手机手环复制教程

模拟实现的条件：：

1.复制器一台

2.手机或者手环一部（必须具备 NFC 功能）

3.可反复擦写的卡一张（UID 或 CUID 都可）

4.需要模拟的 IC 卡（称之为原卡，13.56Mhz 的 M1 卡）

前言：小米从 MIUI12 开始支持模拟加密 IC 卡/华为手机 CPU980 以上支持模拟，但只能模拟加密 IC 卡卡号信息（0 扇区 0 块）

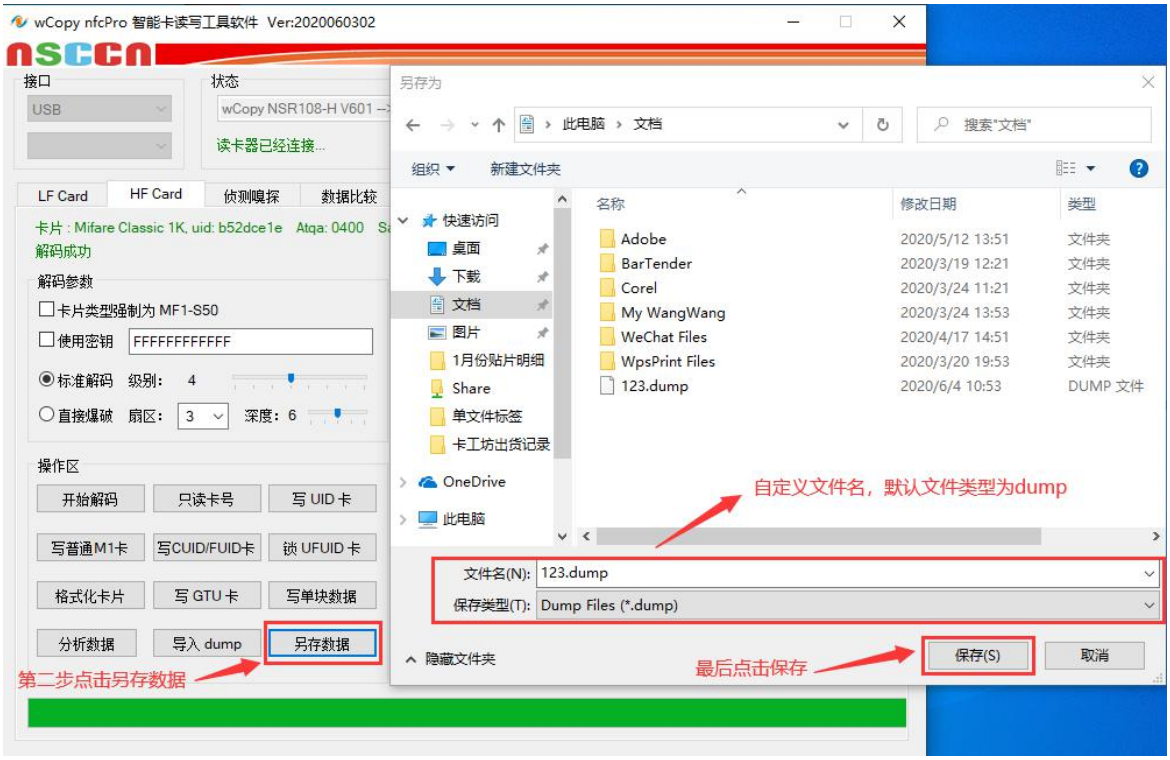
本教程以 NSR108 软件版本为 2020060302，复制加密卡数据到小米 4NFC 手环为例。

第一步：原卡解密

机器连接电脑后打开软件，把需要模拟的卡（原卡）放在机器的感应区域，点击“开始解码”按钮。解码过程中不要移动卡片或者机器，耐心等待解码成功（解码时间根据不同卡加密程度而定，几秒钟至一小时的情况都有）。

第二步：另存数据

解码成功以后，右侧数据栏会出现 16 进制的原始数据，点击“另存数据”按钮，对数据进行保存选好输出路径，保存后会得到一个 dump 文件，并且文件大小标准为 1K 文件，这里我们重命名为“123.dump”



第三步：写入空卡

换上复制空白卡，点击写 UID 卡或者 CUID 卡按钮，写卡成功后点击格式化卡片，格式化成功后得到一份不带加密数据的卡。

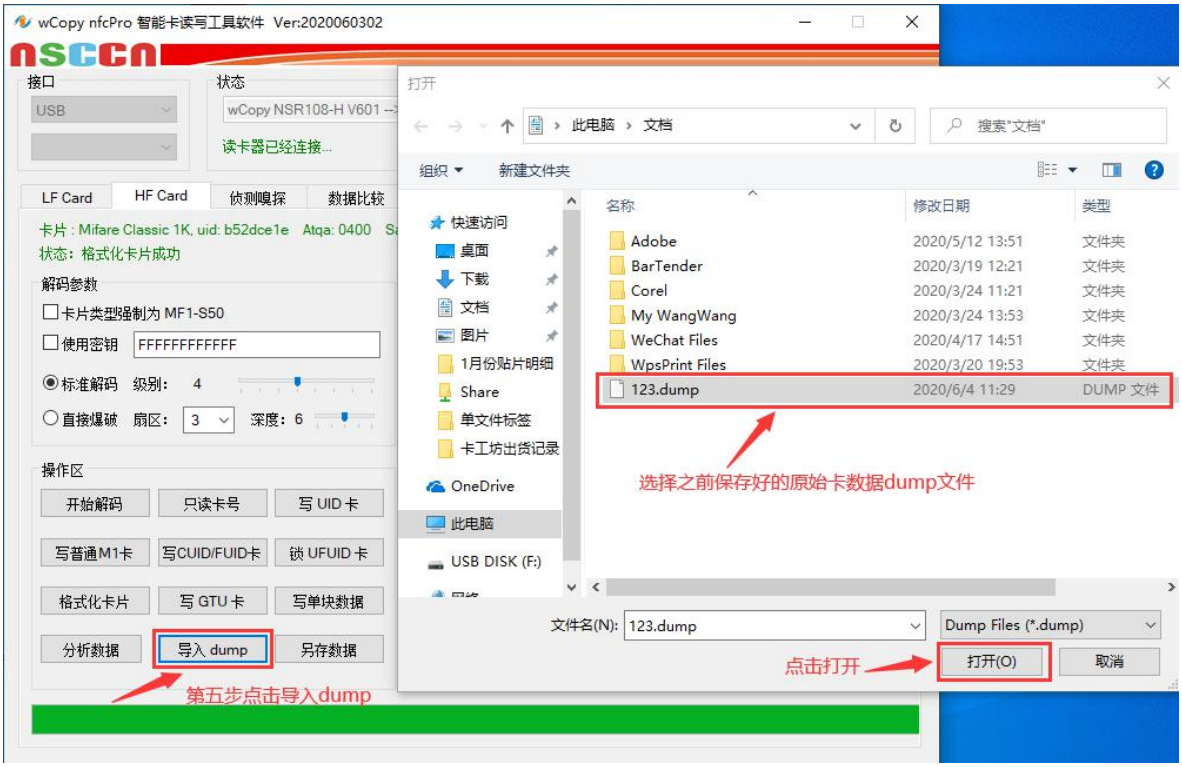
第四步：模拟原卡卡号

手机打开蓝牙点开小米运动（app），连接手环后，找到“门卡模拟”，打开门卡模拟，再次注意此时只是模拟了原卡的卡号而已，加密数据并不会写入，按照提示进行下一步。（手机各有不同请自行操作一下）

检测卡片成功后，点击开始模拟，耐心等待模拟成功，成功后自行添加卡片名称，点击完成。

第五步：写入数据

手机或者手环模拟成功后，把手机或者手环放置复制器的感应区域，导入之前保存好的原始卡数据 dump 文件，点击“写普通 M1 卡”，软件提示写卡成功即模拟成功。



如果写手机时软件提示写卡失败或者验证卡片某扇区密码错误，我们就需要重来了。把模拟进去的空卡删掉，按照步骤重新模拟，模拟成功后点击开始解码，解码成功后，再进行格式化（特别注意：空卡模拟成功后解码手机再格式化，）格式化成功后再按照步骤导入原卡数据 dump 文件，点击‘写普通 M1 卡’按钮，写卡成功即模拟成功。

小米的卡模拟功能只能模拟 0 扇区 0 块的前 8 个字节，且绝大部分梯控只验证 0 扇区 0 块前 8 个字节数据，后 8 字节的厂商编码无法更改。

关于复制加密 IC 卡信息到手机成功后，无法读取到写入手机 NFC 完整信息的解决办法

思路：因为手机手环 NFC 芯片安全等级较高，已经修复了嵌套攻击漏洞，所以 NFC 解码软件不能靠后门破解。虽然后门堵死了，正门有钥匙还是可以进，钥匙就是原卡 dump 文件中的密钥 A 或者密钥 B，有了密钥，安全等级再高也可以读取 NFC 信息。

注意把软件更新到最新版本（检查更新）

解码原卡后，点击“另存数据”，保存原卡数据 dump 文件。再回到软件，点击“导入 dump”按钮，把保存好的原卡 dump 文件导入进去后，软件会自动填写密钥，需手动勾选“使用密钥”，把手机放置机器读卡区域，点击“开始解码”，就可以解码写入手机的数据。如写入手机或者手环后刷卡不成功，此时可另存数据，保存手机解码出来的 dump 文件。切换到软件的“数据比较”界面，分别导入原卡数据 dump 文件与写入手机的数据 dump 文件，比较数据是否一致（此操作可参考复制器使用说明）。