菜单

第三步:

对于无密码卡：选择第四项 READ 后直接转到第五步。

对于有密码卡：选择第二项的 PWD READ 进入“图 2. 4. 3”所示界面。

说明：不确定有无密码请在 2. 4. 1 主菜单界面选择第三项 TYPE TEST 进行测试。



图 2. 4. 3 密码编辑

第四步: 通过数字按键修改密码数值（移动键：◀ ▶调整光标的位置），输完密码后将需要复制的 T5557 母卡放到感应区（液晶屏后面），按 ENT 开始读卡。

第五步: 读卡成功如图 2. 4. 4 所示，按 ENT 或 DEL 退出。数据将会自动保存在主机内，掉电不丢失，如需再次浏览或修改请参照“数据编辑/查看”教程。

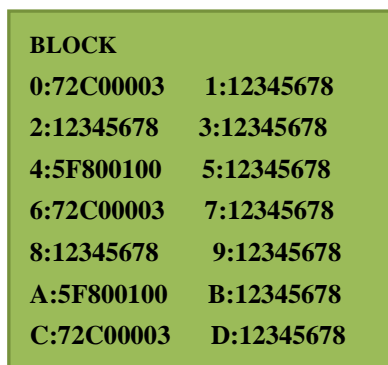


图 2. 4. 4 读卡成功

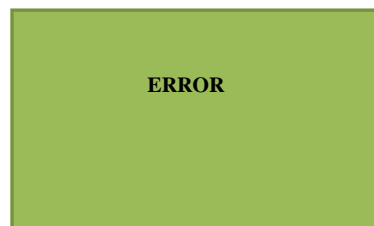


图 2. 4. 5 读卡失败

第六步: 按 ENT 后回到图 2. 4. 2 所示界面选择第三项 COPY 进入图 2. 4. 6 所示界面。

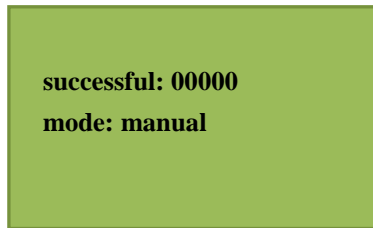


图 2.4.6 复制界面

第七步：将待复制的 T5557 白卡（未使用过）放到感应区（液晶屏背面），按 **ENT** 即可开始复制。

说明：有手动/自动两种复制模式可供选择，按移动键▲可对两种模式进行切换。

手动模式：每次复制需按 **ENT** 开始。

自动模式：无需按键控制，自动循环复制。

成功：计数值加一（掉电不丢失，在手动模式下按▼键可清零）。

失败：显示 ERROR。

2.5 T5557 密码破解

破解视频链接：

http://v.youku.com/v_show/id_XMzQ0ODYwMTI0OA==.html?spm=a2h0k.8191407.0.0&from=s1.8-1-1.2

第一步：连接天线板请参考图“2.5.5”，正确连接电源后，打开侧面的电源开关，屏幕被点亮，出现主菜单界面，进入如“图 2.5.1”所示界面，通过按三次移动键“▼”可切换至主菜单第二屏。

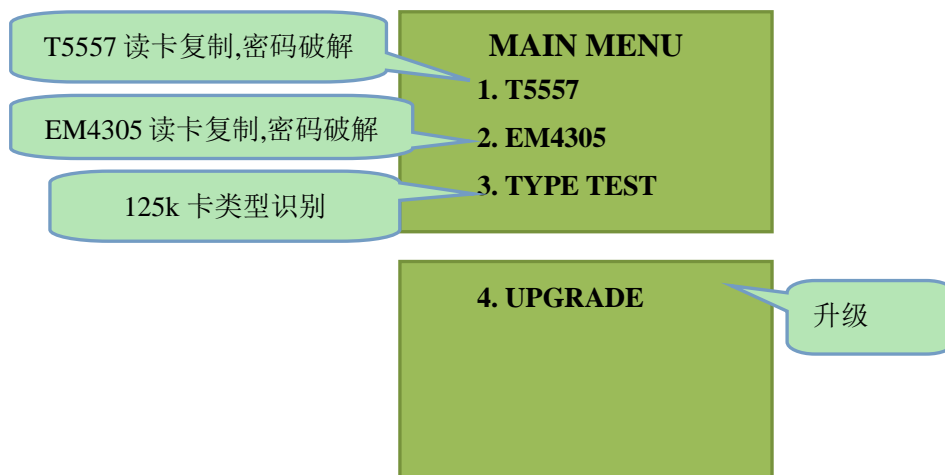


图 2.5.1 主菜单

第二步：通过移动键▲▼，移动选单至第一项 T5557，按 ENT 进入“图 2.5.2”所示界面。

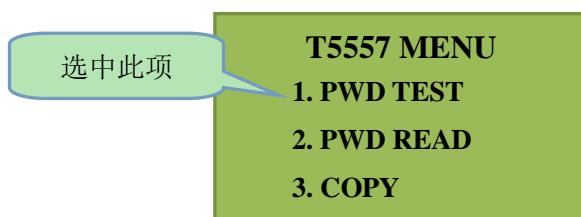


图 2.5.2 T5557 菜单

第三步：选中第一项 PWD TEST，按 ENT 进入如图“2.5.3”所示破解状态。



图 2.5.3 破解状态

第四步：将天线板放置于发卡设备或锁上。

第五步：进行用卡流程后中间 LED 点亮，按 RST 后界面显示如图“2.5.4”，即为破解成功，密码即为显示的数字，显示 ERROR 为破解失败（如破解失败或无法发卡，请将可用的卡置于天线板之上再次重复以上操作）。

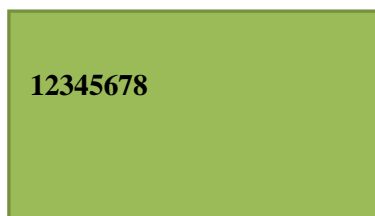


图 2.5.4 破解成功



图 2.5.5 破解连接示意图

2.6 EM4305 密码破解

破解视频链接:

http://v.youku.com/v_show/id_XMzQ0ODY4ODM4OA==.html?spm=a2h0k.8191407.0.0&from=s1.8-1-1.2

第一步: 连接天线板请参考上图 2.5.5, 正确连接电源后, 打开侧面的电源开关, 屏幕被点亮, 出现主菜单界面, 进入如“图 2.6.1”所示界面, 通过按三次移动键“▼”可切换至主菜单第二屏。

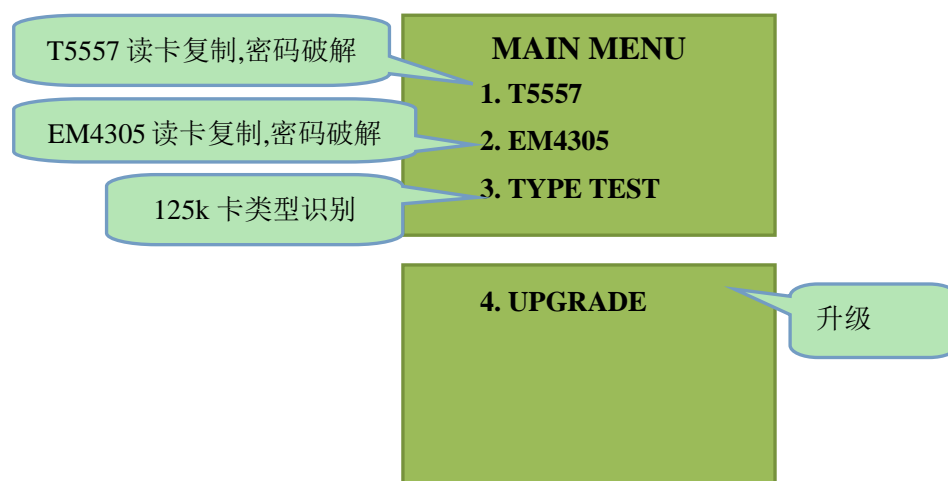


图 2.6.1 主菜单

第二步: 通过移动键▲▼, 移动选单至第二项 EM4305, 按 ENT 进入“图 2.6.2”所示界面。

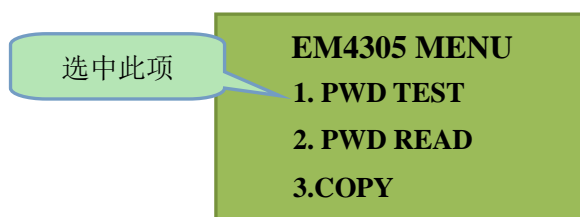


图 2.6.2 T5557 菜单

第三步: 选中第一项 PWD TEST, 按 ENT 进入如图“2.6.3”所示破解状态。



图 2.6.3 破解状态

第四步：将天线板放置于发卡设备，参见图 2.5.5。

第五步：进行用卡流程后中间 LED 点亮，按 RST 后界面显示如图“2.6.4”，即为成功破解，密码即为显示的数字，显示 ERROR 为破解失败（如破解失败或无法发卡，请将可用的卡置于天线板之上再次重复以上操作）。

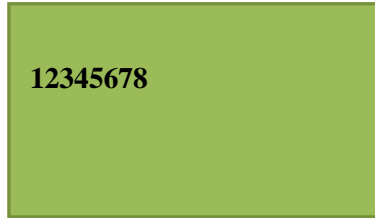


图 2.6.4 破解成功

2.7 T5557 数据编辑

第一步：正确连接电源后，打开侧面的电源开关。屏幕被点亮，出现主菜单界面。进入“图 2.7.1”所示界面，通过按三次移动键“▼”可切换至菜单第二屏。

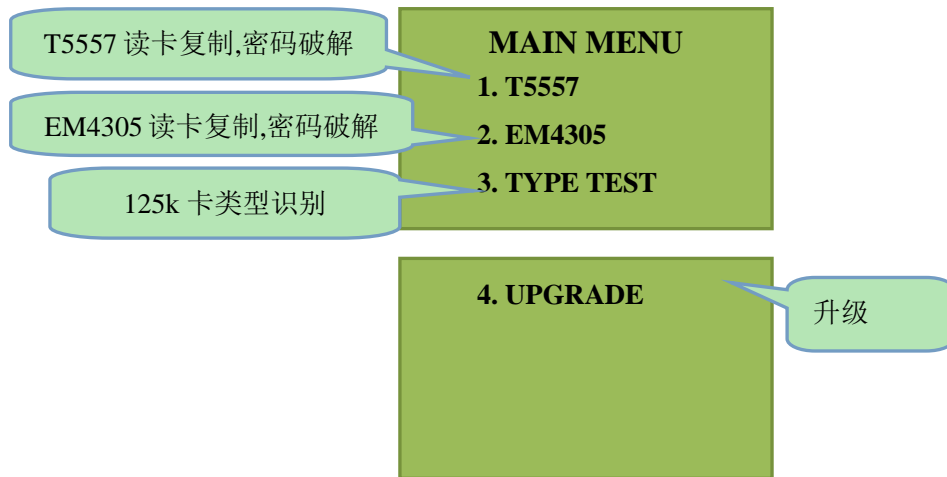
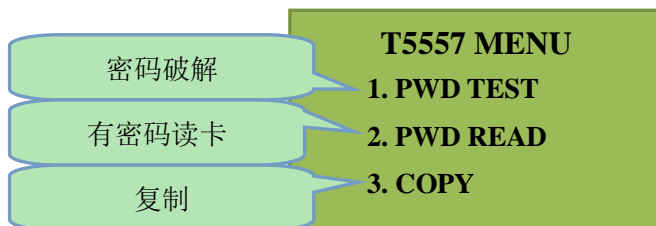


图 2.7.1 主菜单

第二步：通过▲▼移动键，移动选单至第一项 T5557，按 ENT 进入“图 2.7.2”所示界面。



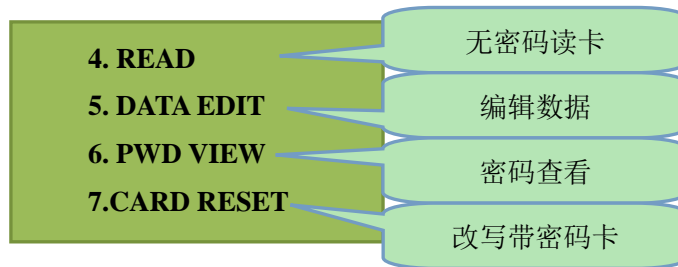


图 2.7.2 T5557 菜单

第三步：选择第五项的 DATA VIEW 进入“图 2.7.3”所示界面。

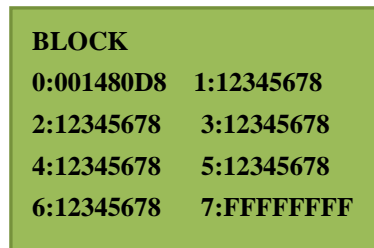


图 2.7.3 数据查看

第四步：按数字键 0-7 选择你想要编辑的扇区，进入“图 2.7.4”所示界面。

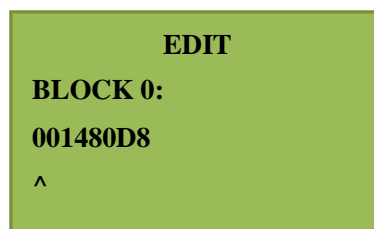
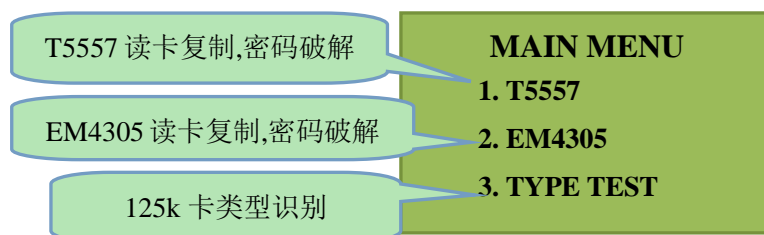


图 2.7.4 数据编辑

第五步：通过数字按键修改数值（移动键◀ ▶调整光标的位置），输完后按 ENT 保存返回“图 2.7.3”所示界面。进行 copy 操作即可将修改的数值写入卡片中。

2.8 EM4305 数据编辑

第一步：正确连接电源后，打开侧面的电源开关。屏幕被点亮，出现主菜单界面。进入“图 2.8.1”所示界面，通过按三次移动键“▼”可切换至菜单第二屏。



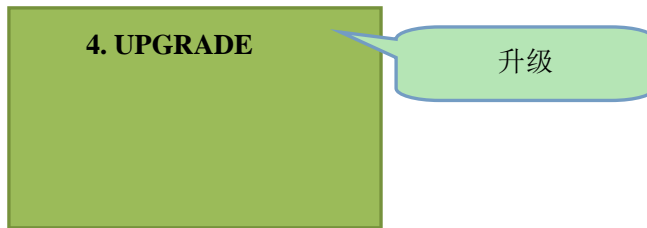


图 2.8.1 主菜单

第二步：通过▲▼移动键，移动选单至第二项 EM4305，按 ENT 进入“图 2.8.2”所示界面。

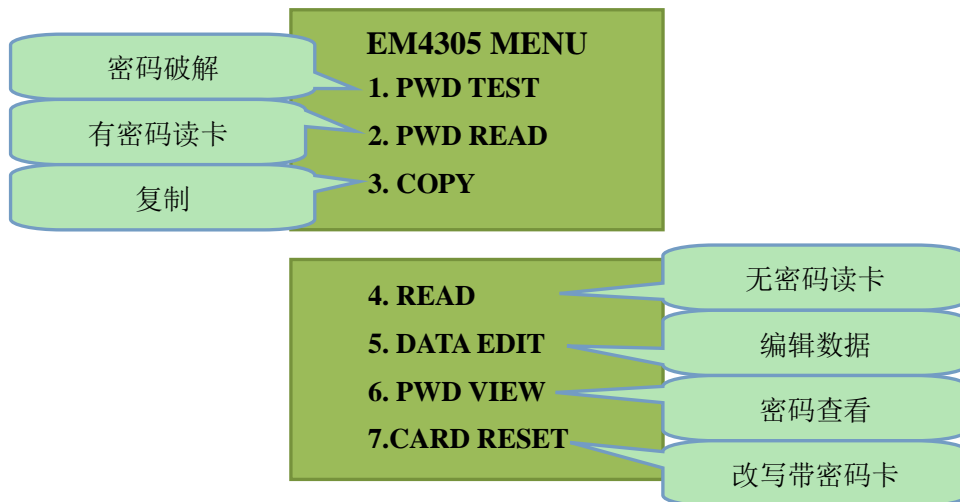


图 2.8.2 EM4305 菜单

第三步：选择第五项的 DATA VIEW 进入“图 2.8.3”所示界面。

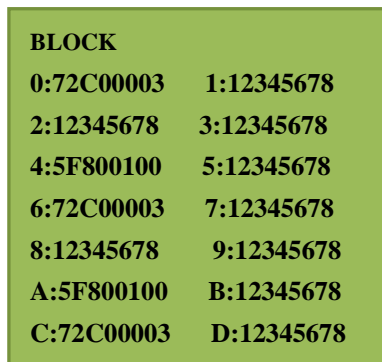


图 2.8.3 数据查看

第四步：按数字键 0-D 选择你想要编辑的扇区，进入“图 2.8.4”所示界面。

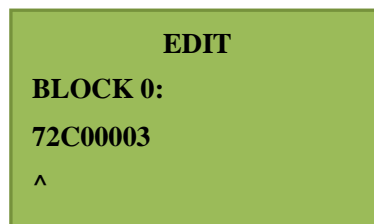


图 2.8.4 数据编辑

第五步：通过数字按键修改数值（移动键◀▶调整光标的位置），输完后按 ENT 保

存返回“图 2.8.3”所示界面。进行 copy 操作即可将修改的数值写入卡片中。

2.9 改写带密码的 T5557 卡

第一步：通过说明书中 2.7 章节“T5557 数据编辑”或直接用“READ/PWD READ”进行读卡操作，将需要写入的数据保存至机器内。

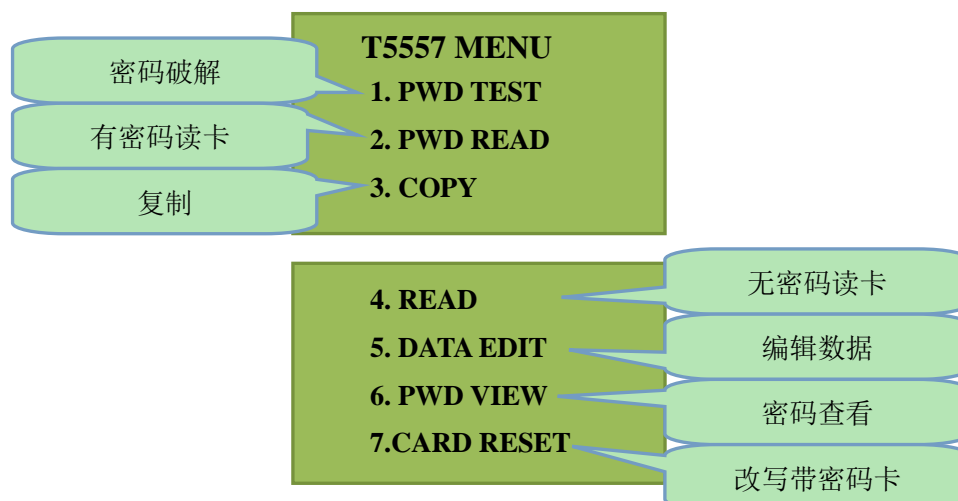


图 2.9.1 T5557 菜单

第二步：在图 2.9.2 所示界面，通过▼移动键选择第七项 CARD RESET 进入图 2.9.2 所示界面。

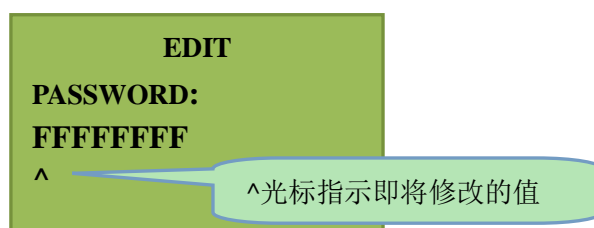


图 2.9.2 子卡密码编辑

第三步：通过数字按键修改密码数值（移动键：◀ ▶调整光标的位置），输入 8 位密码后按 ENT 进入图 2.9.3。

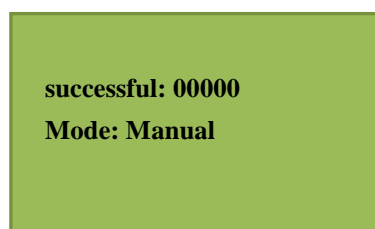


图 2.9.3 复制界面

第四步：将待改写的 T5557 卡放到感应区（液晶屏背面），按 ENT 即可开始复制。

（复制后的内容即为第一步保存的内容）

说明：有手动/自动两种复制模式可供选择，按移动键▲可对两种模式进行切换。

Manual 为手动模式；**Automatic** 为自动模式。

手动模式：每次复制需按 ENT 开始。

自动模式：无需按键控制，自动循环复制。

成功：计数值加一（掉电不丢失，在手动模式下按▼键可清零）。

失败：显示 ERROR。

2.10 改写带密码的 EM4305 卡

第一步：通过说明书中 2.8 章节“EM4305 数据编辑”或直接用“READ/ PWD READ”进行读卡操作，将需要写入的数据保存至机器内。

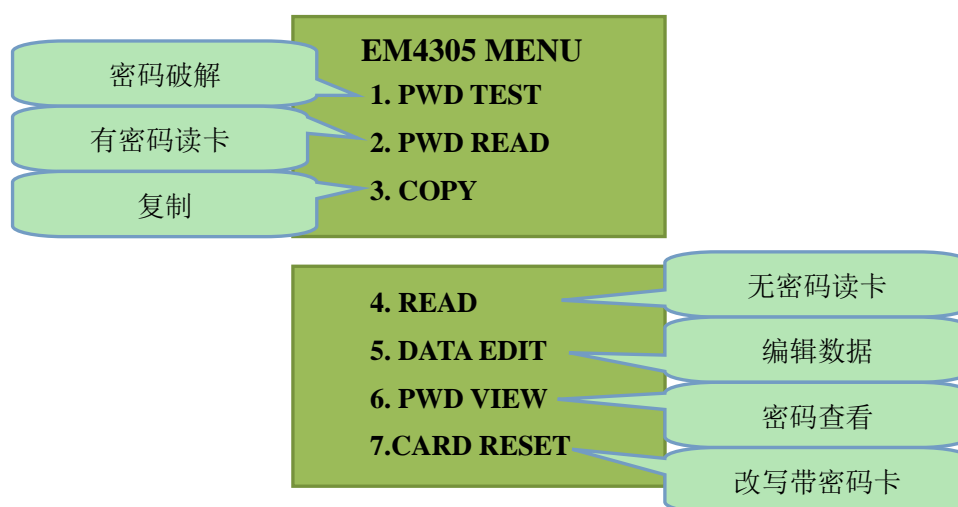


图 2.10.1 EM4305 菜单

第二步：在图 2.10.2 所示界面，通过▼移动键选择第七项 CARD RESET 进入图 2.9.2 所示界面。



图 2.10.2 子卡密码编辑

第三步：通过数字按键修改密码数值（移动键：◀ ▶调整光标的位置），输入 8 位密码后按 **ENT** 进入图 2.10.3。

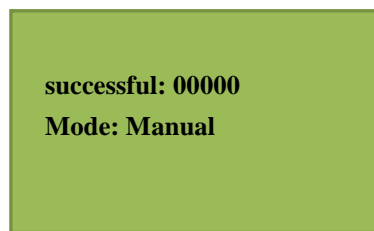


图 2.10.3 复制界面

第四步：将待改写的 T5557 卡放到感应区（液晶屏背面），按 **ENT** 即可开始复制。
（复制后的内容即为第一步保存的内容）

说明：有手动/自动两种复制模式可供选择，按移动键▲可对两种模式进行切换。
Manual 为手动模式；**Automatic** 为自动模式。

手动模式：每次复制需按 **ENT** 开始。

自动模式：无需按键控制，自动循环复制。

成功：计数值加一（掉电不丢失，在手动模式下按▼键可清零）。

失败：显示 **ERROR**。

2.11 远程升级

第一步：正确连接电源后，打开侧面的电源开关。屏幕被点亮，出现主菜单界面。
进入“图 2.11.1”所示界面，通过按三次移动键“▼”可切换至菜单第二屏。

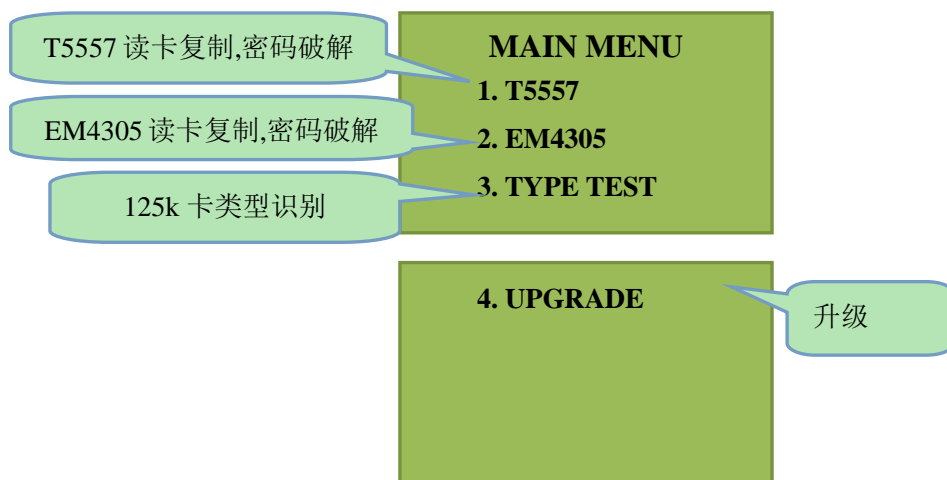


图 2.11.1 主菜单

第二步：通过移动键▲▼，移动选单至第四项 UPGRADE，按 ENT 进入“图 2.11.2”所示界面。

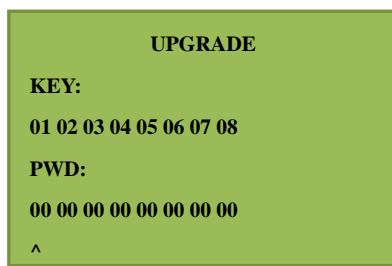


图 2.11.2 远程升级

第三步：将 KEY 下的数据发给本公司；
将本公司发回的数据输入至 PWD 后；

第四步：按 ENT，界面显示 OK 即为通过，相应功能即开放。如界面显示 error 为 PWD 错误，则须重新操作。

3. 常见问题

3.1 关于“无密码读”和“有密码读”

T5557 和 EM4305 均可设为无密码模式或有密码模式，这是由发卡商的设置所决定的。读卡时，采用的读卡模式必须与该卡的设置模式相一致。可采用本机所带的“TYPE TEST”（类型测试）来判断，即根据“TYPE TEST”的结果来选择。

3.2 关于卡的加密方式

T5557 和 EM4305 均可设为无密码模式或有密码模式，这是由发卡商的设置所决定的。只有当一张卡被发卡商设置成有密码模式，才可以采用本装置破解密码。如果一张卡被发卡商设置成无密码模式，则不可以采用本装置破解密码，因为无密码可解。当一张卡被发卡商设置成无密码模式，通常发卡商采用了 UID（唯一序列号）与数据相关联的数据加密模式，所以直接复制的卡并不能使用。

4. 联系我们

网页：www.setchief.com 电话：020-85662866 传真：020-85550217

Email：shichengdz@163.com , 61969088@qq.com Skype：[shichengdz@163.com](https://www.skype.com/user/shichengdz@163.com)

QQ: 61969088

地址：广州市天河区中山大道西 238 号勤天大厦 1802 室， 邮编：510665