

M1T 应用手册

适用版本：v1.6.5

(第一版)

XciCode

1 简介

MifareOneTool, 简称 M1T, 是一款基于 libnfc 的 Mifare Classic 卡片 GUI 操作工具。该 GUI 使用 GPLv3 协议开放了源代码。

由于该软件中部分工具具有一定攻击性, **请注意勿违法使用!** 若使用本软件造成的任何后果由使用者承担。

本手册讲解高级操作模式下的操作。

2 支持的设备及卡片

本软件支持 PN532 (通过串口连接) 及其它兼容指令的串口 NFC 读写器。

注: ACR122U 支持尚不完善。因其版本不同及通信协议的差异, 不再继续考虑支持。

关于 PN532 的串口转接线, 建议使用 CH340 芯片的产品, 部分 PL2303 芯片可能在某些操作系统下工作不够稳定。据用户反映, CP2104 也无法正常工作。

本软件支持对于 Mifare Classic 卡片 (M1 卡) 的操作。

各功能兼容性参见下表:

	S50 卡, 1K (SAK08)	S70 卡, 4K (SAK18)	UID 类, 1K (SAK08)	CUID 类, 1K (SAK08)	CPU 模拟卡 (SAK28)
手动扫描	可以	可以	可以	可以	可以
读 M1 卡	可以	可以	没必要	可以	可以
写 M1 卡	可以	需禁用保护	没必要	可以	可以
清 M1 卡	可以	可以	没必要	可以	可以
UID 读	不行	不行	可以	不行	不行
UID 写	不行	不行	可以	不行	不行
UID 重置	不行	不行	可以	不行	不行
UID 写号	不行	不行	可以	不行	不行
UID 全格	不行	不行	可以	不行	不行
锁 Ufuid	不行	不行	仅 UfUID 卡	不行	不行
CUID 写	不行	不行	不行	可以	不行
差异比较	可以	未支持	可以	可以	可以
Hex 编辑器	可以	未支持	可以	可以	可以
自动判断 Key	可以	仅前 128 块	没必要	可以	未测试
MFOC 读	仅半加密	仅半加密且不一定	没必要/不行	仅半加密	不行
检加密	可以	可以	可以	可以	未支持
知 n 密	可以	不一定	没必要/不行	可以	不行
字典测试	可以	不一定	没必要/不行	可以	不行
全加密爆破	可以	可以	没必要	可以	未测试
Hardnested	可以	未测试	没必要	可以	仅半加密

3 软件功能及介绍

(以高级操作模式的按钮名称为例，复制卡模式中的名称为蓝色字体显示)

◆ **检测设备** 检测连接

检测是否已经连接支持的 NFC 设备，会在终端显示区显示找到的设备。

◆ **手动扫描** 扫描卡片

扫描可读取的卡片并显示 UID、SAK、是否为后门卡 (UID 卡) 等信息。

◆ **手动 CLI**

打开 NFC 命令行，可以自行调用工具、加入自定义参数等。

◆ **读 M1** 已知密钥读

读取 Mifare classic 卡片。(可能需要选择密钥文件)

◆ **写 M1** 写入普通卡

写入 Mifare classic 卡片。(可能需要选择密钥文件)

◆ **清 M1**

清空 Mifare classic 卡片。(需要选择密钥文件)

注：一些情况下可能会出现使用自动判断 Key 时清空卡片后，只清除了控制位而 Key 没有被清除的情况。这种情况下，请取消勾选自动判断 Key，然后重新执行清 M1，询问 KeyABN 时请选择“是”。

◆ **选择 key.mfd** 加载密钥…

选择一个带目标卡 Key 及正确控制位信息的 MFD 文件(卡片数据文件)作为密钥文件。

◆ **UID 读** 从 UID 卡读回

读取 UID 类特殊卡，无视 Key 与控制位。

◆ **UID 写** 写(UF)UID 卡

写入 UID 类特殊卡，无视 Key 与控制位。

◆ **UID 重置**

重置 UID 卡的 0 块，写入随机卡号与复旦卡的厂商号。

◆ **UID 写号**

写入 UID 卡的 0 块，写入输入的卡号与复旦卡的厂商号。

◆ **UID 全格**

无条件擦除 UID 卡全卡，恢复到空白状态。

当卡片数据写入错误导致无法访问时，可使用此功能急救。

◆ **锁 UfUID** 锁 UfUID 卡

注：本功能为测试功能，锁定后请检查是否锁死！若有错误，请报告。

锁定 Ufuid 卡，使其变为普通 M1 卡。

◆ **CUID 写** 写 C/FUID 卡

写入 CUID 卡。(可能需要选择密钥文件)

◆ **差异比较**

打开差异比较器 (DiffTool)。

◆ **Hex 编辑器**

打开卡数据文件编辑器 (S50HTool)。

◆ **自动判断 Key**

注：本功能为测试功能，若工作不正常，请取消勾选复选框并报告问题。

在已加载 key.mfd 时，根据文件中的 Key 及控制位进行卡片认证，可以应对混合访问控

制的情况。

◆ **自动加载 uid.Key 文件**

注：本功能为测试功能，若工作不正常，请取消勾选复选框并报告问题。

在软件目录下的 auto_keys 文件夹中搜索以目标卡片小写 UID 开头的 MFD 文件，并自动加载为 key.mfd。

◆ **数据写入保护**

该功能会在将数据写入卡片前进行逻辑检查，以免将错误的 BCC 及访问控制位写入卡片造成损坏。

注：本功能仅支持 S50 卡片数据文件，操作其他种类卡片数据文件时需要关闭。

◆ **自动以 UID 名保存文件**

将读取出的文件以小写 UID 号+日期时间的格式保存在 auto_keys 文件夹中。

◆ **HardNested: 单线程计算**

仅使用 1 个线程计算密钥，可防止计算机卡顿，但是会消耗更多的时间。

◆ **减少找设备延迟**

在点击“检测设备”时配置 libnfc 的参数，减少后续寻找设备时间。

◆ **MFOC 读 一键解原卡**

尝试对卡片进行 Nested 解密，仅半加密卡片支持。

◆ **检加密 检测加密**

检测卡片的加密及默认密码使用情况。按住 Ctrl 点击可输入自定义 key。

◆ **知 n 密 知一密破解**

在已知一个或多个有效 Key 时，尝试对卡片进行 Nested 解密。

◆ **字典测试**

使用字典中的 Key 尝试对卡片进行 Nested 解密。

解密完成后，请手动关闭 cmd 窗口。

◆ **全加密爆破**

注：本功能可能存在小问题，对于一些卡片（尤其是国产全加密卡）无法得到正确的结果。对于该类卡片，建议使用嗅探方法或 Proxmark3 进行解密。

对卡片执行 Darkside 攻击以尝试取得可能的 Key。

◆ **HardNested**

针对 Mfoc 提示不受 Nested 攻击的某些卡片（如 M1-EV1、CPU 模拟卡）尝试进行 Hardnested 解密（可以看作加强版的 Nested 解密），仅半加密卡片支持。

需要手动根据 Mfoc 的未知扇区提示进行目标卡扇区设置。

若需要更快的计算速度，请在初始化解密勾选“只采集不计算”，然后将采集的数据文件上传到云计算服务（见附 3）。

◆ **清终端**

清空终端显示区的内容。

◆ **停运行 停止**

停止正在运行的功能。

◆ **存日志**

将终端显示区的内容保存到软件运行目录下的 m1t.log 文件中。

4 内置编辑器

M1T 集成了一个 MFD 文件 HEX 编辑器 (S50HTool)，用于 S50 卡的 MFD 文件编辑。

#注意# 手误关闭不会提示文件未保存!!

菜单说明

为了方便您的使用，编辑器所有功能均配置了快捷键。

- 文件
 - 新建打开保存另存为，应该都明白:)
- 工具
 - 修改 UID 转到 0 块的编辑模式并修改 UID 号（自动更正 BCC）
 - 检查全卡 检查卡片是否存在逻辑上的错误
 - 检查全卡并纠正 检查错误并自动修正
 - 导入 MCT 格式 导入 MCT 格式的卡数据文件
 - 导出为 MCT 格式 导出为 MCT 可以读取的文件格式
 - 导出密钥字典 将该卡片的 Key 以字典形式导出（兼容 MCT 格式）

单击“扇区列表”中的扇区可转到该扇区编辑模式。

点击“修改扇区”可验证并保存所做修改到当前工作区（注意不是保存到打开的文件）。

5 入门操作（复制卡模式界面）

1. 首先，确保你已经下载了 M1T 的最新版本。
2. 双击 MifareOneTool.exe 运行软件。
我们以复制一张卡为例进行说明。
3. 在最左侧一栏，依次点击检测连接、扫描卡片、检测加密。若看到检测加密的结果中所有 Key 都是未知，则很可能无法解密。
4. 保持卡与读写器通信良好，点击半加密破解对卡片进行解密。成功后，将卡数据文件（MFD）进行保存。
 - a) 若知道一个或多个 Key，请点击知一密破解并输入以加快速度。
5. 取下原卡，放上空白卡片并选择对应的写卡按键点击。
 - a) 若询问 KeyABN，请点击“取消”。
 - b) UFUID 卡写入后需要进行锁定。
6. 测试复制的卡片是否可以正常使用。

6 基本操作流程

1) 读取原卡

#注意# 本工具现在无法执行对于 SAK=28 的卡片的一键解密，只可已知密钥文件读写，建

议配合手机端 MCT 使用。

1. 连接设备，点击“检测设备”。
 - a) 若检测不到，请检查设备管理器中是否能找到设备、接线是否正确。
2. 放置原卡，点击“手动扫描”。
 - a) 注意观察 SAK，目前仅支持 08/18/28 的卡片。
 - b) 若扫描不到，请换个姿势与天线通信。若仍然无法发现，则可能是不支持的卡类型。
3. 点击“MFOC 读”，开始尝试解密卡片。
 - a) 若提示全加密卡，则须通过其它方式获取一个有效 Key 方可继续解密。
 - b) 若卡片 SAK=28，或提示不受 Nested 攻击，请尝试通过 Hardnested 进行解密。
 - c) 若已经具有该卡片的数据文件，则可以在“选择 key.mfd”处加载，然后使用“读 M1”读出。
4. 保存读取出的卡片数据。

2) 写入卡片

- a) 若目标卡片为非空卡，需要加载该卡片的原数据文件作为 key.mfd，然后点击“写 M1”，选择数据文件写入卡片。
- b) 若目标卡片为 M1 白卡，请点击“写 M1”，选择数据文件写入卡片。若询问 KeyABN，选择“取消”即可。
- c) 若目标卡片为 UID/UFUID 卡，请点击“UID 写”，选择数据文件写入卡片。若为 UFUID 卡，请点击“锁 Ufuid”将卡片锁定。
- d) 若目标卡片为 CUID/FUID 白卡，请点击“CUID 写”选择数据文件写入卡片。若询问 KeyABN，选择“取消”即可。

7 Hardnested 云计算服务

若在本地图算性能低下或占用过多资源，又或是需要较高的解算速度，可以使用云计算服务。步骤如下：

1. 在 HardNested 初始化界面设置好参数后，勾选“只收集不计算”。
2. 收集完成后会显示本次的数据文件名。
3. 打开云计算服务页面，输入您的计算序列号并上传收集的数据文件（后缀.nbf）。
4. 成功提交后会弹出窗口显示您的 JobID，请注意保存。
5. 刷新页面，等待结果。

若提示计算失败，可重新收集尝试。

附 1 手机/手环模拟卡实战

1. 连接 NFC 设备，打开软件，点击“检测设备”，确认可以找到 NFC 设备。
2. 放置原卡，点击“手动扫描”，确认原卡的 SAK 为 08/28。



3. 按照本手册 6.1 部分的内容读取原卡数据。
 4. 下面需要制作一张与原卡 UID 相同的白卡。可选用 UID/CUID 中的一种。
 - a) 若使用 UID 白卡：
 - i. 放置原卡，点击“手动扫描”，复制卡片的 UID（八位字符）。
 - ii. 放置 UID 卡，点击“UID 写号”，将卡片 UID 粘贴在对话框中，去掉其中任何空格，保证最终输入的只有 8 位字符（如“1eec44ef”这样子就是正确的）。
 - b) 若使用 CUID 白卡：
 - i. 放置原卡，点击“手动扫描”，复制卡片的 UID（八位字符）。
 - ii. 点击“Hex 编辑器”，打开 S50HTool。
 - iii. 点击菜单“文件”-“新建”（快捷键 Ctrl+N）。
 - iv. 点击菜单“工具”-“修改 UID”（快捷键 Ctrl+U），将卡片 UID 粘贴在对话框中，去掉其中任何空格，保证最终输入的只有 8 位字符（如“1eec44ef”这样子就是正确的）。
 - v. 点击菜单“文件”-“另存为”（快捷键 Ctrl+Shift+S），将仅含有卡号的数据文件保存。
 - vi. 关闭 S50HTool，回到主界面。放置 CUID 卡，点击“CUID 写”，选择刚刚保存的仅含有卡号的数据文件。若询问 KeyABN，选择“取消”即可。
 5. 使用手机/手环模拟制作好的白卡。
 6. 调起手机/手环刷卡模式，放在 NFC 设备上。
 7. 点击“写 M1”，选择读取出的原卡数据文件。若询问 KeyABN，选择“取消”即可。
 8. 测试模拟卡是否可以正常使用。
- 若手环调起刷卡的时间窗口太小来不及操作，可先做第 7 步，然后调起刷卡放在设备上，软件会自动执行等待卡操作，检测到卡片后再操作。

