

NFC 手机模拟加密门卡教程

前言：目前经过我们测试以及众多买家客户反馈，可以确定支持模拟加密 IC 卡有如下设备

手机：小米红米系列带有全功能 NFC 智能手机；华为麒麟 980 芯片带有全功能 NFC 的智能手机；魅族 16S。三星 NOTE9-10、 S10 操作教程如下

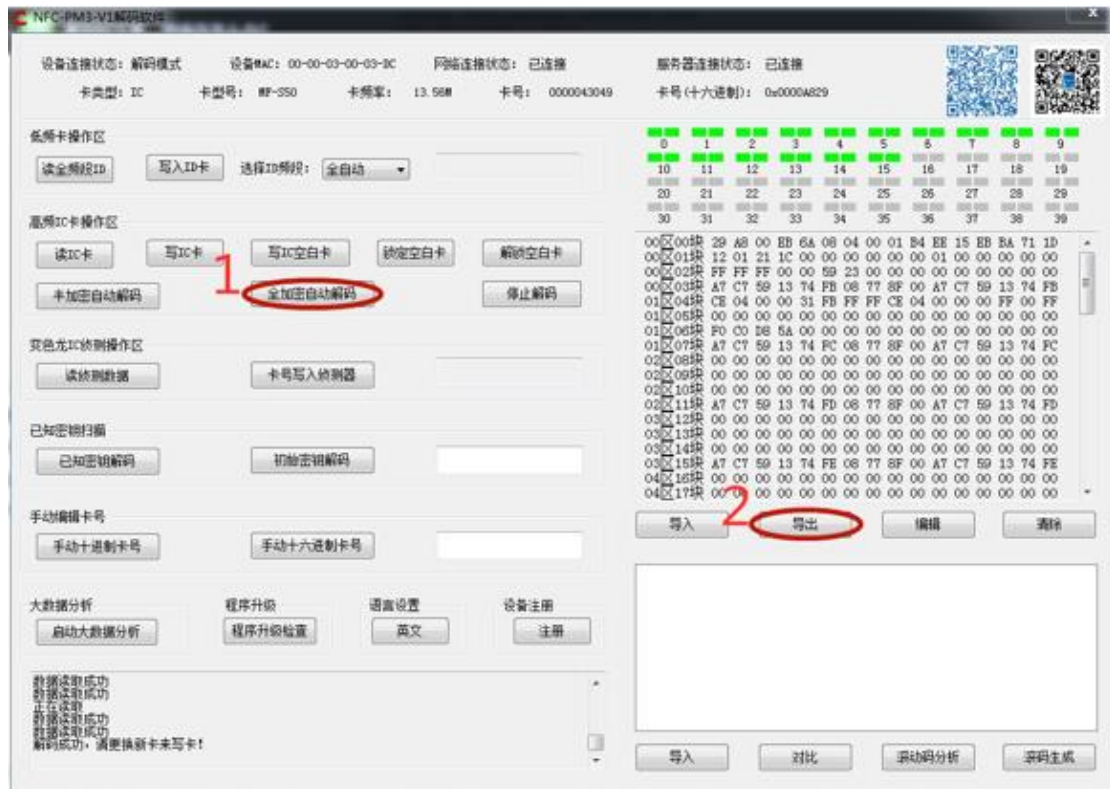
- 准备物品：
- 1、一台 NFC-PM3 读写器
 - 2、小米 NFC 手环（教程以小米手环为例。）
 - 3、门禁卡
 - 4、空白卡（UID、CUID 都行）

第一步：解密门禁卡

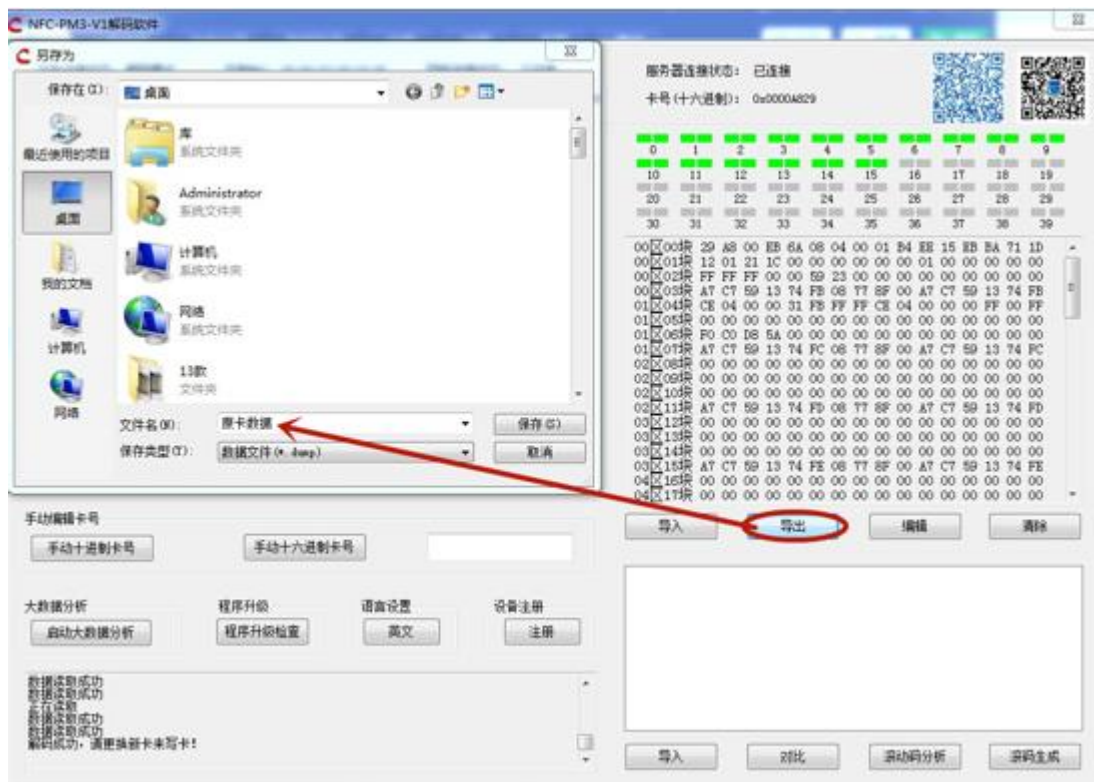
- 1、设备连接电脑，识别设备自带 U 盘，打开 U 盘里面的软件（记得移出桌面，以免软件运行卡顿）
- 2、将门禁卡放置设备的 IC 识别区



- 3、点全加密自动解码获取数据（所有的 IC 卡都可以直接点全加密自动解码，该功能覆盖了读 IC 及半加密自动解码的功能）



- 4、导出数据保存在桌面，后面要用到



第二步：制作模拟卡（很多买家卡在这一步，或者操作有误，切记，这一步的目的就是获取一张 0 区 0 块跟原卡一样的非加密卡）

因手机 NFC 只能模拟无加密的 IC 卡，所以我们要先模拟一张卡号与原卡一样的无加密卡，以便模拟进手机 NFC。通过第一步已获取原卡数据，我们只需把原卡的 0 扇区 0 块（号卡数据）利用软件的编辑功能手动输入到一张空白卡上即可

- 1、把空白卡（ICK）放到设备 IC 识别区，点“读 IC 卡”待软件左侧扇区变绿后显示出数据(未使用过的 IC 空白卡数据都是未加密的)
- 2、按软件界面下方的导入按键，导入原卡数据
- 3、利用软件的“编辑”功能，把原卡 0 扇区 0 块的数据手动输入到空白卡 0 区 0 块



- 4、编辑好后，保存，并写入空白卡。（IC-K、UID 点“写 IC 空白卡”）（CUID 点写 IC 卡）

备注：切记，只修改 00 区 00 块数据，把原卡 00 区 00 块的数据通过“编辑”输入到空白卡的 00 区 00 块上。其他扇区不动！通过以上操作就获得了一张卡号与原卡原一样的无加密 IC 卡，就可以模拟到手机 NFC 了。

解析：IC 卡写入手机手环，主要就是第二步跟第四步。通过这两个步骤，把 IC 里的 16 个扇区数据搬到手机\手环里，第二、第三步就是把 0 区 0 块的卡号数据先通过模拟的方式搬进手机\手环里，然后在通过第四步把剩下的 1-15 扇区数据写入到手机\手环

PS：这步如果操作不来的话，可以点下面的连接，看操作视频

https://market.m.taobao.com/apps/market/content/index.html?wh_weex=true&contentId=234873437445

第三步：用手机\手环模拟第二步制作的那张卡（已经修改了 00 区 00 块数据的那张）。

打开小米钱包。进入门卡模拟，检测成功并身份认证，即可模拟空白卡



用手环模拟白卡后，手环会提示模拟成功，但是由于手环中的虚拟卡仅仅只包含了该门禁卡的卡号信息，所以也是无法开门的，需要你继续把门禁卡的加密信息也写入进去。

第四步:为手环写入加密数据

1、将手环放置 PM3 的 IC 识别区



2、导入门禁卡的数据 点写 IC 卡



3、提示写入失败？



写入后软件会提示写卡失败、**这个是正常现象、是正常现象、正常现象**。

重要的事多说几遍）（因为手环锁定了自身的验证码区域）

通过以上操作，就模拟成功了，各种刷门禁，不可言喻的喜悦.....