

魔锐 1 开发指南

Version 1.0.0.0

许可协议

同意本许可协议的所有条款及此处包含的任何补充或特殊的许可条款是获得本产品许可的必要条件。如果您不同意此协议的所有条款，请在三天内将产品退还北京深思数盾科技股份有限公司。您对本软件的使用将表明您同意接受本协议中条款的约束。

1. 授予您使用许可权。您可以为了备份的目的而复制磁盘中的软件，可以为了将本产品集成到您的软件的目的，根据本产品的文档说明将我们提供的软件合并进您的程序中。
2. 除已按上述第一条被授权外，不可以复制、修改、逆向工程、分解或重组该产品的全部或部分，不可向他人销售、租借、许可、转让、分发全部或部分本产品或本协议授予的权利。
3. 保证在自产品交给您之日起的 12 个月内，在正常使用情况下，产品不会出实现质性的材料上和生产制造上的缺陷。北京深思数盾科技股份有限公司的全部责任和您能获得的全部补救措施为：可选择尝试更换或修理或其他补救措施。
4. 除了上述对本产品的原始购买者所提供的有限保证之外，不向任何人作任何其他的保证。对北京深思数盾科技股份有限公司的产品、性能或服务亦没有明示的或暗示的或其他任何形式的保证，包括但不限于商品的适销性和对特定用途的适用性。
5. 任何情况下，无论如何引起及依据何种责任理论，均不负担任何因使用或不能使用本产品造成的损失责任，包括：丢失数据、损失利润及其他特别的、偶然的、附随的、继发的或间接的损失。
6. 所有的产品，包括魔锐 1 设备、软件、文档、与本产品一并附送的其他材料及您制作的备份的所有权与版权均属于北京深思数盾科技股份有限公司。
7. 违反上述条款时，本协议的授权将自动终止。

“魔锐”是北京深思数盾科技股份有限公司的注册商标。

本文所涉及的其他产品和公司名称可能是各自相应所有者的商标。



联系深思数盾

公司名称：北京深思数盾科技股份有限公司

办公地点：北京市海淀区西北旺东路 10 号院 5 号楼软件园二期互联网创新中心 C510

邮 编：100872

电 话：+86-10-556730936

传 真：+86-10-556730936

电子邮件：sense@sense.com.cn

网 址：<http://www.sense.com.cn>

阅读指南

【手册目标】

本手册主要对北京深思数盾科技股份有限公司开发的魔锐 1 加密锁的使用进行说明，由于实际情况千变万化，本手册很难一次做到面面俱到，需要逐渐完善。

【手册约定】



手册中出现该标志的地方表示需要您引起高度重视，否则可能会引发严重的后果。



手册中出现该标志的地方表示需要您特别引起注意的内容。

目 录

| | | |
|-------|---------------|----|
| 第 1 章 | 产品简介..... | 2 |
| 1.1 | 了解魔锐 1..... | 2 |
| 1.2 | 产品特点..... | 2 |
| 1.3 | 工作原理..... | 3 |
| 1.4 | 名词解释..... | 3 |
| 第 2 章 | 魔锐工具..... | 5 |
| 2.1 | 开发测试工具..... | 6 |
| 2.1.1 | 功能菜单..... | 7 |
| 2.1.2 | 基本信息..... | 7 |
| 2.1.3 | 文件管理..... | 8 |
| 2.1.4 | PIN 管理..... | 11 |
| 2.2 | 批量设置工具..... | 12 |
| 2.3 | 密码学算法工具..... | 13 |
| 2.4 | 加壳工具..... | 20 |
| 2.5 | 制作升级包工具..... | 21 |
| 2.6 | 用户升级工具..... | 22 |
| 第 3 章 | 基本应用..... | 23 |
| 3.1 | 数据保护..... | 23 |
| 3.2 | 密码算法保护..... | 23 |
| 3.3 | 身份认证..... | 23 |
| 3.4 | 加壳保护..... | 24 |
| 3.5 | 综合保护..... | 24 |
| 3.6 | API 使用..... | 25 |
| 第 4 章 | API 函数概要..... | 26 |
| 4.1 | 基本操作类..... | 26 |
| 4.2 | 初始化类..... | 27 |
| 4.3 | 文件操作类..... | 27 |
| 4.4 | 密码算法类..... | 28 |
| 4.5 | 远程升级类..... | 28 |
| 第 5 章 | 附录 I..... | 29 |

第1章 产品简介

1.1 了解魔锐 1

魔锐 1 是北京深思数盾科技股份有限公司开发的一款加密锁，是具有很高性价比的产品。虽然价格较低，但是魔锐使用的是 32 位智能卡芯片，安全性高、速度更快、锁内存储容量更大；

魔锐 1 是基于硬件（智能卡）的软件防盗版系统，数据与密钥以文件的形式保存在智能卡芯片内部，避免盗版者窃取与复制。魔锐 1 还支持国际标准的 AES、DES、RSA 加密算法技术，开发过程中配合使用这些加解密算法，可以极大增强防盗版保护方案的安全强度。为了便于开发，我们还提供的加壳工具，能够让开发商不写任何代码的情况下，实现高强度的软件保护。另外，魔锐 1 还提供了标准的 HMAC-SHA1、HMAC-SHA256 和 HMAC-MD5 算法功能，可用于认证网络客户端的身份，实现身份认证功能。

1.2 产品特点

- **32 位智能卡芯片**

魔锐 1 采用 32 位智能卡（Smart Card）芯片，性能和安全性得到大幅提升。配合魔锐 1 开发系统提供的工具链，绝对可以为您提供可靠的加密保护。

- **高级加密算法**

魔锐 1 支持 AES、DES、TDES、RSA 和 ECC 高级加密算法，密钥以文件的方式保存在智能卡芯片内部，不可读出，只能使用，保证了密钥的安全性；

- **大容量数据存储空间**

按照容量不同，魔锐 1 分为 8K 版本和 32K 版本，并支持文件系统，可以让您存放需要的数据及密钥文件，满足您对数据存储需要。

- **安全隧道技术**

魔锐 1 利用 AES 算法建立了与设备通信的“安全隧道”，并使用了随机加扰措施，让破解者无法通过数据侦听来获得有效的信息，从而提高了软件保护的安全强度。

- **无需安装驱动**

魔锐 1 设备支持自适应驱动方式，在您没有安装驱动时，魔锐 1 设备会被识别成 HID 模式，如果您有特殊需求，安装了我们的驱动包，魔锐 1 设备会被识别成 USB 模式。

- **加壳工具**

魔锐 1 开发系统，自带深思数盾高强度外壳，能让您不写一行代码，实现软件保护。加壳后的程序与您要发售的魔锐 1 硬件锁绑定，只有插入您发售的硬件锁，软件才能运行。

- **全球唯一序列号**



全球唯一序列号是魔锐 1 出厂时设定的硬件序列号，您可以利用它来实现软件与设备的绑定或者实现产品的跟踪与追溯。

- **高度集成技术**

魔锐 1 的 CPU 内核、ROM、RAM、非易失性存储器这些关键部件全部在单一的硅片上集成制造，使其稳定性达到了前所未有的高度，从而最大程度的降低了由于坏锁和丢锁问题所带来的风险。

- **HMAC 算法**

魔锐 1 支持 HMAC-SHA1、HMAC-SHA256、HMAC-MD5 算法，可以实现“挑战-响应”方式的认证，从而保证用户的合法性。兼容多种算法，可以方便您选择使用。

- **可控的 LED 状态**

魔锐 1 支持 LED 状态的控制功能，即可以设置 LED 的状态为亮或灭，合理的利用此功能，可以让软件开发商或者最终用户方便的查看加密锁的实际运行状态。

- **高速性**

魔锐 1 支持全速 USB2.0。

- **支持远程升级**

采用内置安全密钥，远程签发升级包，可直接升级加密锁，方便安全。

- **支持批量生产**

开发包自带批量生产工具，可以直接完成加密锁批量设置，不需要再开发生产工具。

1.3 工作原理

魔锐 1 提供了大容量存储空间，并支持以文件系统方式管理，用户可以将重要的数据存放到加密锁的数据区中，当软件中需要用到这些数据时，可以使用我们提供的 API 函数，通过验证需要的权限后，读取加密锁中的数据。这样，就可以实现将软件与加密锁绑定在一起，达到保护软件的效果，

您也可以把密钥数据以文件的形式存放到加密锁中，密钥数据无法被读出加密锁，只能通过调用我们提供的 API 接口，验证安全权限后，使用加密锁内的密钥文件对需要重要的数据进行加解密或签名验签操作，如果配合数据存储功能，可以实现更高强度的加密保护方案。

魔锐 1 还提供了加壳工具，可以实现一键式快速安全的加密保护，加壳后的程序就与您的魔锐 1 进行绑定，只有插入您发售的魔锐 1，才能启动运行您的程序了。

魔锐 1 还提供了标准的 HMAC-SHA1、HMAC-SHA256 和 HMAC-MD5 算法功能，密钥同样以文件方式存储在加密锁内部，不可读出，通过 API 接口使用加密锁内部密钥文件计算 HMAC，可用于实现挑战响应式身份认证，保证身份认证的安全可靠。

1.4 名词解释

- **全球唯一序列号**

全球唯一序列号是魔锐 1 出厂时设定的硬件序列号,您可以利用它来实现软件与设备的绑定或者实现产品的跟踪与追溯。

- **种子码**

种子码是在设置 PID 时使用,种子码是生成产品 PID 的重要数据,需要妥善保存,只有相同的种子码才能生成相同的 PID。

- **PID**

产品标识,通过种子码生成,可以用于标识某一类产品或某个子开发商,是你区别于其他产品魔锐的一个标识,使用魔锐前必须先设置产品 PID。



- ◆ 所有的魔锐出厂状态的 PID 都是一样的,默认为"0",使用前请务必修改设置成自己的 PID,否则无法使用初始化锁以外的任何功能。
- ◆ 设置 PID 需要开发商权限,获取开发商权限后,PID 可以重复设置。
- ◆ 某个种子码生成的 PID 是唯一的,不同的种子码生成的 PID 不同,所以,在设置某一类型产品的时候,请务必使用相同的种子码进行 PID 设置,否则,将生成不同的 PID 加密锁;

密码及权限

魔锐 1 使用密码来管理不同的权限,密码验证通过后即可获得相应的权限,魔锐 1 共设置了三种不同的权限,即开发商权限、用户权限和默认权限。

➤ 开发商权限

开发商权限是您管理魔锐 1 设备时所使用的权限,您必须验证开发商密码才拥有操作魔锐 1 设备的最高权限,验证通过后可以完成文件的读写,文件的删除,设置密钥,重置密码,恢复出厂等管理级别的操作。

➤ 用户权限

普通用户密码验证通过后,可以用于读取加密锁内的数据文件,也可以对有用用户写权限的文件进行读写操作,还可以调用 API 接口,使用锁内的密钥文件。

➤ 默认权限

不需要验证密码,直接通过魔锐 1 API 可以进行的操作权限,主要是用来获取设备的一些信息与状态。



- ◆ 在您收到魔锐 1 之后，请务必将开发商密码更改为自己的开发密码，只有修改了密码后，才能使用相关加密锁的应用功能。
- ◆ 由于开发商密钥是管理设备的最高权限，拥有对锁的所有操作权限，所以，请妥善保存好修改后的开发商密码，这是保护你加密方案安全性的重要保障之一。

对于上述几个名词的其它属性，请参见表 1-1 中的内容。

表 1-1 名词的属性

| 名词 | 长度 | 初始值 | 唯一性 | 软件开发商是否可更改 |
|---------|---------|------------------------------------|--------------|--------------------------|
| 全球唯一序列号 | 16 字节 | 各设备均不相同 | 全球唯一 | 不可更改 |
| 种子码 | 4~32 字节 | 无 | 您自己设置 | 需要妥善保管，验证开发商权限后，可以用新的种子码 |
| PID | 4 字节 | 0 | 根据种子码和随机算法生成 | 可以重新初始化 |
| 开发商密码 | 24 字节 | “00000000000000000000000000000000” | 软件开发商自己设置 | 可更改 |
| 用户密码 | 8 字节 | “00000000” | 软件开发商自己设置 | 可更改 |

第2章 魔锐工具

为了快速方便的使用魔锐 1，我们提供了一整套的工具链，工具链包含了魔锐 1 的所有功能，使用工具链中的工具，可以快速的完成从加密方案开发、测试，以及生产整个流程，方便快捷。

工具链包含了：开发测试工具、密码学算法工具、加壳工具、批量生产工具, 以及远程

升级工具，除加壳工具外，其他工具都放在开发包的 Tools 目录中，加壳工具单独放置 shell 目录中，各工具的作用如表格 2-1 魔锐 1 工具链中的内容所示。

| 文件名 | 工具名称 | 作用 |
|---------------------|-----------|--|
| DevTestTool.exe | 魔锐开发测试工具 | 初始化魔锐 1 设备，比如生成或修改 PID、修改 PIN 码；文件操作，如：新建、导入、删除、编辑等； |
| CryptoTool.exe | 密码学算法工具 | 测试使用您想使用的各种加密算法，生产相关魔锐 1 密钥文件 |
| BatchTool.exe | 批量设锁工具 | 使用生成的模板，批量生产 PID 相同的锁 |
| UpdateTool.exe | 用户升级包导入工具 | 给您的客户使用，可以把您传给客户的升级包导入到锁中 |
| virboxprotector.exe | 加壳工具 | 提供一种更便利的保护方式，可以实现不写代码和锁进行关联 |

表格 2-1 魔锐 1 工具链

2.1 开发测试工具

魔锐开发测试工具是使用魔锐 1 最常用的工具，该工具不仅可以用来初始化设置加密锁，还可以用来开发测试加密方案。插入一把魔锐 1 设备，双击开发包 Tools 目录中的“DevTestTool.exe”启动魔锐开发测试工具，其界面如图 2-1 所示

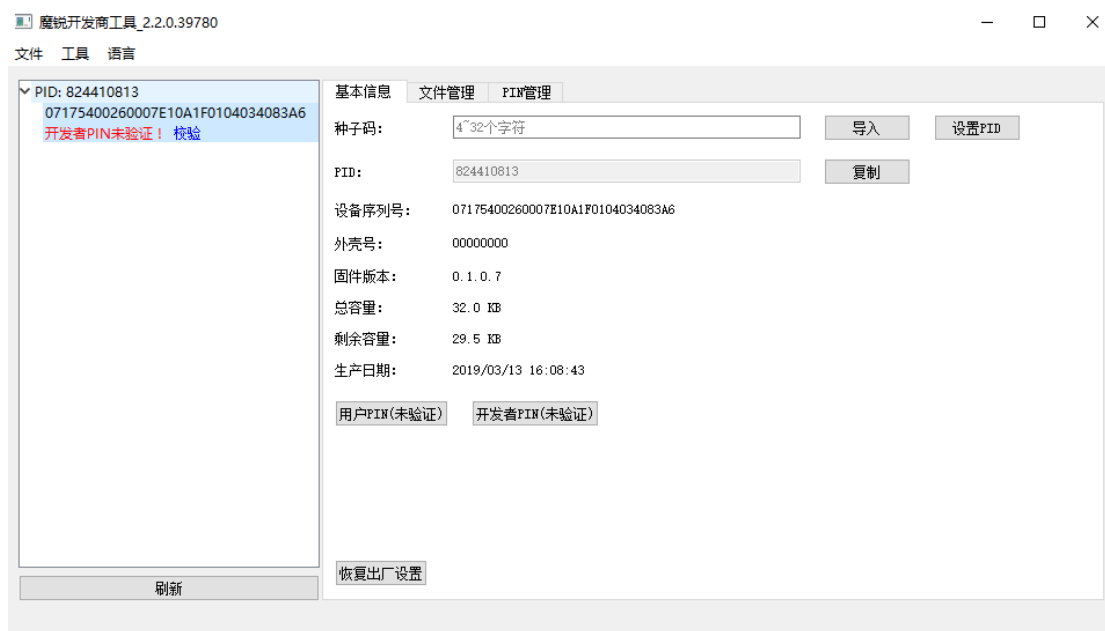


图 2-1

从图中可以看出，工具启动后，在左侧设备栏中会显示当前主机上的所有魔锐设备，你可以选择你需要操作的设备，在右边的页签栏选择进行的操作。在基本信息页签栏显示当前选择设备的基本信息，在这里您可以查看到设备序列号、PID、外壳号等一些基本信息，在此页面，你还可以进行设备 PID 的设置、恢复出厂、校验 PIN 码等操作。在文件管理页签进行锁内文件的管理，您可以管理当前选择的设备内部文件，比如：查看文件属性、创建文件、导入文件以及删除文件，还可以使用锁内的密钥文件，进行一些密码学算法的验证。在 PIN 管理页签，您可以修改开发商密码和用户密码，设置错误限制次数。

2.1.1 功能菜单

功能菜单主要包括工具的退出与其他相关辅助工具的打开，以及工具语言显示选择。

❖ 文件

是对本工具的操作，目前主要是退出功能。

❖ 工具

这里可以打开其他 3 个辅助工具：密码学算法工具、批量设置工具、升级包制作工具，后面章节会详细说明。

❖ 语言

可以选择工具使用的语言类型，目前支持中文与英文两种。

2.1.2 基本信息

基本信息页签如图 2-1，主要是显示设备基本信息，校验 PIN 码操作，并提供 PID 设置功能。

显示的主要信息有 PID、设备序列号、外壳号（锁外壳激光印制号）、固件版本、总容量、剩余容量和生产日期。

开发测试工具的很多操作都是需要权限的，基本信息下方的两个按钮分别用于用户权限与开发商权限的验证，当验证过权限后，相应的按钮会由“未验证”转变为“已验证”显示状态，同时，在左侧的设备列表栏中选择的设备下面的状态也会变为“用户 PIN 已验证”或“开发商 PIN 已验证”状态。

在这个页面还可以进行设备的 PID 设置，在种子码编辑框中直接输入 4~32 字节长度数据，或者使用导入按钮导入种子码文件数据，点击设置 PID 按钮，可完成设备 PID 的设置工作。



- ◆ 种子码是生成 PID 的唯一信息，只有相同的种子码才能生成相同的 PID，所以，请妥善保管好种子码，避免泄露或遗忘。

2.1.3 文件管理

魔锐的文件类型主要有数据文件与密钥文件两种类型。数据文件又分为用户只读文件与用户读写文件两种类型，开发商可以创建不同类型的数据文件，实现用户端文件的读写控制。密钥文件是不可读取的，只能使用，即使是开发商权限也不能读取，保证密钥的安全性。

文件管理页面主要功能是管理锁内文件，通过文件管理页面可以编辑数据文件，或使用设备内密钥文件进行加密算法测试验证，如图 2-2 所示：



图 2-2

文件管理页面所有管理操作都是需要具有开发商权限，所以需要先在基本信息页面验证开发商 PIN，获得开发商权限后，才能使用此页面的相关管理功能。

文件管理页面的左侧是设备内的文件列表，右侧是文件相关信息与可进行的功能操作组件，当选中某个文件时，右边相应的显示此文件的文件名、文件类型、文件大小及创建时间等文件的基本信息。根据文件类型不同，右侧还会显示的不同编辑测试功能操作组件。

文件列表下方是一些文件操作的功能按钮，通过这些按钮可以刷新文件列表中的显示，新建一个数据文件到所选择的设备内部，或是导入一个密钥到设备内部，还可以删除指定的文件。

当左侧选择的是数据文件时，显示如图 2-3，会显示文件数据内容，数据文件根据权限不同分为用户只读文件与用户读写文件，根据选择的数据文件权限与当前操作的设备权限状态，数据编辑框内数据会显示可编辑或不可编辑两种状态，如果是开发商权限，或者文件是用户读写权限，数据编辑框内数据均可以修改，编辑完成后，可以直接将编辑好的数据保存到设备内部，也可以将编辑好的数据文件导出保存到本地电脑。

提示：在编辑状态，你可以直接编辑编辑框内数据，可以使用ctrl+c 或ctrl+v 进行复制粘贴操作，也可以直接导入外部数据；

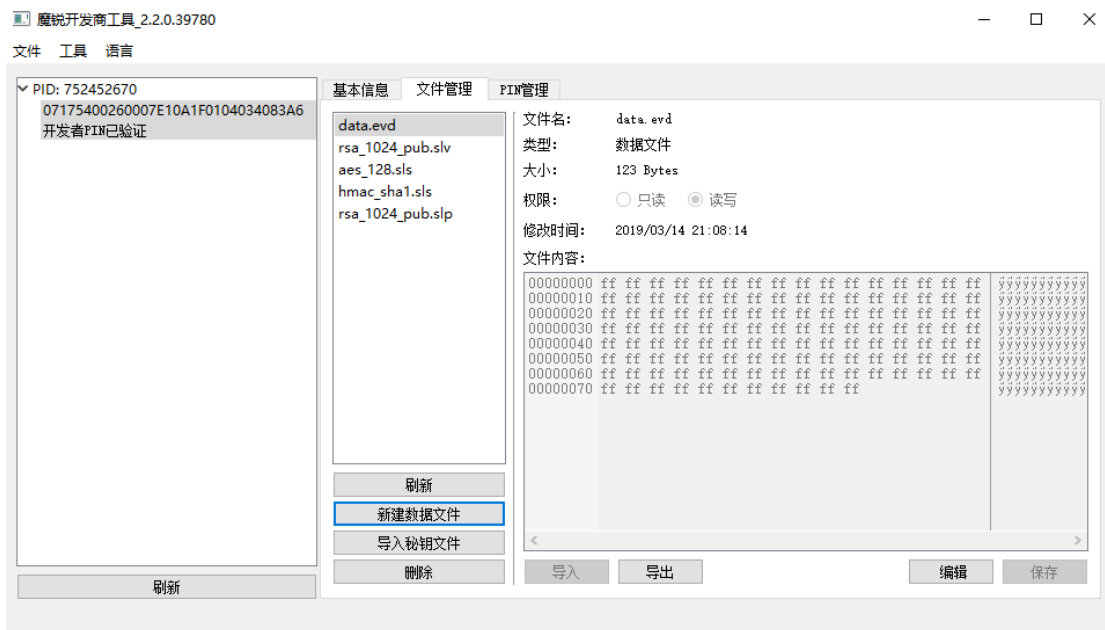


图 2-3

当左侧选择的是密钥文件时，显示如图 2-4，会显示个密钥测试的按钮，点击按钮后进入密钥测试页面，对密钥文件可以进行三种测试：签名/验签测试、加密/解密测试与 Hmac 测试，如图 2-5、图 2-6、图 2-7。



图 2-4

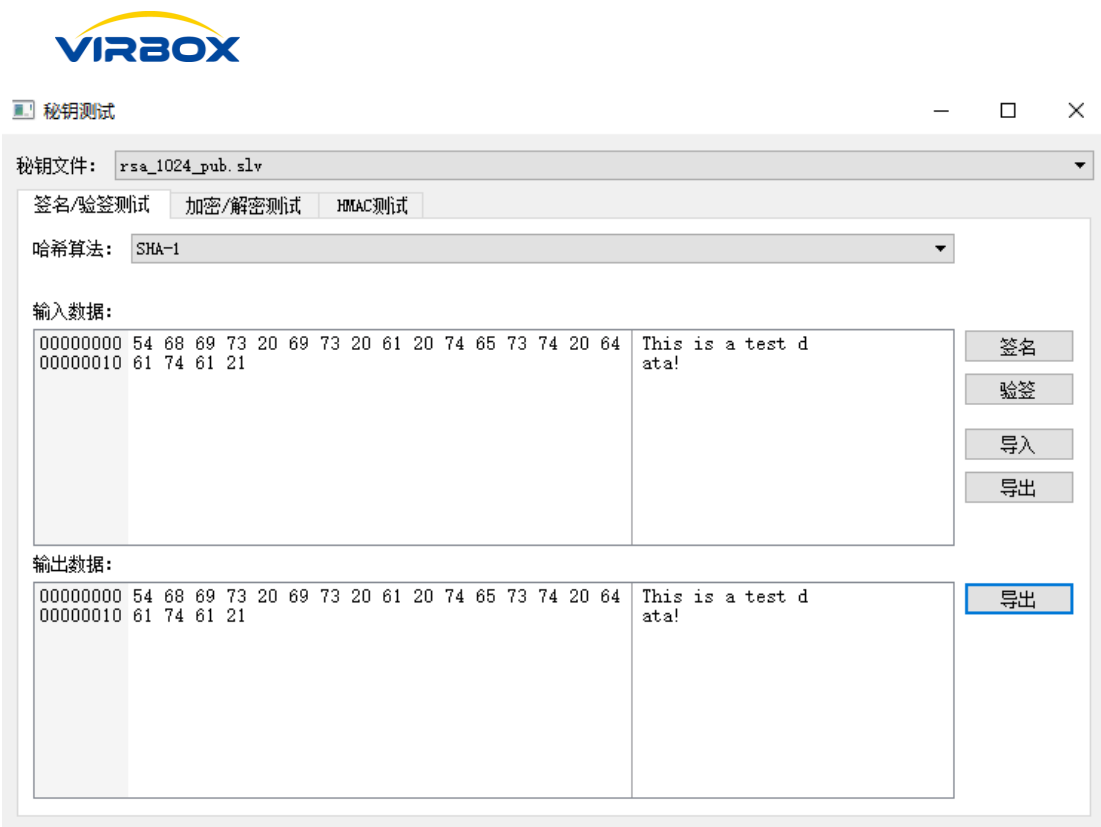


图 2-5

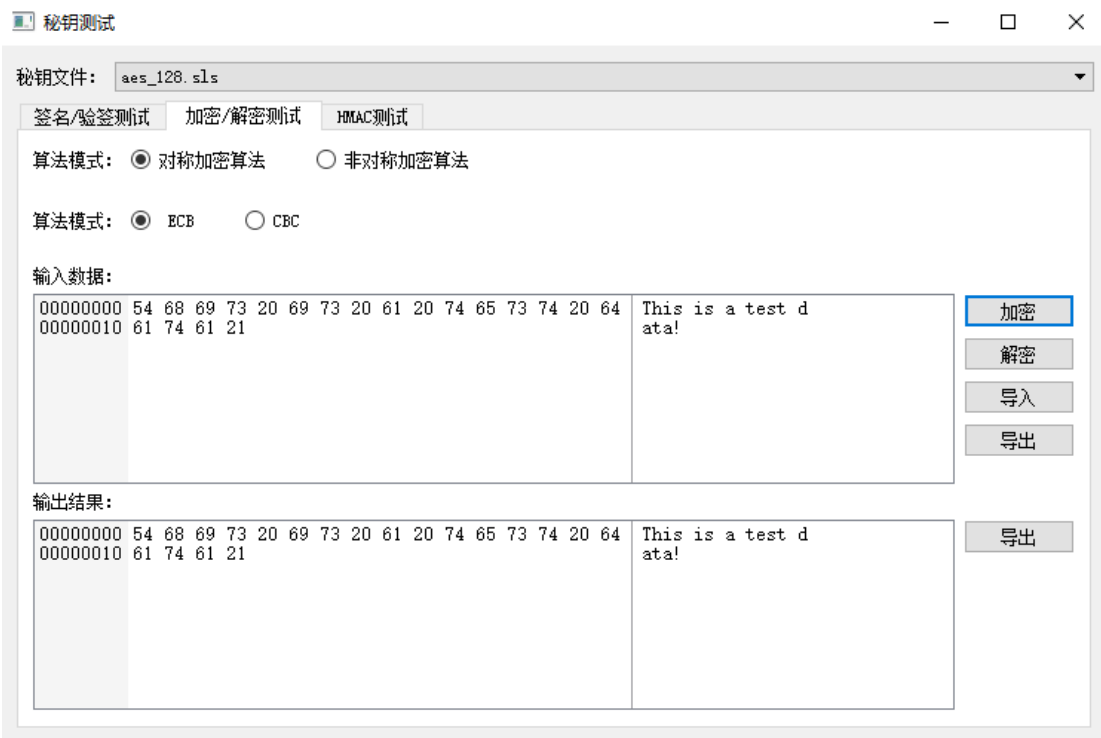


图 2-6

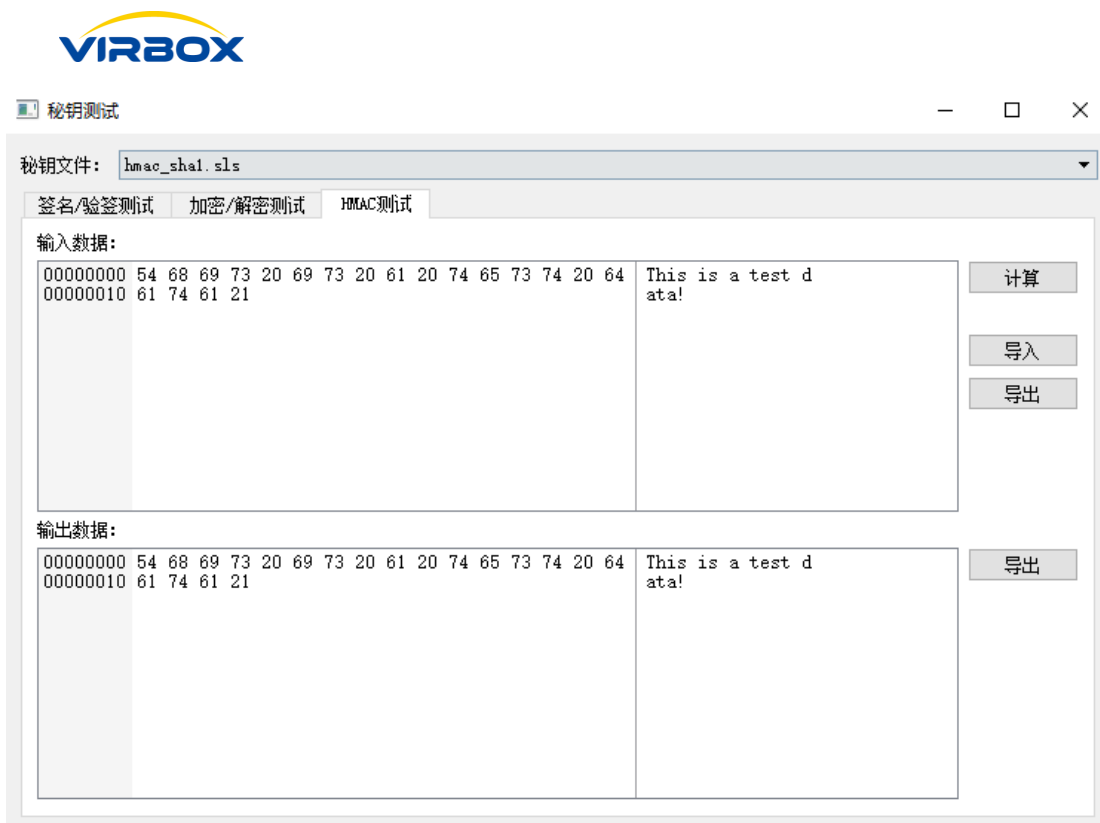


图 2-7

在密钥测试对话框中，你可以在密钥文件下拉列表中，选择当前选择设备的内部的密钥文件，进行设备内部密钥文件的相关算法测试，在签名/验签测试、加密/解密测试、Hmac测试三个签页中，分别有各自的算法相关模式及参数的选择，数据输入框，以及数据输出框，可以很方便灵活的完成对应算法的各个模式及数据进行测试。另外，页面还提供了编框内数据的导入导出功能，可以实现与其他工具程序的配合测试。

2.1.4 PIN 管理

PIN 管理页面主要是管理锁的开发商 PIN 码和用户 PIN 码，在 1.4 章中，这里主要是设置修改对应的 PIN 码。具体操作如图 2-8 所示：



图 2-8



- ◆ 最大尝试次数为 1~15 次，如果在修改 PIN 过程中不填写，则默认为不设置错误尝试次数限制功能。

2.2 批量设置工具

批量设置工具的主要作用是让你的设计方案批量生产设置到加密锁里。当你在批量设置工具中设计好加密方案后，您可以对单个锁进行设置，也可以对多个锁同时进行设置，你可以将工具中设计好的加密方案保存成模板，方便后续再次批量设置使用，在后续使用中，你只需要导入使用之前已经制作保存的模板，点击开始批量制作按钮即可，不需要在工具中重新设计自己的加密方案。

双击开发包 Tools 目录中的“BatchTool.exe”启动魔锐批量设置工具，工具界面如图 2-9，左侧为当前主机所有设备，设备签名红色标记代表没有进行量产。设计新的加密方案，需要确认种子码信息，即：先填入右侧种子码数据，也可以外部导入种子码文件，点击生成 PID 测试，验证是否种子码生成的 PID 是即将批量生产的产品类型。确认过 PID 后，可以在 PIN 码设置栏输入新旧 PIN 码，设置 PIN 码的校验次数限制，如果不想做限制，不填数据为空即可。在文件设置区域进行加密方案文件设置，可以导入数据文件与密钥文件，数据文件需要根据方案需求设置对应的权限，设置完文件，此时，加密锁端加密方案设置完成，点击最下面的按钮即可开始批量生产，当生产完成后，左侧设备列表栏中的设备前面红色标记变为绿色，标记量产成功，更新生产计数。



在工具右上方，有两个模板管理按钮，可以将当前加密锁设计方案保存为一个模板，也可以导入模板，直接使用导入的模板，直接开始量产。

注意：确认种子码信息，需要当前主机至少有一把设备存在，用于生成PID验证；正常批量生产的设备都是出厂魔锐，出厂魔锐开发商默认PIN为24字节“0”，所以，在开发商旧PIN中设置为24字节“0”即可，如果是再次批量，旧的PIN码需要输入设备当前的开发商PIN码；

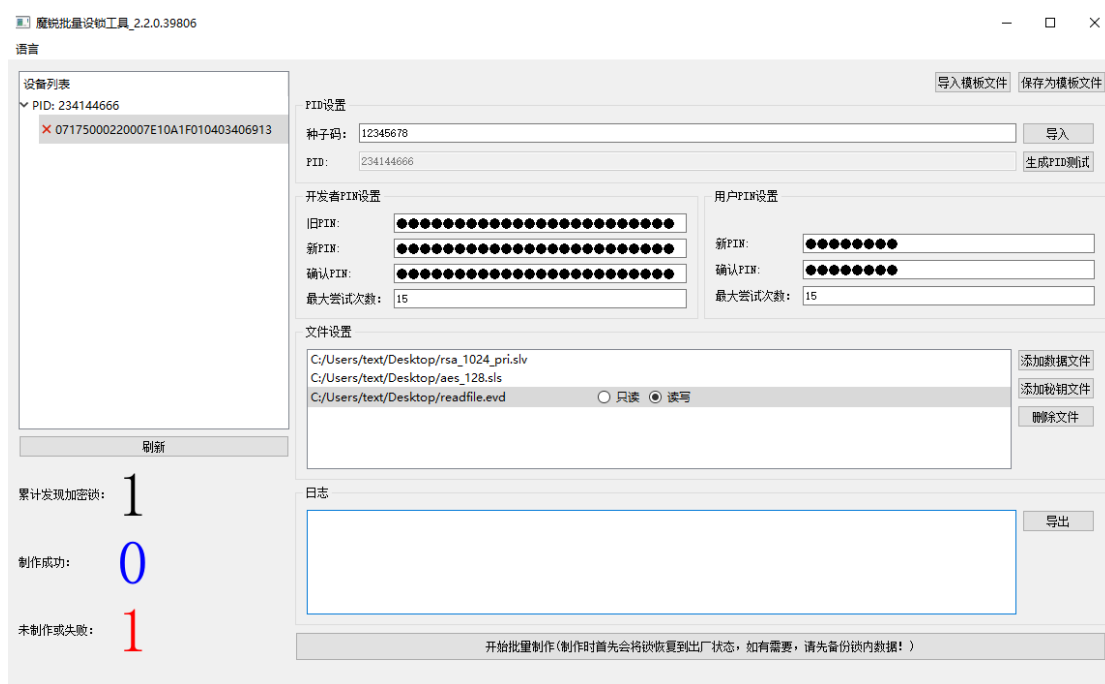


图 2-9

2.3 密码学算法工具

密码学算法工具是纯软件实现的工具，所有功能都是通过主机运算实现的，和加密锁硬件设备无关；

密码学算法工具的主要作用是生成密钥文件，并可以对密钥文件进行测试。

注意：魔锐1的密钥文件具有特殊的格式，必须要通过密码学算法工具或密码学API工具生成

双击开发包 Tools 目录中的“CryptoTool.exe”启动魔锐密码学算法工具，其界面如图 2-10 所示，工具菜单有文件与语言两个，可以选择中英文两种显示。算法工具按功能模块区分，可以分为：签名/验签、加密/解密、HASH/HMAC、随机数四个部分，如图中左侧功能选择栏。



图 2-10

❖ 签名/验签

选择签名/验签按钮后，工具右侧显示如图 2-11，在下拉菜单中选择需要生成密钥算法类型，目前支持 ECC-192、ECC-256、RSA-1024、RSA-2048。

点击生成密钥文件按钮后，可以直接选择密钥文件的保存目录，确定后生成公私钥文件到指定保存地址；

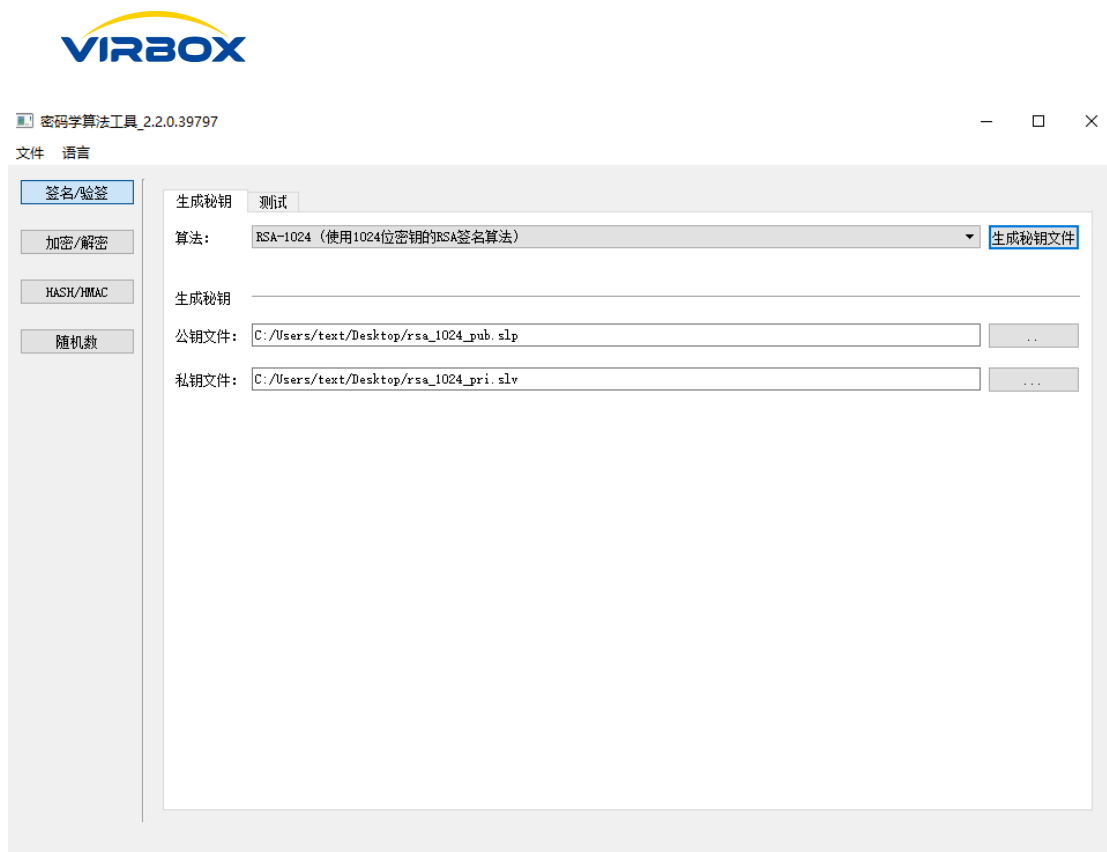


图 2-11

选择右侧测试页签，如图 2-12，公私钥文件会直接显示生成密钥页签生成的文件，也可以自己重新选择需要验证的密钥文件，之后选择签名需要使用的哈希算法，为了方便操作，签名数据框与签名结果框数据都是可以直接编辑或导入导出数据，这个使得签名验签更加方便灵活，当数据编辑完成后，点击签名或验签即可完成测试，工具会提示测试结果。

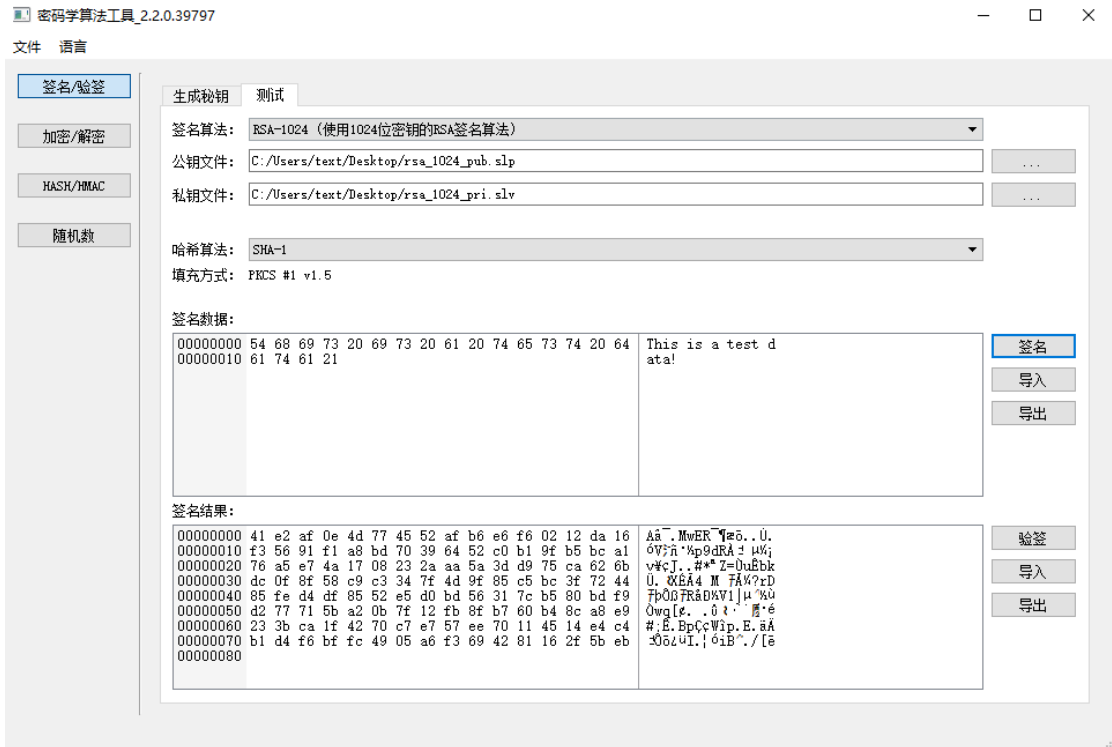


图 2-12

注意：使用密码学算法工具验证密钥文件，选择的文件一定要与选择的密码学算法匹配，否则会测试失败，会报文件类型错误；数据编辑框可以使用ctrl+c 或ctrl+v 进行操作，更加便捷；

❖加密/解密

选择加密/解密按钮后，工具右侧显示如图 2-13，在下拉菜单中选择需要生成密钥算法类型，目前支持 ECC-192、ECC-256、RSA-1024、RSA-2048。

点击生成密钥文件按钮后，可以直接选择密钥文件的保存目录，确定后生成密钥文件到指定保存地址；

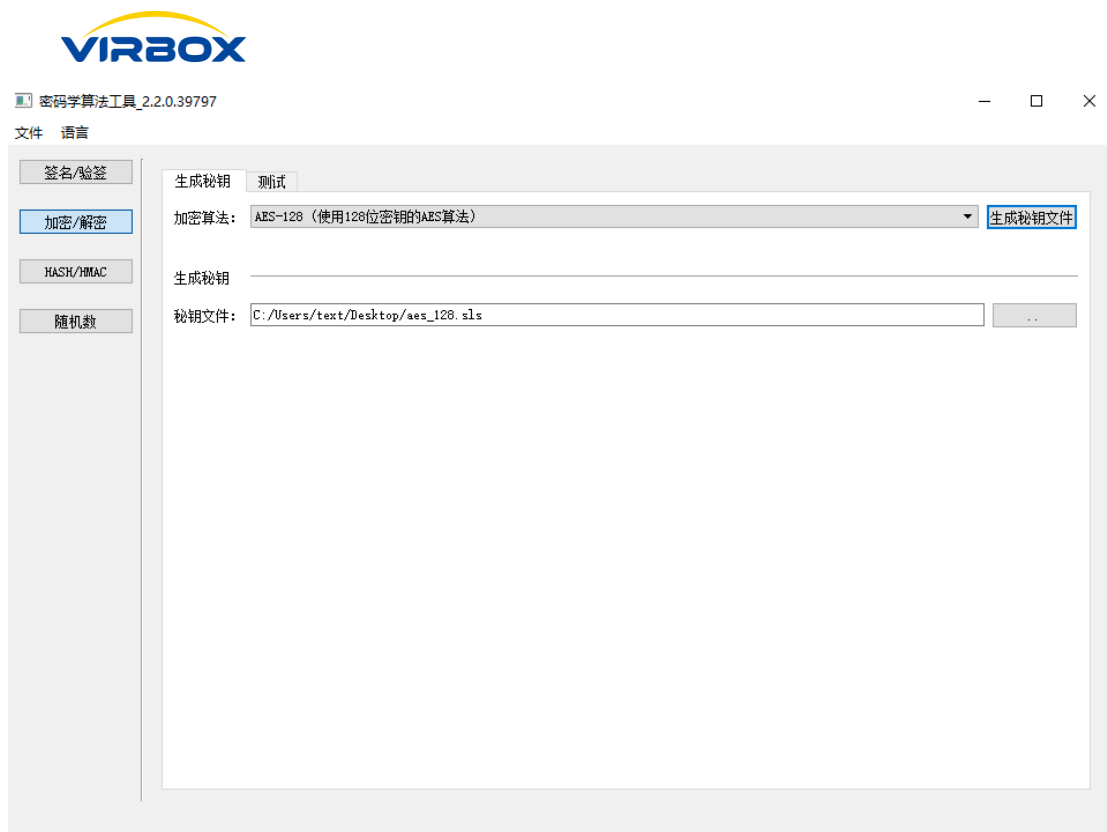


图 2-13

选择右侧测试页签，如图 2-13，密钥文件会直接显示生成密钥页签生成的文件，也可以自己重新选择需要验证的密钥文件，之后选择加密算法模式，根据选择算法不同，模式选项也不相同。为了方便操作，加密数据框与解密数据框都是可以直接编辑或导入导出数据，这个使得签名验签更加方便灵活，当数据编辑完成后，点击加密或解密即可完成测试，工具会提示测试结果。

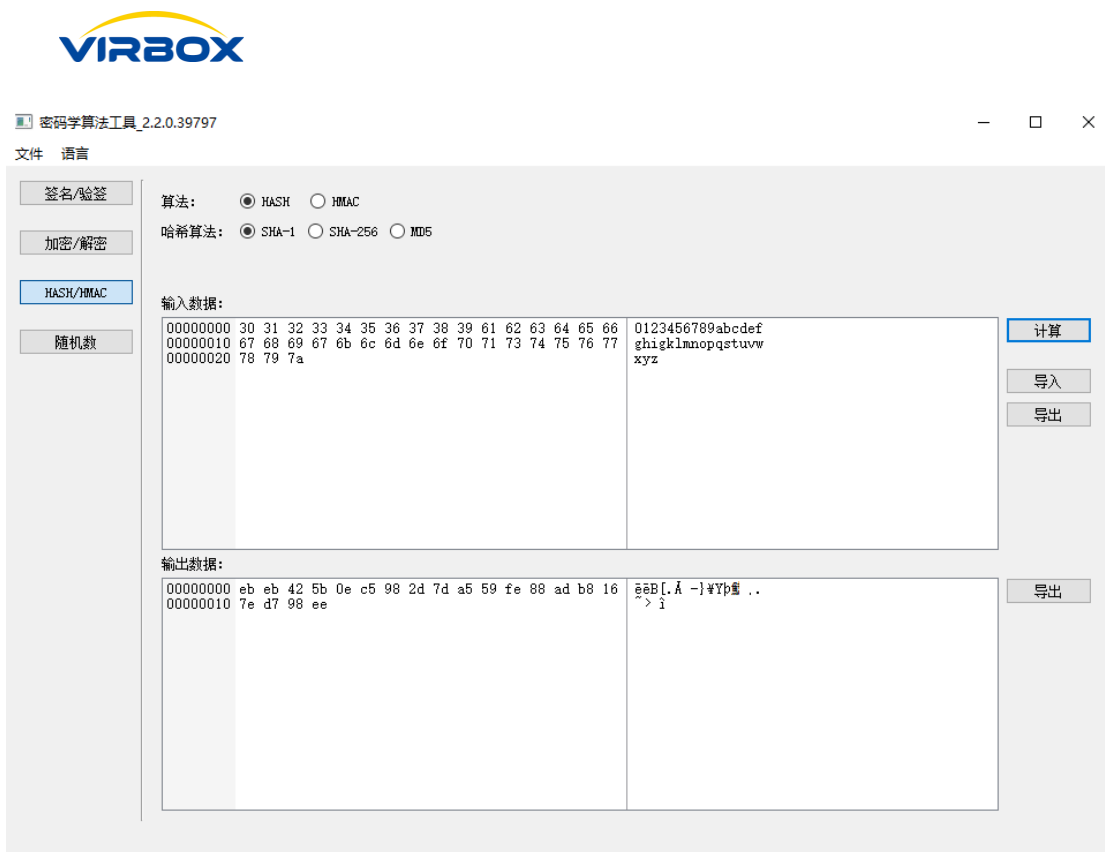


图 2-14

❖HASH/HMAC

选择 HASH/HMAC 按钮后，工具右侧显示如图 2-14，HASH 与 HMAC 算法均支持哈希算法 SHA-1、SHA-256 与 MD5 三种类型计算。

当选择 HASH 算法，如图 2-14，选择需要使用的哈希算法类型，为了方便操作，加输入数据框都是可以直接编辑或导入导出数据，输出数据是可以直接导出，编辑好输入数据后，点击计算按钮既可以完成算法的计算测试。

当选择 HMAC 算法时，如图 2-15，选择需要使用的哈希算法类型，输入密钥长度，点击生成可以生成 HMAC 密钥到指定位置，也可以直接选择本地的 HMAC 密钥文件，为了方便操作，加输入数据框都是可以直接编辑或导入导出数据，输出数据是可以直接导出，编辑好输入数据后，点击计算按钮可完成 HMAC 计算测试，工具会提示计算结果：

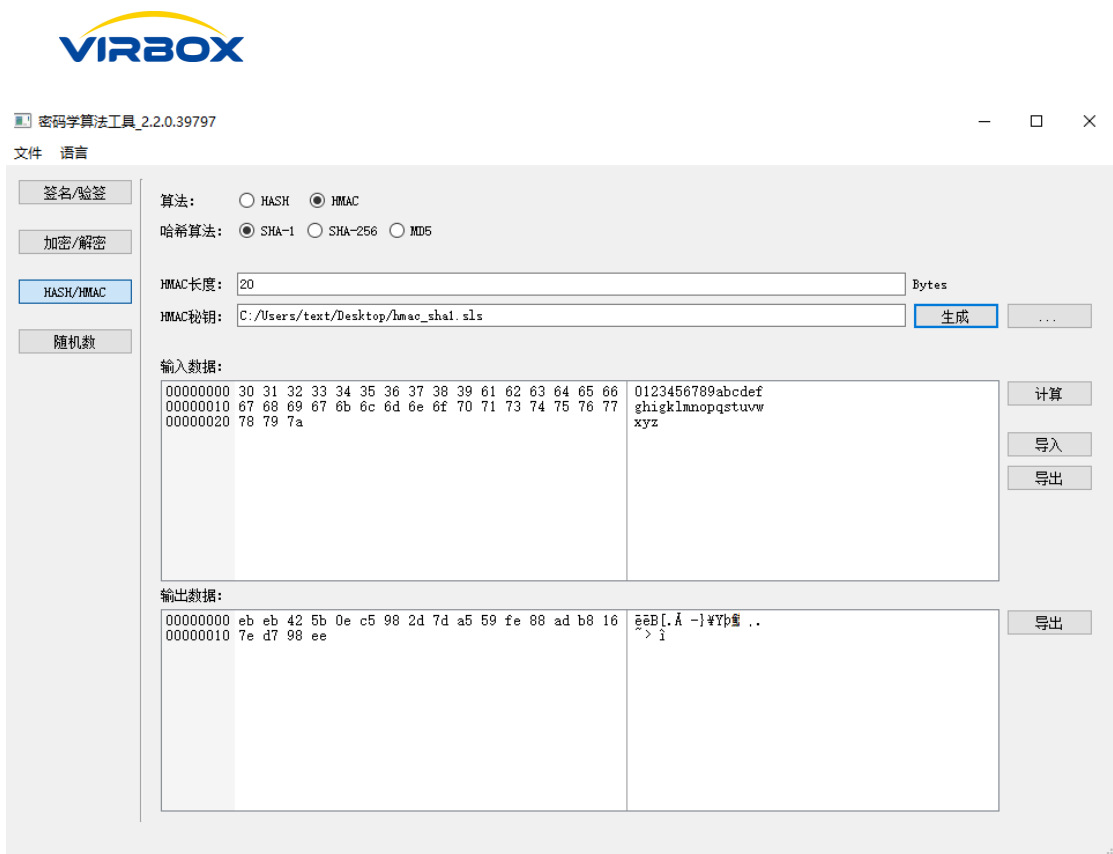


图 2-15

❖ 随机数

随机数功能可以生成指定数据长度的随机数据，很方便作为密钥、密码、挑战数据使用，随机数页签如下图 2-16，填入随机数长度，点击生成按钮，在数据框中生成指定长度的随机数据，可以直接导出保存到本地。

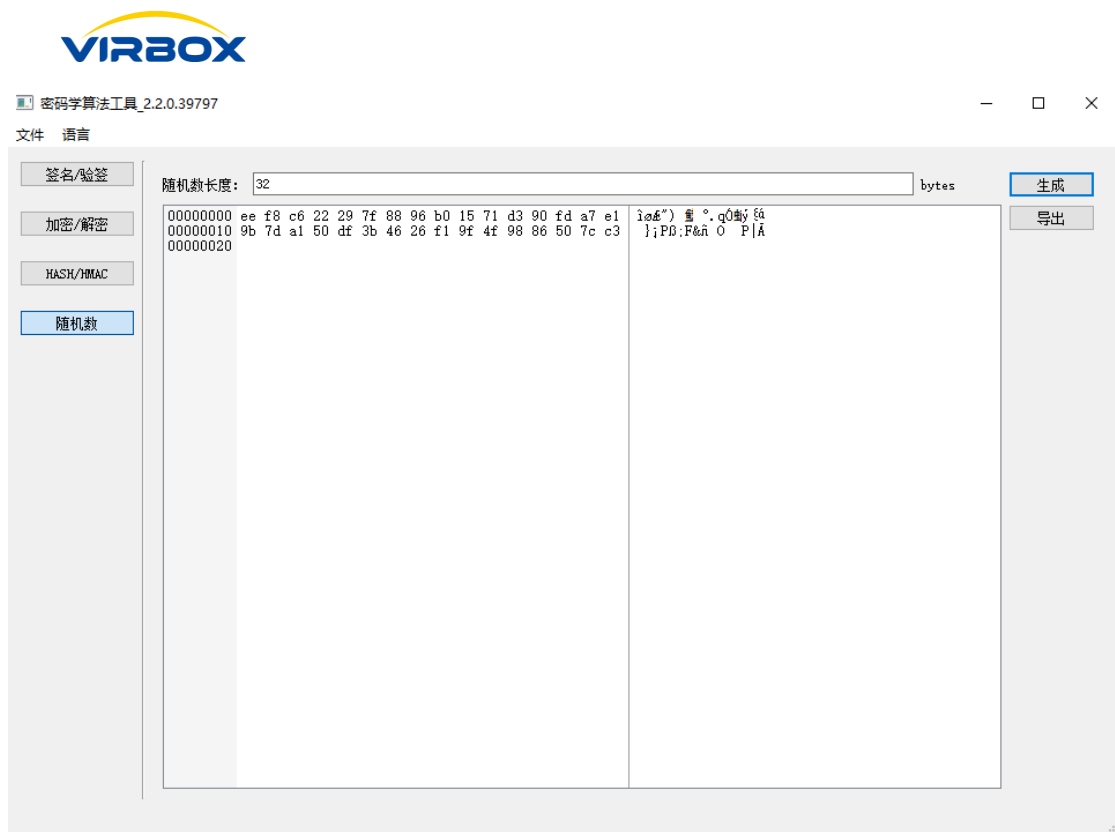


图 2-16

2.4 加壳工具

双击开发包 Tools 目录中的“virboxprotector.exe”启动加壳工具，工具界面如图 2-17。目前加密工具只支持 PE 及.NET 格式文件。

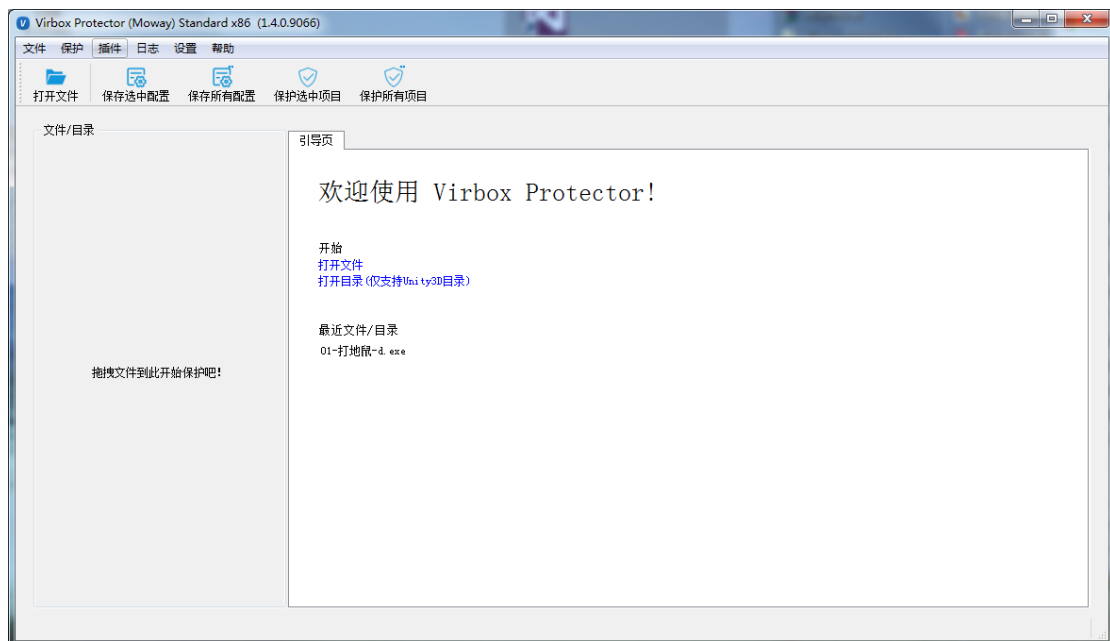


图 2-17

选择打开文件，打开需要保护的软件程序文件，如下图 2-18。

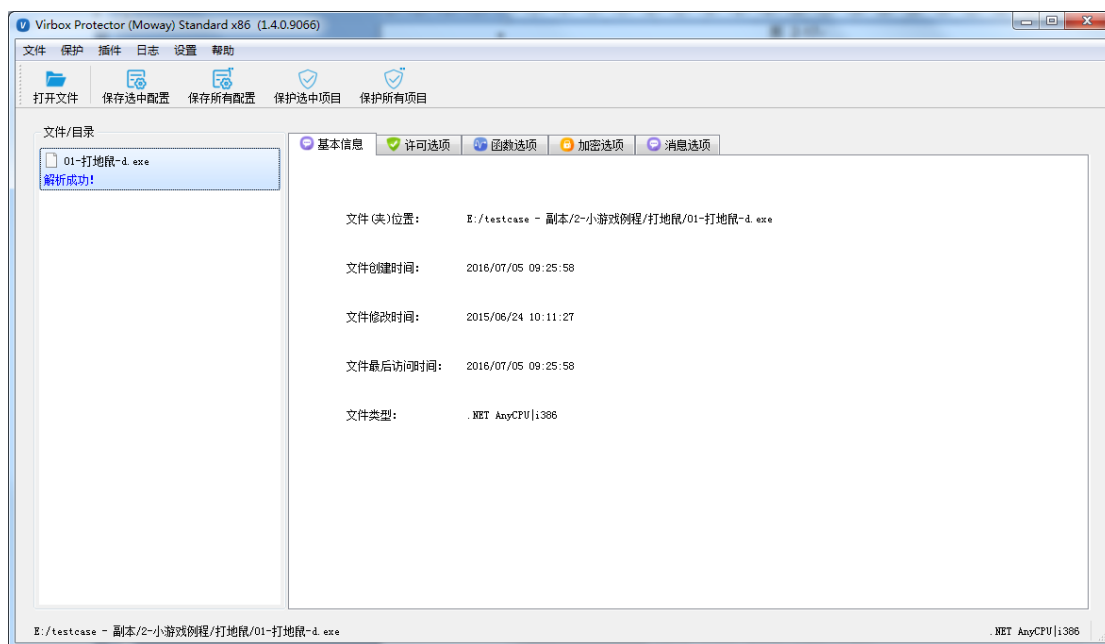


图 2-18

选择许可选项页签，输入加壳使用的 PID 设备，以及用户 PIN 码，如果指定某个加密锁，需要填写加密芯片的 SN 号，点击“保护选中项目”按钮，完成加壳，如下图 2-19。

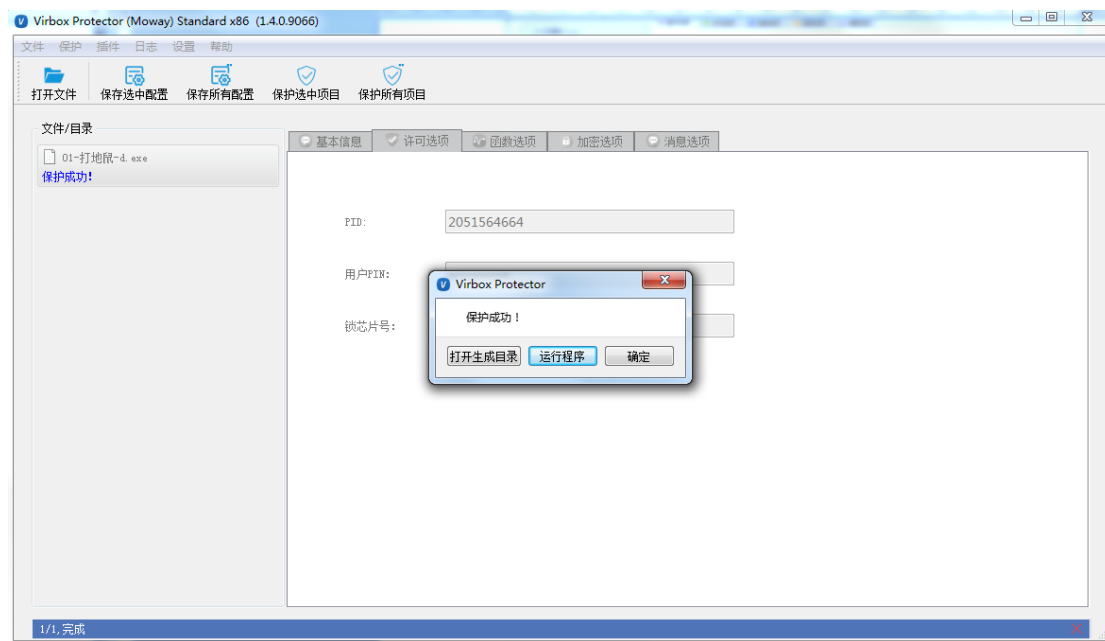


图 2-19

以上是加壳工具基本使用功能，加壳工具本身还支持更加高级的保护功能，如果需要使用，请与我公司联系沟通。

2.5 制作升级包工具

双击开发包 Tools 目录中的“MakePackageTool.exe”启动魔锐制作升级包工具，工

具界面如图 2-20;

在工具设备列表中显示当前主机存在的升级控制锁列表，选择需要制作 **PID** 类型升级包的控制锁，输入升级控制锁开发商 **PIN** 码，如果是制作给某个设备升级的升级包，需要勾选指定锁 **SN** 复选框，并输入指定升级设备的 **SN**。右边三个功能按钮可以编辑需要升级的设备内文件，完成设置后，点击开始制作，选择升级包需要保存的目录，完成升级包制作。

*注意：制作升级包需要使用升级控制锁，普通用户锁没有权限签发升级包；升级控制锁需要初始化过才能进行签发升级包，升级控制锁只能签发与它相同 **PID** 类型的用户锁升级包；*



图 2-20

2.6 用户升级工具

双击开发包 **Tools** 目录中的“**UpdateTool.exe**”启动魔锐用户升级工具，工具界面如图 2-21;

在加密锁列表中选择需要升级的加密锁，输入用户 **PIN**，然后选择升级包，点击升级，即可完成设备的升级工作。

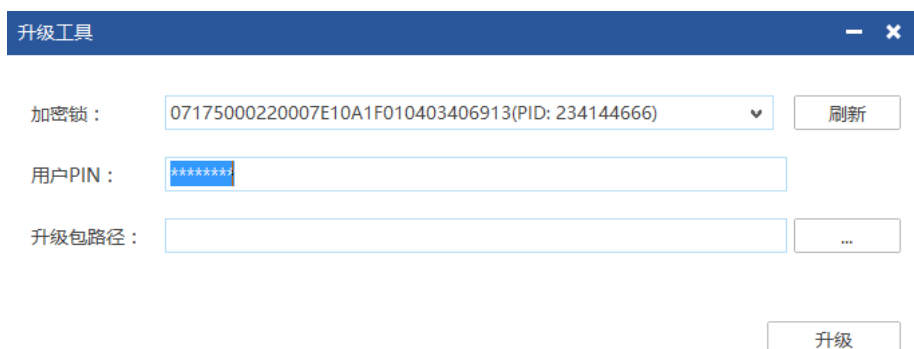


图 2-21

第3章 基本应用

在 1.3 章节我们简单的介绍了魔锐 1 的工作原理，本章将详细的介绍魔锐 1 提供的各种功能及应用方法。

3.1 数据保护

对于魔锐 1 来说，一般的使用方式就是将其作为数据存储设备，您可以将软件运行过程中需要使用的关键数据存放到魔锐 1 中，由于软件运行过程中需要使用这些数据，所以没有魔锐 1，软件就无法正常运行，这样就将软件和魔锐 1 紧密的结合到一起了。您也可以使用魔锐 1 文件权限机制，创建可读写的文件，将软件运行过程中的临时数据存储在这里，这样也可以增加软件与魔锐 1 结合的紧密程度。

3.2 密码算法保护

除了使用魔锐 1 的存储功能保护软件之外，还可以利用密码学算法使您的软件与魔锐 1 结合的更加紧密，我们建议您使用密码学算法来提高软件保护的强度。

魔锐 1 提供了多种先进的标准加密算法，标准加密算法的特点在于安全并不依赖于算法本身，而是依赖于所使用的密钥，所以只要不知道密钥，就没有办法去完全模仿整个计算过程。魔锐 1 将密钥以文件的形式保存在加密锁内部，加密锁内智能卡芯片保证了密钥存储的安全性，外部只能通过安全的 API 接口使用此密钥，所以，除非拥有加密锁，否则无法模拟出此密钥的进行密码学计算。

魔锐 1 目前支持的密码学算法有：对称算法 DES、TDES、AES128、AES256，非对称算法 RSA1024、RSA2048、ECC192、ECC256。通过密码学算法工具，可以生成指定算法的密钥文件，将密钥下载到加密锁内，通过 API 接口使用密钥文件，可以实现数据的加密解密与签名验签操作。根据密钥文件类型的区别，加密解密可以分为对称加解密与非对称加解密两种，目前非对称加解密只支持 RSA 算法。使用非对称密钥文件，还可以实现签名验签运算。

3.3 身份认证

魔锐 1 支持 HMAC-MD5、HMAC-SHA1、HMAC-SHA256 算法，能够实现“挑战-响应”方式的认证，可以取代传统的“用户名-密码”的方式，实现更加可靠的身份认证功能。其认证原

理是：预先在魔锐 1 设备中存放密钥 K_n ，密钥无法读出魔锐 1，只能使用，不需要考虑密钥保存的安全性问题，认证时服务器端发送随机数（挑战）给客户端的魔锐 1 设备，并验证设备返回的计算结果（响应）是否是由此密钥 K_n 计算出来的，计算结果正确就认为客户端拥有密钥 K_n ，由于密钥 K_n 在客户端的魔锐 1 中，无法被仿制，此时就可认为客户端是密钥 K_n 对应的客户。其实现原理如图 3-1 所示。

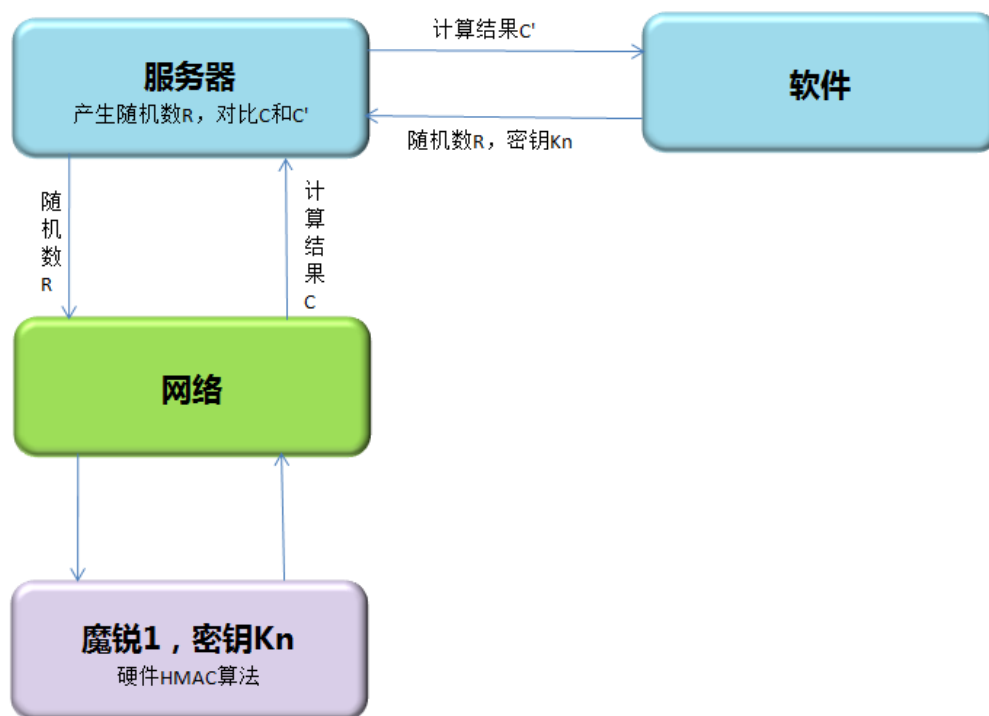


图 3-1

3.4 加壳保护

您可以使用我们提供的加壳工具，无需编程就能达到高安全强度的保护。您只需要运行加壳工具，输入您的 PID，即可对已经编译好的软件进行加壳保护，加壳工具会使用一些高级的算法与逻辑，紧密的将魔锐与软件结合在一起。加壳保护后，只有插入您发布设置的对应 PID 的锁，软件才能运行，从而达到保护目的。

3.5 综合保护

以上小节中都是使用魔锐的某个单独的模块功能实现的保护，安全强度并不是很高。在实际的加密方案设计过程中，可以结合多个保护模块，实现高强度的加密保护。

例如：在数据保护过程中，直接将数据保存在加密锁内，数据是以明文存储的，很容易被非法人员获取，并分析数据结构，造成安全信息泄露。在综合保护中，可以先通过加密锁内部的一个密钥文件对数据进行加密，再将加密数据保存到设备内部，在使用的过程中，通

过加密锁内的密钥解密数据，得到真实使用的数据，这样，即使获取到数据，没有加密锁内的密钥解密，也无法获得有效的数据信息，这样的数据的安全性就比较有保证。如果你还担心软件端的数据安全，可以使用加壳工具对软件进行加壳保护，这样，就可以实现一个完整的高强度加密保护方案：

3.6 API 使用

您可以使用我们提供的魔锐开发设置工具对加密锁进行设置，也可以使用 API 函数完成加密锁的初始化。本章节主要介绍在软件中使用我们提供的 API 函数访问魔锐 I 的流程。

软件访问魔锐 1 分为管理权限访问和普通用户权限访问。管理权限访问是软件开发商拥有的权限，是加密方案开发阶段使用的权限，该权限下访问魔锐 1，需要先校验开发商 PIN 码，校验通过后，拥有魔锐 1 的最高权限，对加密锁的任何操作都没有限制。普通用户权限是最终用户所拥有的权限，是使用权限，该权限下访问魔锐 1，需要先校验普通用户密码，校验通过后，允许的操作包括：对有操作权限的文件进行操作、对数据进行加解密以及升级升级包操作。

管理权限访问魔锐 I 的流程如图 3-2 所示。



图 3-2

普通用户权限访问魔锐 1 的流程如图 3-3 所示。



图 3-3

第4章 API 函数概要

魔锐 1 的 API 接口按功能可以分为 5 大类：基本操作类、初始化类、文件操作类、密码算法类、远程升级类。本文档简要概述各个功能 API 的基本用途，详细的 API 接口说明，请参考 API 接口说明文档《mowayAPI.chm》。

4.1 基本操作类

设备操作的基本函数，主要用于打开关闭加密锁，以及获取锁信息相关等。

❖mw_enum

枚举当前主机所有的魔锐 1 设备；

❖mw_open

打开指定魔锐 1 设备；

❖mw_close

关闭魔锐 1 设备；

❖mw_verify_pin

校验魔锐 1 的 PIN 码，获取 PIN 码对应的设备操作权限；

❖mw_control



复位设备状态、控制 LED 亮灭；

❖mw_get_device_info

获取魔锐 1 设备的基本信息相关；

❖mw_get_device_status

获取魔锐 1 设备的当前工作状态；

❖mw_error_help

当调用 API 返回错误时，使用此接口获得错误情况的解析；

4.2 初始化类

出厂的魔锐 1 设备一切信息都是默认的，需要进行初始化后才能使用，主要是修改默认 PIN 码与设置设备 PID。

❖mw_change_Pin

修改设备的 PIN 码；

❖mw_set_pid

设置设备的 PID；

4.3 文件操作类

通过文件操作类接口可以操作魔锐 1 内部存储的文件。

❖mw_enum_file

枚举当前魔锐 1 内部所有的文件名称；

❖mw_create_file

在魔锐 1 内部创建一个文件；

❖mw_read_file

读取魔锐 1 内部指定文件的数据；

❖mw_write_file

写数据到魔锐 1 内部指定文件内；

❖mw_delete_file

删除魔锐 1 内部指定文件；

❖mw_get_file_property

获取魔锐 1 内部指定文件的文件属性；

4.4 密码算法类

- ❖ 通过密码算法类 API，使用魔锐 1 内部密钥文件，完成密码学运算。

`mw_sym_encrypt`

使用存储在魔锐 1 内部的对称密钥进行加密运算；

- ❖ `mw_sym_decrypt`

使用存储在魔锐 1 内部的对称密钥进行解密运算；

- ❖ `mw_rsa_encrypt`

使用存储在魔锐 1 内部的 RSA 密钥进行加密运算；

- ❖ `mw_rsa_decrypt`

使用存储在魔锐 1 内部的 RSA 密钥进行解密运算；

- ❖ `mw_signature`

使用存储在魔锐 1 内部的非对称密钥进行签名运算；

- ❖ `mw_verify_sign`

使用存储在魔锐 1 内部的非对称密钥进行签名验证运算；

- ❖ `mw_hmac_calc`

使用存储在魔锐 1 内部的 HMAC 密钥进行 HMAC 计算；

4.5 远程升级类

- ❖ 通过远程升级类 API 可以制作远程升级包，远程升级魔锐 1 内部文件。

`mw_make_update_pkg`

通过远程升级控制锁制作远程升级包；

- ❖ `mw_update`

用户使用远程升级包对加密锁进行升级；

第5章 附录 I

A. 支持的开发语言

C、C#、Java、Delphi 等。

B. 支持的操作系统

Windows 2000 以上(32 位, 64 位)

Linux(32 位, 64 位)

MAC(32 位, 64 位)。

C. 硬件技术规格

| 项目 | 值 | 备注 |
|--------|-------------|-----------------|
| 工作电压 | DC 4.5~5.5V | 无 |
| 最大功耗 | 150mW | 无 |
| 工作温度 | -10~70℃ | 无 |
| 数据存储时间 | 10 年 | 典型值 |
| 擦除/写周期 | 10 万次 | 最低值 |
| 设备接口 | USB 2.0 全速 | 全速设备, 符合 HID 规范 |