链滴

手机手环 nfc 模拟加密门禁卡

作者：ghostsf

原文链接：https://ld246.com/article/1603262296335

来源网站：链滴

许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

<span class="vditor-linkcard__image" style="background-image: url("https://cdn.ghossf.com/logo_square.png");">

Hi, ghostsf

Do what i love and just do it！

本文来自博客 https://ghostsf.com

现在很多手机和手环都支持NFC了，也新增了公交卡，模拟门禁卡等功能。

手上的小米手环4 NFC版吃灰好久了，拿出来试一试其模拟门禁卡功能，希望到现在了应该能有所突（比如可以模拟一些加密IC卡）。

然而并没有什么实质性的进展：

门卡支持范围

使用门卡模拟功能，需要先进行检测

门卡种类	门卡样式 仅供参考
普通门卡	
异形门卡	

温馨提示:

1. 目前仅支持模拟市面上未经加密且频率为13.56MHz的门卡;
2. 带有 门卡功能的银行卡和 储值消费、公交消费功能的门卡 暂时不能被模拟。即使模拟成功，这些卡片也不具备银行、公交等功能。

原文链接：手机手环 nfc 模拟加密门禁卡

目前依然仅支持模拟市面上未经加密且频率为13.56MHz的门禁卡

不抱希望地试了下，提示都简单明了，“加密卡”，搞不定。

原文链接：手机手环 nfc 模拟加密门禁卡

不过另外看到新增一项可以添加空白卡的功能：

开通后可以去物业授权或激活？？？

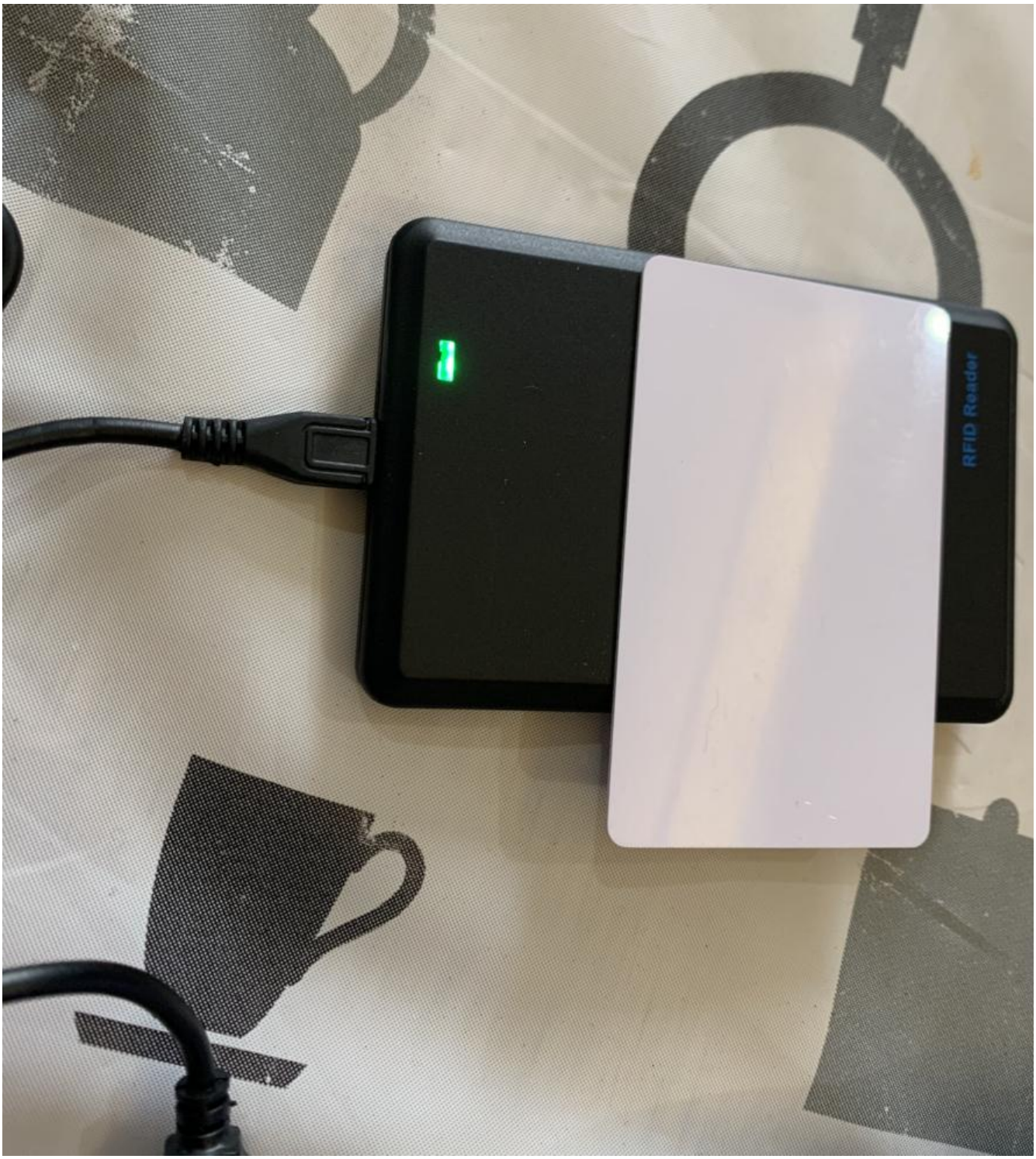
看来小米也在尽可能地为用户考虑啊。不过找物业搞，可能性估计还是很小的，也麻烦。

进入正题

NFC加密卡的种类等问题，这里就不科普了。

解这种加密卡，一般需要专业的nfc读写器。这里推荐个PN532。我买的ICID双频版(你值得拥有，当不是广告)。

原文链接：手机手环 nfc 模拟加密门禁卡

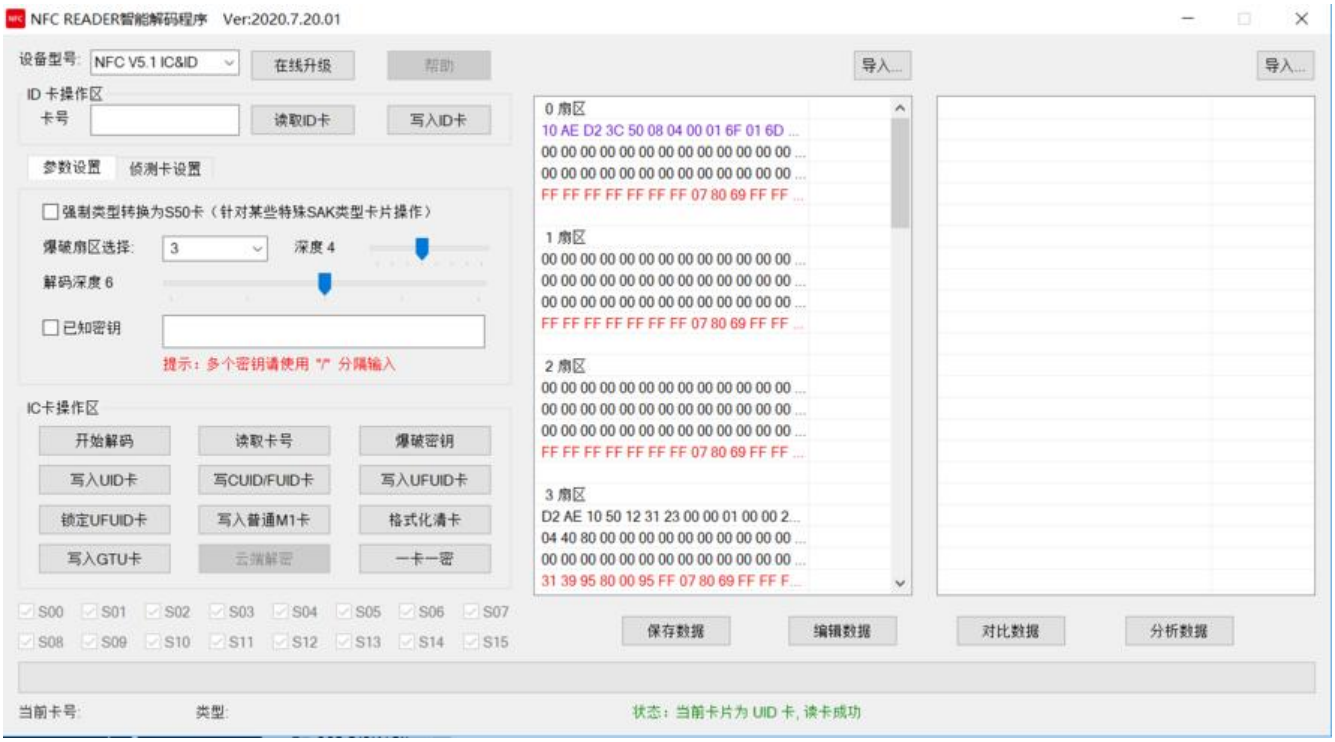


用PN532解卡

我买的这款设备自带软件，usb插上后即可打开获得软件，还是很方便的，软件功能也很强大，当然备更强大（后面还有大用处）。

名称	修改日期	类型	大小
nfcPro_kgf_v6.exe	2020/7/20 10:02	应用程序	708 KB
下载最新软件.txt	2020/6/15 15:59	文本文档	1 KB

原文链接：手机手环 nfc 模拟加密门禁卡



几乎秒解，保存数据，获得加密数据。

```
10ae d23c 5008 0400 016f 016d 4568 f81d
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
ffff ffff ffff ff07 8069 ffff ffff ffff
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
ffff ffff ffff ff07 8069 ffff ffff ffff
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
ffff ffff ffff ff07 8069 ffff ffff ffff
d2ae 1050 1231 2300 0001 0000 2359 0000
0440 8000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
3139 9580 0095 ff07 8069 ffff ffff ffff
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
ffff ffff ffff ff07 8069 ffff ffff ffff
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
ffff ffff ffff ff07 8069 ffff ffff ffff
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
ffff ffff ffff ff07 8069 ffff ffff ffff
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
ffff ffff ffff ff07 8069 ffff ffff ffff
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
ffff ffff ffff ff07 8069 ffff ffff ffff
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
ffff ffff ffff ff07 8069 ffff ffff ffff
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
ffff ffff ffff ff07 8069 ffff ffff ffff
0000 0000 0000 0000 0000 0000 0000 0000
```

绑定写卡

这里需要了解的是，这里手环或手机绑定nfc卡，只有0扇区0区块的数据，因此只需要给设备绑定一空白卡之后，写入剩下的数据即可。

那么怎么绑定空白卡呢?

一般购买nfc读写设备会送一些nfc卡，我这各种类型的都送了：ID,CUID,UID很全。

这里可以先给设备绑定一张空白卡，绑定成功后，再将读取到的原门禁卡数据写入，注意只要写入除扇区0区块以外的数据，原空白卡0扇区0区块的数据保留即可。

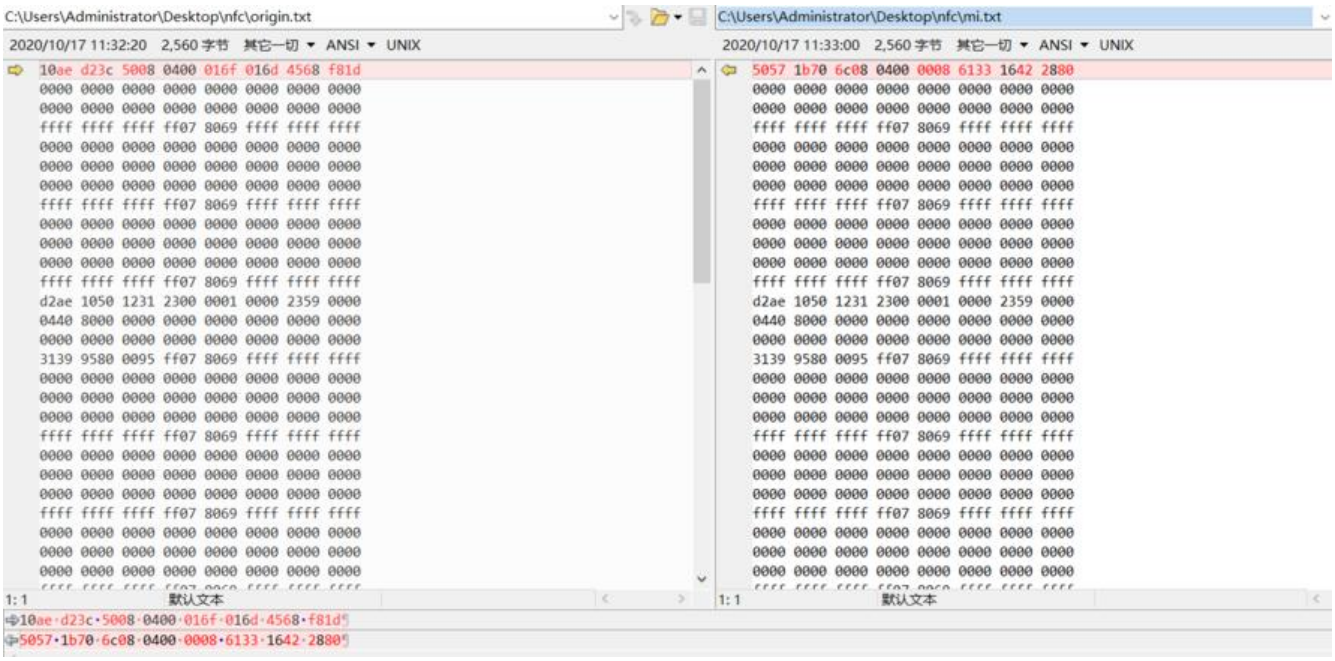
用文本编辑器编辑好数据（然后导入），或者用软件自带的编辑功能区编辑，然后再写入卡即可。

原文链接：手机手环 nfc 模拟加密门禁卡

这里的绑定空白卡，现在还有更简单的方式了，当然就是上面提及的，小米新增了直接创建空白卡的能。那么上用nfc空白卡绑定的操作就不需要了，直接先创建一个空白卡，然后写入除0扇区0区块以的数据即可。

验证

验证是否成功，对比下原门禁卡数据和现在手环上nfc的数据，除0扇区0区块以外的数据是否一致即（也可以用软件自带的比较功能，功能是真的多）。或者你拿去小区门禁上刷一下，就知道了嘛。



小米手机 MI6

另外试了下小米手机MI6。

最新的MIUI 12，发现竟然更新了可以直接开通小区门卡，可以搜索选择已有的小区，MIUI果然还是重视用户啊。（然而没有我的小区 = =）。

试了下直接绑定门卡，竟然直接绑定成功了！（然而，实际并不能打开门禁= =）。

还新增了智能门锁的门卡。

可以说功能很详尽了。MIUI还是值得点赞的！

iPhone

现在就剩iPhone手机没整了。看了下，目前iPhone还是只能通过绑定任意一张交通卡，然后刷一下禁，再找小区物业激活（当然需要小区门禁识别iPhone nfc交通卡）。当然也有可能绑好交通卡后，如上面的操作，写入加密数据（成功可能性不大，还要开花钱开一张和废一张，交通卡暂时没试过，手环用就够了）。当然，越狱就另当别论了。

End

有了手环开门禁还是方便些的，至少不用多带一个门禁卡了。 ==