飞天诚信

ROCKEY-ARM 用户工具手册

V1.0

飞天诚信科技股份有限公司

网址：www.FTsafe.com

修订记录：

修订日期	版本	修订内容
2013 年 7 月	V1.0	第一版发布

软件开发协议

飞天诚信科技股份有限公司（以下简称飞天）的所有产品，包括但不限于：开发工具包，磁盘，光盘，硬件设备和文档，以及未来的所有定单都受本协议的制约。如果您不愿接受这些条款，请在收到后的 7 天内将开发工具包寄回飞天，预付邮资和保险。我们会把货款退还给您，但要扣除运费和适当的手续费。

1. 许可使用

您可以将本软件合并、连接到您的计算机程序中，但其目的只是如开发指南中描述的那样保护该程序。您可以以存档为目的复制合理数量的拷贝。

2. 禁止使用

除在条款 1 中特别允许的之外，不得复制、反向工程、反汇编、反编译、修改、增加、改进软件、硬件和产品的其它部分。禁止对软件和产品的任何部分进行反向工程，或企图推导软件的源代码。禁止使用产品中的磁性或光学介质来传递、存储非本产品的原始程序或由飞天提供的产品升级的任何数据。禁止将软件放在服务器上传播。

3. 有限担保

飞天保证在自产品交给您之日起的 12 个月内，在正常的使用情况下，硬件和软件存储介质没有重大的工艺和材料上的缺陷。

4. 修理限度

当根据本协议提出索赔时，飞天唯一的责任就是根据飞天的选择，免费进行替换或维修。飞天对更换后的任何产品部件都享有所有权。

保修索赔单必须在担保期内写好，在发生故障 14 天内连同令人信服的证据交给飞天。当将产品返还给飞天或飞天的授权代理商时，须预付运费和保险。

除了在本协议中保证的担保之外，飞天不再提供特别的或隐含的担保，也不再对本协议中所描述的产品负责，包括它们的质量，性能和对某一特定目的的适应性。

5. 责任限度

不管因为什么原因，不管是因合同中的规定还是由于刑事的原因，包括疏忽的原因，而使您及任何一方受到了损失，由我方产品所造成的损失或该产品是起诉的原因或与起诉有间接关系，飞天对您及任何一方所承担的全部责任不超出您购买该产品所支付的货款。在任何情况下，飞天对于由于您不履行责任所导致的损失，或对于数据、利润、储蓄或其它的后续的和偶然的损失，即使飞天被建议有这种损失的可能性，或您根据第 3 方的索赔而提出的任何索赔均不负责任。

6. 协议终止

当您不能遵守本协议所规定的条款时，将终止您的许可和本协议。但条款 2，3，4，5 将继续有效。

Software Developer's Agreement

All Products of Feitian Technologies Co., Ltd. (Feitian) including, but not limited to, evaluation copies, diskettes, CD-ROMs, hardware and documentation, and all future orders, are subject to the terms of this Agreement. If you do not agree with the terms herein, please return the evaluation package to us, postage and insurance prepaid, within seven days of their receipt, and we will reimburse you the cost of the Product, less freight and reasonable handling charges.

1. Allowable Use – You may merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. You may make archival copies of the Software.

2. Prohibited Use – The Software or hardware or any other part of the Product may not be copied, reengineered, disassembled, decompiled, revised, enhanced or otherwise modified, except as specifically allowed in item 1. You may not reverse engineer the Software or any part of the product or attempt to discover the Software's source code. You may not use the magnetic or optical media included with the Product for the purposes of transferring or storing data that was not either an original part of the Product, or a Feitian provided enhancement or upgrade to the Product.

3. Warranty – Feitian warrants that the hardware and Software storage media are substantially free from significant defects of workmanship or materials for a time period of twelve (12) months from the date of delivery of the Product to you.

4. Breach of Warranty – In the event of breach of this warranty, Feitian's sole obligation is to replace or repair, at the discretion of Feitian, any Product free of charge. Any replaced Product becomes the property of Feitian.

Warranty claims must be made in writing to Feitian during the warranty period and within fourteen (14) days after the observation of the defect. All warranty claims must be accompanied by evidence of the defect that is deemed satisfactory by Feitian. Any Products that you return to Feitian, or a Feitian authorized distributor, must be sent with freight and insurance prepaid.

EXCEPT AS STATED ABOVE, THERE IS NO OTHER WARRANTY OR REPRESENTATION OF THE PRODUCT, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5. Limitation of Feitian's Liability – Feitian's entire liability to you or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price you paid for the unit of the Product that caused the damages or are the subject of, or indirectly related to the cause of action. In no event shall Feitian be liable for any damages caused by your failure to meet your obligations, nor for any loss of data, profit or savings, or any other consequential and incidental damages, even if Feitian has been

advised of the possibility of damages, or for any claim by you based on any third-party claim.

6. Termination – This Agreement shall terminate if you fail to comply with the terms herein. Items 2, 3, 4 and 5 shall survive any termination of this Agreement.

目 录

第1章 ROCKEY-ARM 集成编辑工具

ROCKEY-ARM 集成编辑工具是一款功能强大的管理工具，它支持了 ROCKEY-ARM 系列产品几乎所有的功能。用户可以使用此工具，对 ROCKEY-ARM 加密锁进行了解熟悉，也可以对相关数据进行查看设置，还可以进行生产、升级、加解密等操作。

本章节除了介绍 ROCKEY-ARM 集成编辑工具的功能外，也将更具体的介绍 ROCKEY-ARM 系列加密锁所具备的功能，使用户对 ROCKEY-ARM 系列产品有一个更加全面的了解。

1.1 介绍

ROCKEY-ARM 集成编辑工具的主要用途是配置锁内数据并进行批量生产。具备以下功能模块有：基本功能、文件管理、加密解密、密码管理、远程升级、制作母锁、时钟管理和批量初始化。如下图所示：

图 1 登录界面

从登录界面可以看到加密锁的基本信息，ROCKEY-ARM 集成编辑工具最多可以枚举出 32 个 HID ROCKEY-ARM 加密锁和 32 个 CCID ROCKEY-ARM 加密锁，在设备的下拉列表中选中一个设备，则在加密锁信息中就可以查看到相关设备的信息。

ROCKEY-ARM 系列加密锁的登录模式分为三种，分别是开发商模式，用户模式和匿名模式。不同的登录模式拥有不同的权限，开发商模式拥有开发商权限，用户模式拥有用户权限，匿名模式拥有匿名权限。匿名模式登录无需验证密码，因此匿名模式具有最小的权限，无法对锁内的重要信息进行操作。用户模式登录时，需要验证用户 PIN 码，用户 PIN 码由开发商设定，默认值为 12345678，用户权限的级别要高于匿名权限，能对部分重要信息进行操作。使用开发商模式登录系统，需要验证开发商密码，开发商权限是最高的权限级别，可以进行所有的操作。

ROCKEY-ARM 系列加密锁的状态共分为三种，分别为空锁、子锁和母锁。空锁是出厂状态，锁内没有数据，一切信息值都为默认值。开发商在得到锁后，需要对加密锁进行唯一化锁操作（详见 1.5.1 唯一化锁），通过唯一化锁将空锁变为子锁，此操作类似于对锁进行初始化操作。若有需要，可以通过制作母锁操作（详见 1.7 制作母锁）功能，将子锁变为母锁，变为母锁后，便可以使用母锁生产子锁。

1.2 基本功能

点击左侧菜单导航上的“基本功能”，即可进入基本功能的操作界面，如图所示：

图 2 基本功能

1.2.1 数据存储区

在基本功能的界面上显示的数据存储区就是 ROCKEY-ARM 系列加密锁所提供的 8K 数据存储区，其中的前 4K 数据存储区域，即 0~4095 位置，任意权限可以进行读写操作，后 4K 数据存储区域，即 4096~8191 位

置，所有权限都可以进行读取，但只有使用开发商权限才可以进行写入操作。

导出、导入的操作任何权限都可以执行。在导入时，数据仅仅是导入到了工具内，并没有写入锁中，只有再点击“写入”按钮是，才执行了写入操作。

1.2.2 共享内存区

ROCKEY-ARM 系列加密锁的 32 字节共享内存区可供锁内程序和锁外 API 方式共同访问，数据掉电就会擦除。集成编辑工具提供了对共享内存区的读写功能，任意权限都可对此共享内存区进行读写操作。

1.2.3 产生随机数

ROCKEY-ARM 系列加密锁为用户提供了产生随机数的功能，用户可以将所产生的随机数运用到所保护的程序之中。有了随机数的参与，可以使得被保护的程序更具有不确定性，可以增强其安全强度。用户也可以使用所产生的随机数作为种子码，进行唯一化锁的操作（详见 1.5.1 唯一化锁）。

集成编辑工具为用户提供了随机数的产生和导出功能，匿名及以上权限即可操作。用户可以用集成编辑工具来测试加密设备产生随机数的功能，不过 ROCKEY-ARM 系列加密锁只可以产生 1~128 字节长度的随机数，用户可根据需求进行操作。

1.2.4 LED 控制

集成编辑工具的 LED 控制功能是设置 ROCKEY-ARM 加密锁 LED 灯的亮、灭和闪三种状态。

1.2.5 锁内信息

在基本功能页面上显示的锁内信息一共为两项，分别是硬件 ID 和用户 ID。硬件 ID 即 HID，是加密锁的唯一标识，具有全球唯一性，并且是在加密锁出厂时被烧制在加密锁锁中，不可被修改。用户 ID 即 UID，方便加密锁开发商标识自己的最终用户，另外，需要说明的是，只有开发商权限才可以对用户 ID 进行设置。

1.2.6 允许的种子码运算次数

种子码运算是 ROCKEY-ARM 加密锁提供的一个非公开的专有算法，加密锁在非空锁时才可以调用其中的种子码算法。并且，可使用集成编辑工具，在开发商权限下对种子码可以运算次数进行设定。

-1 表示对种子码运算的调用次数不进行限制。如果需要对种子码运算次数进行限制，可设置运算次数的范围为 1~2147483647，设定之后，每调用一次种子码运算时，此值都会递减，递减到 0 时，此种子码算法将无法再被调用。

1.2.7 切换通讯协议

ROCKEY-ARM 系列加密锁为用户提供了两种通讯协议，分别为 HID 和 CCID。HID 通讯方式跟 CCID 通讯

方式相比，操作系统的兼容性更好些（在 XP 以上 windows 操作系统中是无需安装驱动的）。而 CCID 通讯方式跟 HID 通讯方式相比，CCID 通讯的速度要更快些，选用哪一种方式进行通讯，开发商可以根据自己的情况进行取舍。

在基本功能的页面上，集成编辑工具为用户提供了切换通讯协议的功能。当前设备的通讯协议类型可以在登录页面的设备类型中查看到。

1.3 文件管理

点击左侧菜单导航上的“文件管理”，即可进入文件管理的操作界面，如图所示：

图 3 文件管理

ROCKEY-ARM 系列加密锁一共提供了 5 种文件类型，分别是：数据文件、RSA 私钥文件，ECC 和 SM2 私钥文件(ECC 和 SM2 私钥文件存储结构相同，属同一类型)、3DES/SM4 密钥文件以及可执行文件。在文件类型的下拉列表框中选中某种文件类型，则在其下方的列表框中便会显示出相应文件类型所创建了的文件。在开发商权限下，才可创建文件。以下对文件管理中的操作进行几点说明：

1）所有文件类型的文件 ID 不能使用 0000, 3 F00 和 FFFF。

2）ROCKEY-ARM 系列加密锁一共提供了 128K 文件存储空间，其中 64K 为可执行文件的存储空间。

3）数据文件创建个数受锁内空间大小和文件系统其他因素的影响，最大个数不超过 54 个。例如，文件大小设为 252 字节，最多可创建 54 个文件；如果文件大小设为 1024 字节，最多可创建 31 个文件，如果文件大小设为 4096 字节，最多可创建 9 个文件。由于实际应用中文件大小的情况比较复杂，可自行测试确定文件个数。

4）RSA 私钥文件允许创建的最大数量为 8 个。

5）ECC 和 SM2 私钥文件允许创建的最大数量为 16 个。

6）3DES 和 SM4 密钥文件允许创建的最大数量为 32 个。

7）可执行文件允许创建的最大数量为 64 个，但总大小不能超过 64K。

8）可执行文件为.bin 格式的文件，可以使用 Keil uVision4 进行编写，提供了的工程向导工具（详见第 5 章 ROCKEY-ARM 工程向导工具）来方便用户创建工程。可执行文件仅支持一次性下载，即每次下载可执行文件时，都会将锁内已存在的可执行文件进行擦除后再写入。

9）无论是 RSA 私钥文件还是 ECC 和 SM2 私钥文件，对用户来说私钥文件都是非常重要的，因此在产生公私钥文件时，用户务必将备份到本地的公私钥文件进行妥善保存。

10）在创建 RSA 私钥文件以及 ECC 和 SM2 私钥时，集成编辑工具提供了是否限制调用次数的功能，如图所示：

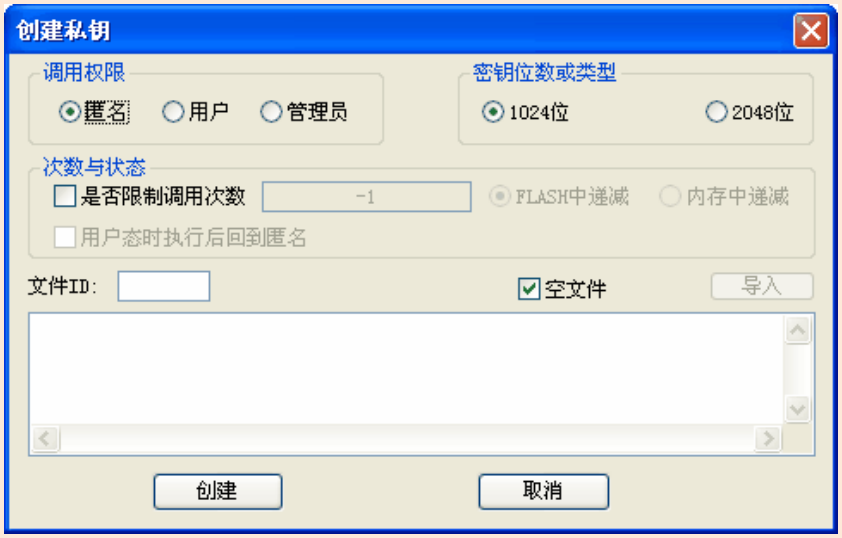

图 4 创建私钥

当设定了限制调用次数时，其递减方式提供了两种，分别为 FLASH 中递减和内存中递减，所谓 FLASH 中递减表示在锁内 FLASH 中递减，每调用一次调用次数值就会真正的递减 1；所谓内存中递减，是指在调用的过程中在锁的内存中递减，而不是真正的递减，当重新插拔锁后，限制调用次数还会恢复到设置值。

1.3.1 可执行文件的下载

ROCKEY-ARM 的可执行文件是可以在锁内本地运行的程序文件，由于 ROCKEY-ARM 系列加密锁使用的是高性能 ARM 智能卡芯片，这种智能卡芯片耗电少功能强，采用 16 位/32 位双指令集，其程序的运算速度要比传统的 C51 虚拟机中运行的程序快 60—70 倍。由于可执行程序对软件的保护相对来说比较重要，所以在此对可执行文件的操作进行比较详细的介绍。

可执行文件与其他类型的文件不同，它是使用 Keil 4 编写的二进制文件，编译后.bin 格式文件可在锁内运行，可以通过集成编辑工具下载（写入）到加密锁内。需要强调的是，出于安全性的考虑，这款加密锁的可执行文件只能批量下载，每次下载之前都将清空锁内原有的所有可执行文件。

在文件类型下拉列表框中选中可执行文件，点击下载，弹出下载可执行文件对话框，如图所示：

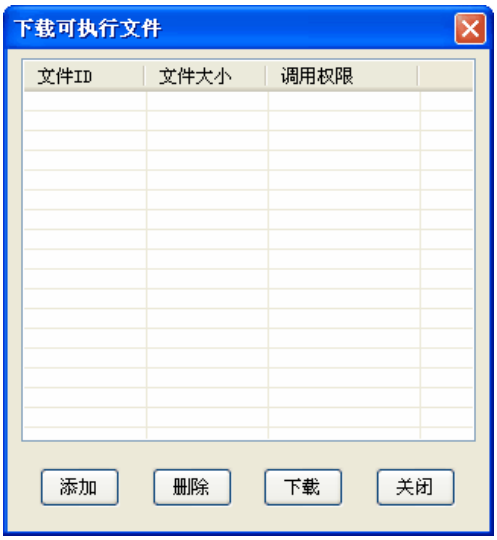

图 5 下载可执行文件

点击添加按钮，就可以加载可执行程序，如图所示：

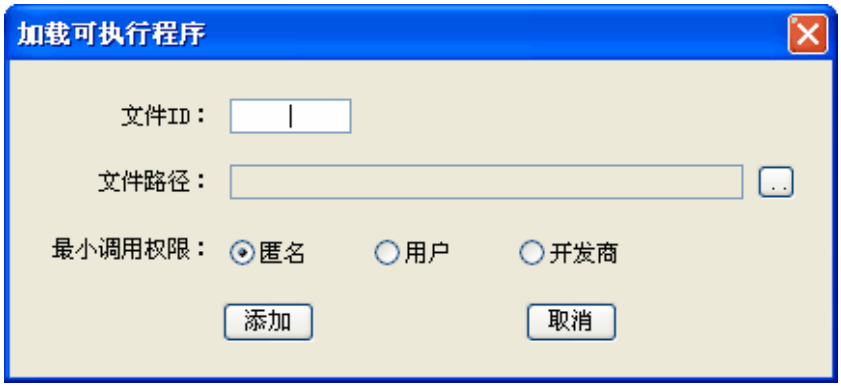

图 6 加载可执行文件

输入正确的文件 ID（除 0000, 3 F00 和 FFFF 以外），浏览并选择所要加载的可执行文件，按照需要选择最小的调用权限，然后点击添加按钮，则在图 5 的列表中就会有所显示。

当将所有的可执行文件都添加完成后，点击图 5 中的下载按钮，此次加载的全部可执行文件就会被下

载（写入）到加密锁内。由于新下载（写入）的可执行文件会将以前的可执行文件全部覆盖，因此在进行下载（写入）操作时，请谨慎对待。

1.3.2 可执行文件的运行

对于下载到 ROCKEY-ARM 锁内的可执行文件，集成编辑管理工具提供运行可执行文件的功能。在文件管理界面上的文件类型下拉列表中选中可执行文件，然后选中一个可执行文件，点击运行程序，则弹出运行锁内可执行文件的对话框，如图所示：

图 7 运行可执行文件

在输入数据文本框中导入或者输入相关数据，点击运行，运行成功与否，界面的下方会有文字提示。

对图中所示内容做一下说明：

1、输入输出缓冲区的大小不能超过 1024 字节，因为锁内程序的缓冲区 InOutBuf 最大为 1024 字节。

2、上图所示的“锁内 mian 函数的返回值”为锁内可执行程序的主函数 main 的返回值。

3、锁内的输入输数据共用同一个数据缓冲区，所以，缓冲区的大小要同时考虑输入和输出数据来指定。

1.4 加密解密

点击左侧菜单导航上的“加密解密”，即可进入加密解密的操作界面，如图所示：

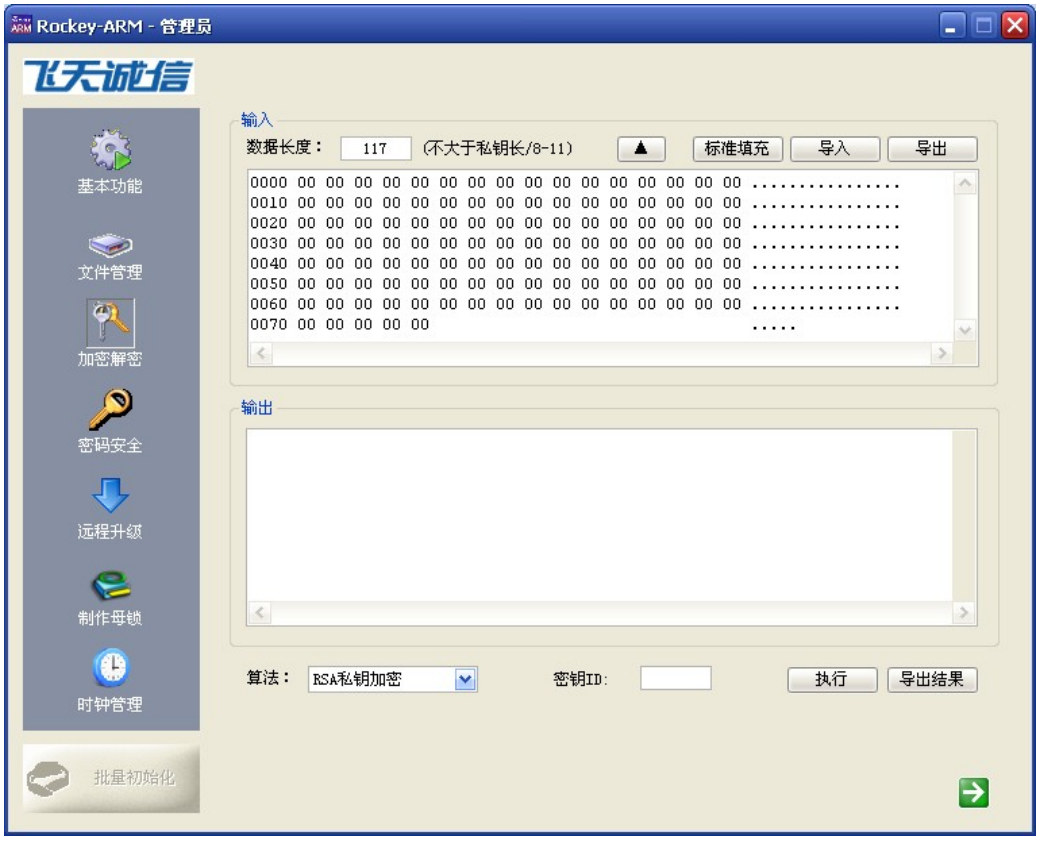

图 8 加密解密

集成编辑工具的加密解密是提供给用户测试各种运算功能的，在这个功能模块中，基本上涵盖了 ROCKEY-ARM 所提供的所有算法。算法包括：RSA 私钥加密、RSA 公钥解密、RSA 公钥加密、RSA 私钥解密、ECC 私钥签名、ECC 公钥验签、SM2 私钥签名、SM2 公钥验签、SM4 加密、SM4 解密、3DES（ECB）加密、3DES（ECB）解密、HASH 运算、种子码算法。

其中有以下几点需要进行说明：

1）HASH 算法支持的类型有：MD5、SHA1 和国密 SM3。

2）种子码算法只有当加密锁的状态为非空锁时才可以调用。

1.5 密码管理

点击左侧菜单导航上的“密码管理”，即可进入密码管理的操作界面，如图所示：

图 9 密码管理

1.5.1 唯一化锁

唯一化锁就是对加密设备进行初始化操作，首次进行了唯一化锁后，加密设备的状态将从空锁状态变为子锁状态，特征是，产品 ID 将不再是 FFFFFFFF。产品 ID 和开发商 PIN 码都是通过种子码算法产生的，因此用来产生开发商 PIN 码的种子码很重要，种子码需要安全的保存，其中，种子码算法产生的 PID 不可更改。

1.5.2 更改密码

使用更改密码功能，可以更改开发商 PIN 码，也就是使用种子码在唯一化锁时产生的密码，也可以更改用户 PIN 码。在加密锁没有进行过唯一化锁操作前，也就是加密锁是空锁状态时，是无法对加密锁进行更改密码操作的。

在更改密码时，可以设置其密码的允许重试次数。当重试次数设置为 255 时，表示不限制重试次数，设为其他值，则每输错一次，允许重试次数将会递减 1，当次数递减到 0 时，加密锁将被锁死，此时将无法再进行相应权限的操作。

当用户 PIN 码允许重试次数递减到 0 时，可以有两种方式进行解锁，一种是开发商制作远程解锁升级包（详见 1.6 远程升级），另一种是使用开发商权限重置用户 PIN 码，重置后的用户 PIN 码将恢复出厂状态时的值。 但是，当开发商 PIN 码的重试次数递减到 0 时，加密锁将无法被解锁，如果想重新获得开发商权限，只能将加密锁返厂重烧 COS。

注意：用户工具中“*”视为特殊字符，请勿将 PIN 码修改为带有 “*”的字符串。

1.5.3 重置用户 PIN 码

重置用户 PIN 码的功能，可以在开发商权限下将用户 PIN 码恢复到出厂时的值，即“12345678”。可以将这种功能应用在解锁用户 PIN 码上。

1.5.4 恢复到出厂状态

点击“一键恢复”按钮，就能将加密锁恢复到出厂状态，加密锁的状态也将恢复到空锁状态，锁内的数据将被全部清空，所有信息将全部恢复到出厂时的默认值。

1.6 远程升级

点击左侧菜单导航上的“远程升级”，即可进入远程升级的操作界面，如图所示：

图 10 远程升级

远程升级是指，开发商将加密锁出售给最终用户后，若想对锁内的某些数据进行更改，无需将加密锁从最终用户那里收回，而是制作好远程升级包，通过网络直接发给用户，最终用户通过升级工具，将远程升级包中的操作在用户加密锁中执行，从而到达了对锁内数据文件进行更改的目的。

ROCKEY-ARM 系列加密锁的远程升级就是通过制作远程升级包，使用远程升级工具（详见 第 3 章 客户端远程升级工具）进行升级的。集成编辑工具中的远程升级模块，就可以用来制作远程升级包。

ROCKEY-ARM 系列加密锁的远程升级包是由 RSA 密钥进行加密的，因此就算是将其直接在网络上传输，也可以保证远程升级包的安全。

1.6.1 配置升级文件

升级文件就是远程升级包，配置升级文件就是将升级的功能项进行设置，设定升级包中都包含哪些功能。集成编辑工具所提供的远程升级功能，涵盖了 ROCKEY-ARM 系列加密锁所支持的全部远程升级功能。功能包括了：创建文件、写文件、删除文件、文件权限、种子码调用次数、可执行文件、解锁用户 PIN、使用截止日期。

关于配置升级文件，需要进行以下几点说明：

1) 并不是所有文件类型的文件都支持远程升级的方法进行创建和写入，可执行文件就不能支持远程升级中的创建文件和写文件。因此，创建文件和写文件对应的文件类型仅为，数据文件、RSA 私钥文件、ECCSM2 私钥文件和密钥文件。

2) 可执行文件选项实际意义为下载可执行文件，通过制作升级可执行文件的升级包，可以将升级包中存在的可执行文件下载到被升级的加密锁中，但是，需要注意的是，新下载到锁内的可执行文件会全部替换原有的可执行文件，原来的文件将全部不存在。

3) 使用期限的升级包只针对时钟锁使用。

4) 升级包可以配置多个功能项，并没有冲突，但是每个升级包针对一把加密锁仅能使用一次。

5) 出于安全考虑，解锁用户 PIN 码功能，必须要绑定硬件 ID。

对于升级包的配置信息，ROCKEY-ARM 集成编辑工具提供了保存和加载的功能，当将远程升级包的功能项配置好后，点击保存配置按钮，则配置信息将以文件形式保存，若日后再想创建相同功能的升级包，则可以直接点击加载配置按钮，将配置文件导入集成编辑工具，使用非常的方便。

1.6.2 制作升级包

子锁制作升级包需要导入 RSA 公钥对升级包加密，母锁制作升级包时不需要导入 RSA 升级公钥，这是因为母锁中包含有与子锁对应的 RSA 密钥信息，可用母锁直接进行加密。另外，当为升级包绑定了加密锁的硬件 ID 后，那么只有具有此硬件 ID 的加密锁才可以升级成功。

1.6.3 写入远程升级私钥

远程升级私钥用在远程升级过程中解密升级包数据。它需要与制作升级包时的 RSA 公钥匹配，只有这样才可以解密升级包，进行升级。

1.6.4 升级

工具提供的升级功能可以用来执行升级操作，导入升级包后，如果解密升级包和执行操作都正确，则升级就会成功。例如，升级包的功能是创建了数据文件 0001，那么经过升级测试功能成功升级后，查看数据文件，就可以发现已经成功创建了 0001 的数据文件。

在实际应用远程升级功能时，最终用户并不需要使用集成编辑工具的升级测试功能来升级加密锁，可以使用我们提供的升级工具（详见 第 3 章客户端远程升级工具）。使用升级工具会更加简单，也更加安全。

1.7 制作母锁

点击左侧菜单导航上的“制作母锁”，即可进入制作母锁的操作界面，如图所示：

图 11 制作母锁

母锁内存储有生产子锁的基本信息，用来生产子锁。在制作母锁时，需要设置相应子锁数据。母锁的主要应用就是安全的批量生产子锁和远程升级子锁。使用母锁批量生产子锁可以使用 RyARMInitSon 工具（详见 第 2 章 ROCKEY-ARM 子锁初始化工具）。子母锁模式远程升级在 1.7.2 子锁中的远程升级私钥中进行了说明。

只有加密锁为子锁状态（唯一化锁之后）才可以制作成母锁，空锁是不能制作成母锁的。

1.7.1 种子码

在制作母锁时设置的种子码，是将来母锁生产出来的子锁对应的种子码，也就是说，使用此母锁生产出来的子锁的产品 ID 和开发商 PIN 码，是用此导入的种子码通过种子码产生的。这里的种子码只能导入，不能随意写入。

1.7.2 子锁中的远程升级私钥

此处的远程升级私钥，会在子母锁生产中从母锁中取出并写入子锁中。另外，需要说明的是，在制作母锁中所导入的“子锁内的远程升级私钥”，与母锁自身的远程升级私钥不能相同。也就是说，母锁制作的远程升级包不能用来升级自己，这种设计是出于生产过程中的安全考虑。

1.7.3 子锁中的密码设置

由于母锁所生产的子锁的开发商 PIN 码是由导入的种子码所决定的，在此处对子锁中的密码设定，仅可以设定用户 PIN 码、用户 PIN 码的最大重试次数和开发商 PIN 码的最大重试次数。这些设置都会在以后产生的子锁中生效，母锁本身不会有所变化。

1.7.4 批量设置

ROCKEY-ARM 加密锁可以使用子母锁模式进行批量生产，这也是母锁的重要应用之一。在批量初始化的过程中可以设置允许初始化空锁的数量，超过设定的数量，母锁将不能再用于批量生产。若设定数量的值为-1，则表示对母锁生产子锁的数量不限制，若要对初始化空锁的数量进行限制，则数量值的范围为 1~2147483647。

起始用户 ID 表示在使用此母锁生产子锁时，生产出来的第一把子锁的用户 ID 编号。该 ID 值会随着初始化子锁数量的递增而递增。

1.8 时钟管理

点击左侧菜单导航上的“时钟管理”，即可进入时钟管理的操作页面，如图所示：

图 12 时间管理

时间管理模块的功能只针对 ROCKEY-ARM 的时钟锁有效，当使用的是非时钟锁时，在此功能界面会有相应提示，如图所示：

图 13 时间管理

ROCKEYTime-ARM 时钟锁采用的是硬时钟，锁内包含时钟芯片。锁内时间在出厂时设定后，永远无法再更改，所以，用户无需担心时间被破解者篡改的问题。

1.8.1 设置到期时间

ROCKEYTime-ARM 时钟锁到期后将限制用户权限的访问，如果需要在到期后限制使用锁内资源，需要将该资源设置为用户权限，例如文件的读写权限，私钥的调用权限。时钟锁可以采用两种方式对使用时间进行限制，分别是设置到期日期和到期小时数。

设置到期日期就是设置具体的到期截止日期。例如，选定了到期的日期值，然后在其日期选择器中选择 2014 年 11 月 27 日，然后点击设置按钮，提示操作成功，这就意味着，到 2014 年 11 月 27 日后，加密设备不能再使用需要用户权限的资源，即所有需要用户权限的操作都无法再进行。

设置到期小时数就是用户可以访问加密锁的小时时长。例如，选定了到期的小时数，然后在其输入框中输入 24，然后点击设置按钮，提示操作成功，这就表示，从最终用户以用户权限访问锁，即第一次校验用户 PIN 码后开始算起，24 小时后，加密锁将不能再以用户权限进行访问了，所有需要用户权限的操作都无法再进行。

设置无限期的使用加密锁，需要以开发商权限登录后，选定取消时间限制，然后点击设置按钮，则可取消到期时间的限制。开发商也可以使用远程升级的方式，制作升级包对到期时间进行设定。

对于如何合理的设置到期时间，进行以下几点说明：

1. 锁内时间采用的是 UTC 时间（相当于本初子午线，即经度 0 度上的平均太阳时，比北京时间晚大概 8 小时），因此在设置时间时，集成编辑工具会将本地的具体时间转化成 UTC 时间后，设置到锁内。
2. 当加密设备到期后，仅仅是对用户权限进行了限制，因此在对锁内数据尤其是文件的读写和调用权限进行设置时，需要注意。

1.8.2 获取锁内时间和到期时间

对于时钟锁获取锁内时间和到期时间，匿名权限即可完成，但是锁内的时间是 UTC 时间，所以在获取锁内时间可能与本地时间是有差距的。到期时间也需要设置为标准的 UTC 时间，因此在设置到期时间时，最好先获取一下锁内时间，以锁内时间作为参照标准。

获取的到期时间就是设定好的使用截止时间，但是在此有一点需要进行说明，当设定到期时间选择的是到期的小时数，那么在没有使用用户权限登录加密设备之前，所获取到的到期时间是一个数值，而不是具体截止日期时间，只有当使用用户权限登录后，加密设备会自动计算出使用截止日期，这个时候再获取到期时间，则会显示具体的到期日期。

例如，使用开发商权限设置到期的小时数为 50，那么在没有校验过用户 PIN 码前，无论使用开发商权限（开发商权限）还是匿名权限，获取的到期时间都只是会显示 50 小时。而当加密锁校验过用户 PIN 码后，无论使用哪种权限登录，都会显示一个具体的到期时间。这也正说明了，若设定了到期的小时数，是从设置后的第一次校验用户 PIN 码开始计时的。

1.9 批量初始化

登录了集成编辑工具后，点击右下角的  图标，则可以返回到登录界面。此时，左下方的批量初始化按钮才可使用，点击“批量初始化”，即可进入批量初始化操作界面，如图所示：

图 14 批量初始化

ROCKEY-ARM 系列加密锁提供了两种批量生产的方式，一种是之前所介绍的使用母锁和升级包的方式（详见 1.7 制作母锁 和 1.6 远程升级），另一种方式就是使用集成编辑工具的批量初始化功能。

使用母锁加升级包的方式无需知道开发商 PIN 码、种子码、锁内数据等相关信息，更加的方便，安全，尤其更适用于保护与生产分离的生产模式中。使用集成编辑工具的批量初始化功能需要手动的配置锁内的信息。

ROCKEY-ARM 集成编辑工具还在批量初始化中提供了保存配置和加载配置的功能，也就是说，用户对批量初始化部分的数据进行了配置后，可以对所有的配置直接保存成文件，若日后生产相同配置的加密锁时，可以直接将保存好的配置文件加载到集成编辑工具中，无需再次进行相同的配置，十分方便。

1.9.1 基本设置（BASE）

双击列表框内的基本设置（BASE），弹出的设置框如图所示：

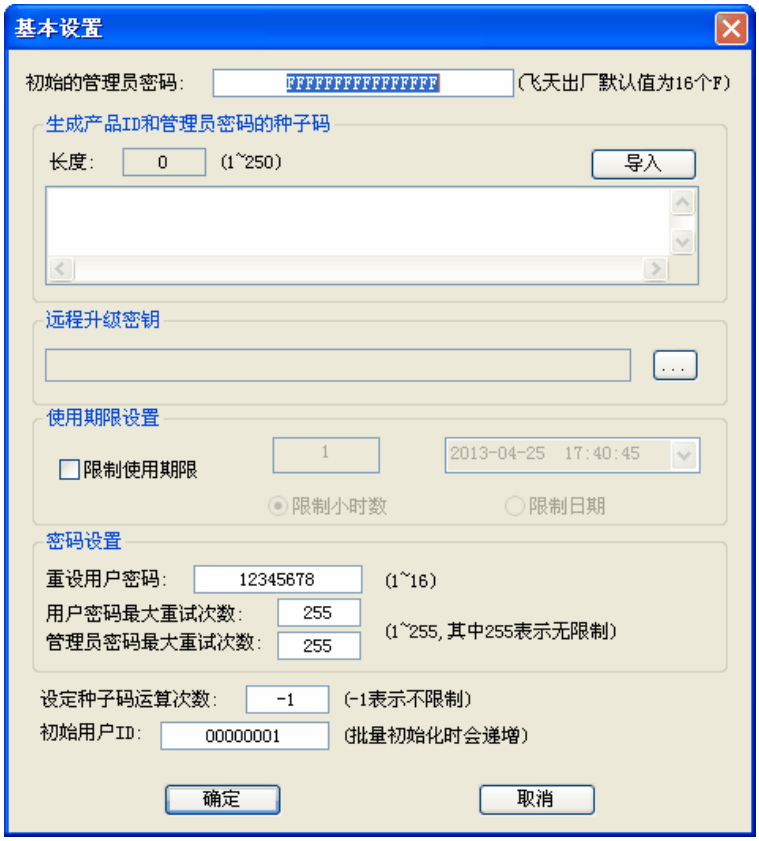

图 15 基本设置

初始的开发商 PIN 码是指的被初始化的加密锁当前的开发商 PIN 码，若对空锁进行初始化，那么初始的开发商 PIN 码为“FFFFFFFFFFFFFFFF”；所导入的生成产品 ID 和开发商 PIN 码的种子码不能为全 0，初始化后所产生的子锁的产品 ID 和开发商 PIN 码，就是用这里导入的种子码计算出来的；此处导入的远程升级密钥就是写入子锁的远程升级私钥，若要升级初始化后的子锁，则加密升级包的 RSA 升级公钥要与此私钥匹配。

使用期限设置是针对时钟锁有效的，对非时钟锁，即使在此设置了使用期限，在进行批量初始化的时候，工具会自动识别是否是时钟锁，不是时钟锁的情况下不会影响升级，但是此设置无效。

1.9.2 数据存储区（Memory）

在批量初始化中设置的数据存储区就是初始化后的子锁的数据存储区（详见 1.2.1 数据存储区），双击数据存储区（Memory），则弹出导入数据的对话框，如图所示：

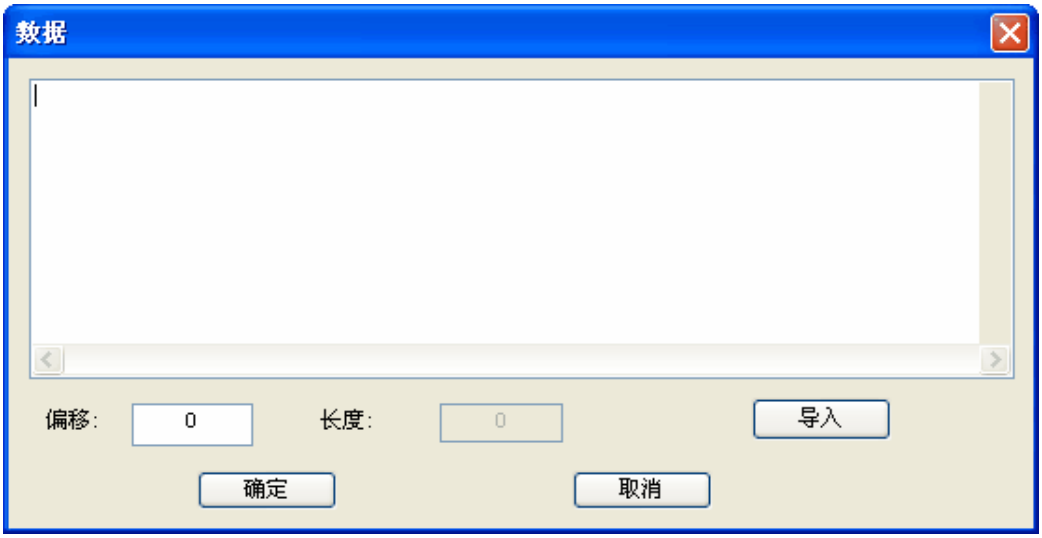

图 16 数据存储区

在进行批量初始化时，此数据存储区不能为空，必须导入数据。

1.9.3 初始化

在初始化数据设置中，配置好需要初始化的数据，添加好需要写入初始化到锁内的文件，对文件的添加和文件管理一致（详见 1.3 文件管理），点击初始化按钮，工具就能够依照配置信息，初始化加密锁。若勾选了自动批量初始化按钮，则可以根据配置数据初始化多把加密设备。

第2章 ROCKEY-ARM 子锁初始化工具

ROCKEY-ARM 系列加密锁对子锁的初始化方法有很多种，在第一章也有过相应的介绍（详见 1.51.唯一化锁 和 1.9 批量初始化），其中还有一种比较简单方便的方式，那就是使用基于母锁的子锁初始化工具（RyARMInitSon），如图所示：

图 17 基于母锁的子锁初始化工具

RyARMInitSon 工具的使用非常简单，只需点击一下初始化按钮，就可以达到对子锁初始化的目的。由于它是基于母锁来初始化的，因此在进行初始化时需要一把母锁和一把空锁。初始化完成后，空锁会按照母锁锁内的配置，初始化成相应的子锁。

使用 RyARMInitSon 工具来进行初始化子锁会更加的安全，尤其适用于保护与生产相分离的业务模式。初始化子锁的人员只需要拿到相应的母锁即可，无需知道生成子锁的种子码，远程升级私钥文件、用户 PIN 码等信息，因此，也确保了生成流程上的安全可靠。

第3章 ROCKEY-ARM 客户端远程升级工具

ROCKEY-ARM 系列加密锁的远程升级是指，开发商将加密锁卖给最终用户后，当需要对加密锁内部的数据进行更改时，不需要将加密锁从最终用户那里收回，而是制作远程升级包（详见 1.6 远程升级），将远程升级包通过网络发送给最终用户，而最终用户使用客户端远程升级工具 RyARMUpdater，将升级包导入进行升级，从而到达对加密锁内部数据进行更改的目的。

RyARMUpdater 客户端远程升级工具使用简单、安全，如图所示：

图 18 客户端远程升级工具

用于升级的数据文件就是远程升级包，开发商将远程升级包制作好，发送给最终用户，最终用户只需要将升级包导入到 RyARMUpdater 工具中，并且将相对应的锁插在 PC 机上，点击升级按钮，就可以升级成功，在状态的文本框中会有升级成功的提示信息，若升级中出现问题，则也会在状态的文本框中进行相应提示。

在使用客户端远程升级工具时，需要注意的是：

1) 所导入的升级包需要与加密锁匹配，即加密远程升级包的 RSA 升级公钥要与锁内的 RSA 升级私钥匹配，否则无法升级成功。

2) 每一个远程升级包对一把加密锁只有一次有效，也就是说，一个远程升级包无法对同一个加密设备进行重复性升级。

第4章 ROCKEY-ARM 外壳加密工具

外壳加密工具是通过加壳的手段对软件进行保护的。所谓加壳，其实是利用特殊的算法，对文件里的资源进行加密。加壳后的程序可以独立运行，数据会以密文形式存储，解密过程完全隐蔽，都在内存中完成。它们附加在原程序上通过 Windows 加载器载入内存后，先于原始程序执行，得到控制权，执行过程中对原始程序进行解密、还原，还原完成后再把控制权交还给原始程序，执行原来的代码部分。加上外壳后，原始程序代码在磁盘文件中一般是以加密后的形式存在的，只在执行时在内存中还原，这样就可以比较有效地防止破解者对程序文件的非法修改，同时也可以防止程序被静态反编译，这也是软件保护的通用手段。

加壳工具通常分为压缩壳和加密壳两类，ROCKEY-ARM 外壳加密工具属于加密壳，主要实现的就是对软件程序的保护，防止反汇编、反编译，防止黑客的逆向工程，从而保障了软件的安全。

本章将重点介绍 ROCKEY-ARM 外壳加密工具的使用方法，从介绍中也可以体会到 ROCKEY-ARM 外壳加密工具极高的安全强度，以及几乎无法破解的优越性。

4.1 介绍

ROCKEY-ARM 外壳加密工具在软件保护中起到了至关重要的作用，并且在对文件进行加密时，将加密锁与待加壳的程序建立起了紧密的联系。程序运行过程中使用加密锁进行加解密，使软件对加密锁的依赖性大大的增加。利用加密锁专用芯片的不可复制性，使软件也具有不可复制性，从而实现软件保护的目的。

ROCKEY-ARM 系列产品提供了一个 32 位外壳加密工具，可以为 32 位的可执行文件（.exe、.dll、等）、数据（视频文件、音频文件等）和 Java 程序（.jar 文件、.class 文件等）加壳，其操作界面如图所示：

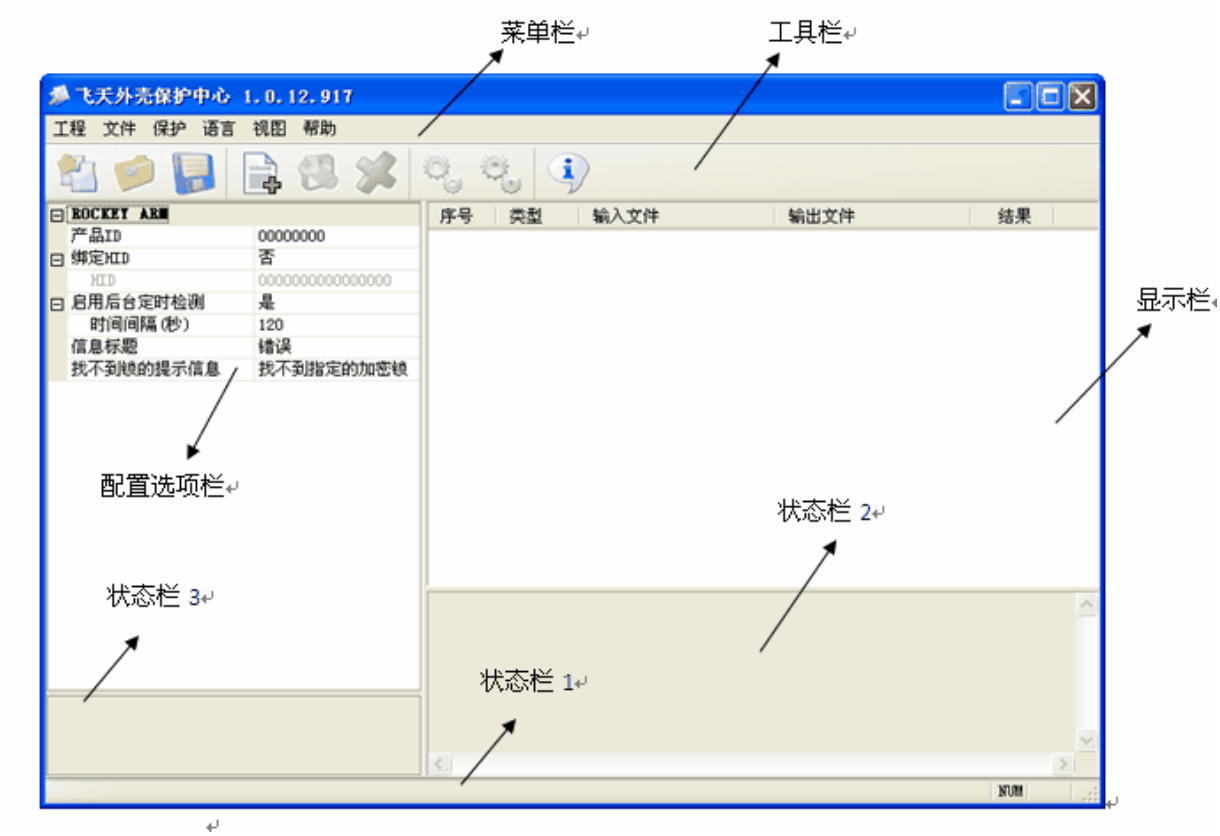

图 19 外壳加密工具

4.2 外壳加密的优点

外壳加密工具使用极为简便，只需几秒钟就可完成对文件的加密。ROCKEY-ARM 外壳加密工具有如下优点：

1. 不需要源代码
2. 操作简单易用
3. 零开发成本
4. 加密强度高
5. 加密文件类型多、范围广
6. 加密速度快
7. 可多个文件同时加密
8. 不需要开发者学习很多的加密知识
9. 对于加密后文件，即使用户在加密锁内定义了极其复杂的加密算法，也能够保证用户程序的顺畅运行

ROCKEY-ARM 外壳加密工具从用户角度出发，最大限度地简化使用接口。用户能够在很短的时间内掌握 ROCKEY-ARM 外壳加密工具的加密方法，节约在软件加密上所投入的时间。

进行外壳加密时，加密文件的速度快，即使是多个文件同时加密，花费的时间也很短。ROCKEY-ARM 外壳加密工具是在一定的算法复杂度的前提下进行加密，程序被破解的可能性几乎为零。

在采用外壳加密工具（Envelope）加密保护您的软件之前，请您注意备份要保护的文件。您可以仅利用一把 ROCKEY-ARM 加密锁使用外壳加密工具（Envelope）来多次和采用不同方法处理保护您的软件。

4.3 使用指南

4.3.1 添加文件的三种方式

1. 通过菜单栏的文件。选择“添加文件”选项，弹出如下对话框：

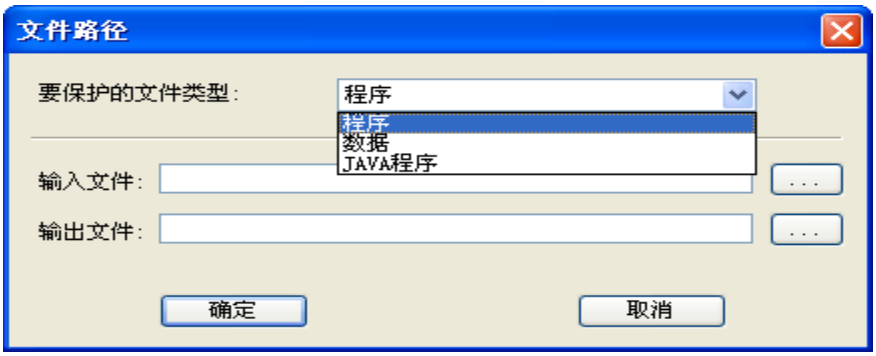

图 20 添加文件

在“要保护的文件类型”处选择要添加的文件类型，对要保护的文件要选择正确的文件类型， 即使文件以一种与其不匹配的类型的形式添加，并成功加密，但是加密文件运行不会成功。

在输入文件处点击  ，弹出打开窗口，如图所示：

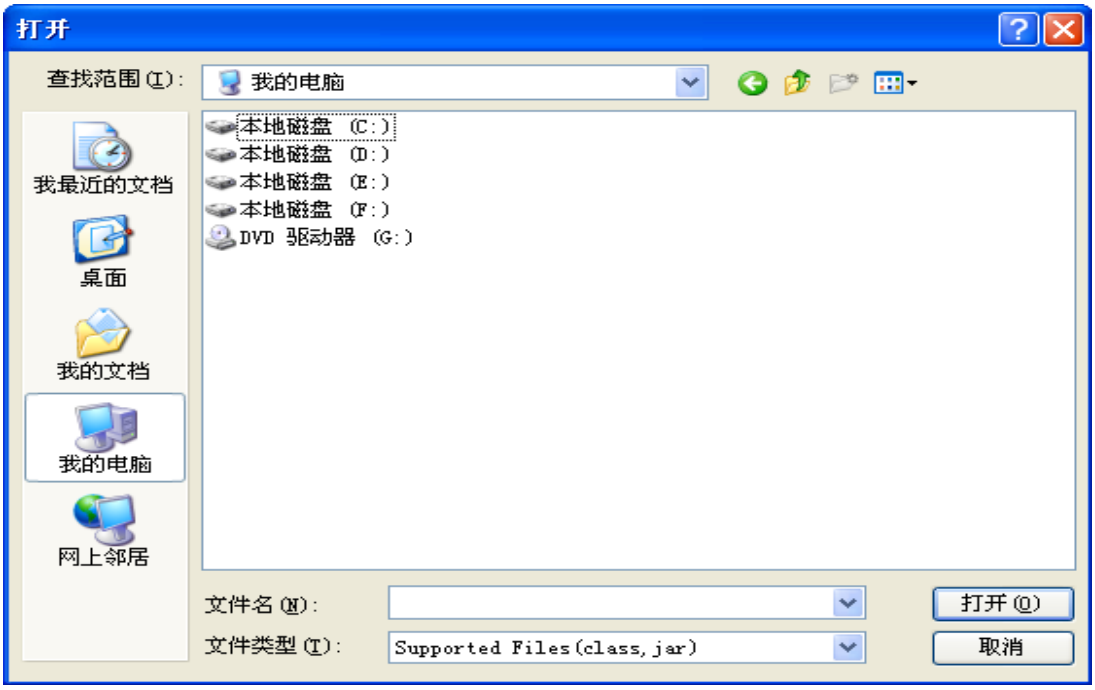

图 21 打开输入文件

选择要添加的文件路径，选择文件（文件类型为.class 或者.jar）点击打开按钮，这时添加文件窗口如图所示：

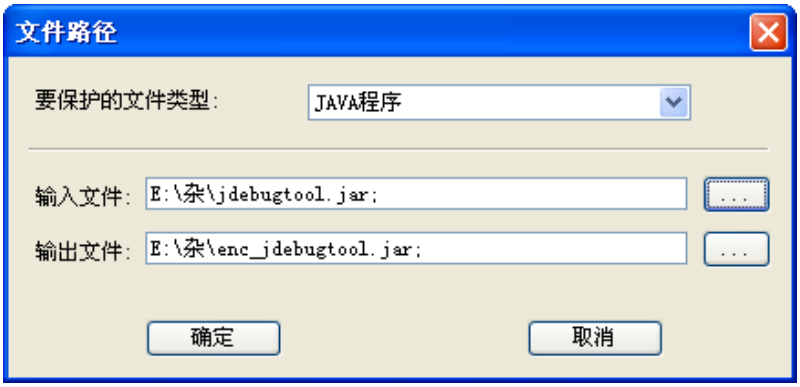

图 22 完成添加文件

“输出文件”会自动显示输出文件路径和输出文件名，我们可更改输出文件路径，具体操作详见 4.3.2 编辑文件路径三种方式。点击确定按钮，该文件将会成功添加到外壳加密窗口内，在显示栏会相应的显示刚刚添加的文件。如图所示：

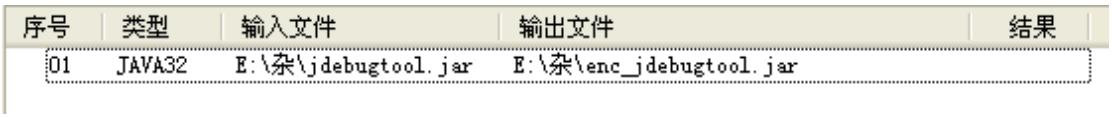

图 23 显示添加文件

新添加文件的路径和加密后文件的路径都会显示在界面上，如上图。如果想继续添加文件，只需在文件菜单再次选择添加文件，用上面提到的同样的步骤添加文件。

2. 通过工具栏的图标按钮  。鼠标左键单击该图标，出现如图 20 一样的窗口，接下来的添加文件步骤同上类似，这里不再赘述。

3. 通过拖拽的方式。将 Envelope 窗口和你要添加文件所在的文件夹同时打打开，选择你要添加的文件，可单个也可多个，选定完成后，按住鼠标左键不放将文件拖拽到外壳加密工具窗口后放开鼠标，若添加成功，选定的文件信息会出现在显示栏中。添加完成后，程序会自动识别添加的文件类型，如图 23 所示。若要继续添加文件，重新拖拽即可。

4.3.2 编辑文件路径三种方式

1. 文件菜单的编辑文件路径。在显示栏选定一个文件，以刚刚添加的文件为例，如图 23 所示文件，选择文件菜单中的编辑文件路径选项，弹出如下对话框：

图 24 文件路径

在输出文件处点击  ，弹出“浏览文件夹”窗口，如图所示：

图 25 浏览文件

选择输出文件要存储的路径，点击确定按钮，修改路径完成。文件加密成功后，加密文件会自动存储在修改的路径下。

2. 工具栏的图标按钮  。选定文件，鼠标单击该图标，弹出如图 24 所示窗口，接下来的编辑文件路径步骤同上类似，这里不再赘述。

3. 双击文件。在显示栏选定文件，鼠标双击该文件，弹出如图 24 所示窗口，接下来的编辑文件路径步骤同上类似。

4.3.3 移除文件的两种方式

1. 文件菜单的移除文件：选定单个文件或多个文件，在菜单栏的文件菜单下选择“移除文件”，选定 的文件将会移出外壳加密工具窗口。

2. 工具栏的图标按钮  ：选定单个文件或多个文件，鼠标单击图标按钮  ，选定文件就会移除。

4.3.4 工程

1. 保存到工程：若想将添加的文件信息保存起来，可选择工程菜单下的“保存到工程”选项，也可通过单击图标按钮  将所有添加的文件保存到工程，弹出另存为对话框，选择工程要保存的路径，在“文件名”处写入工程要保存成的名称，点击“保存”，工程保存成功。

2. 打开工程：选择工程菜单下的“打开工程”选项或单击图标按钮  ，弹出“打开”对话框，选择要打开的工程，打开工程后，显示栏会显示工程中的所有文件信息。

3. 新建工程：选择工程菜单下的“新建工程”选项或单击图标按钮  ，Envelop 窗口界面会出现一个新的 Envelope 界面。

4.3.5 保护

1. 保护当前文件：选定单个文件或多个文件，选择保护菜单下的“保护当前文件”或单击图标按扭  ，即可对当前工程下选定的文件加密，不选定的文件不会加密。

2. 保护全部文件：选择保护菜单下的“保护全部文件”或点击图标按钮  ，即可对当前工程下的全部文件加密。

4.3.6 语言

1. English：选择语言菜单下的English，窗口界面转换为英文界面。
2. Sample_Chinese：选择语言菜单下的Sample_Chinese，窗口界面转换为简体中文界面。
3. Tradition_Chinese：选择语言菜单下的Tradition_Chinese，窗口界面转换为繁体中文界面。

4.3.7 视图

1. 工具栏：视图菜单下，工具栏前有√，窗口界面会显示工具栏，若无√，窗口界面不显示工具栏。
2. 状态栏：视图菜单下，状态栏前有√，窗口界面会显示状态栏1，若无√，窗口界面无状态栏1。

4.3.8 帮助

在帮助菜单下，点击关于选项或点击图标按钮  ，弹出关于对话框，此框内会显示有关该外壳加密工具相关的一些信息。

4.3.9 加密文件

在电脑上插入一把 ROCKEY-ARM，为以后叙述方便，现将该把锁记为 A。打开 Envelope 工具，进入如图 19 所示的 ROCKEY-ARM 外壳加密工具窗口界面。添加文件，根据添加的文件类型不同，配置选项栏会相应的显示与该文件相匹配的外壳选项。文件添加成功后根据需求，在配置选项栏处选择要绑定的信息，信息绑定后就可以对文件进行加密操作。在配置选项栏选定某一信息栏时，在操作状态栏 3 处将会相应的显示选定的信息。

4.3.9.1 配置选项栏

1. 配置选项栏界面如图 19 所示，下面分别介绍配置选项栏中不同选项的功能：

产品 ID：外壳加密工具加密文件时，产品 ID 是必须要输入的。外壳加密工具加密文件会用产品 ID 去找加密锁，输入不是加密锁 A 的产品 ID，会找不到加密锁 A，文件加密不会成功。产品 ID 初始值为“00000000”，可以通过 ROCKEY-ARM 加密锁设置工具来重新设置产品 ID。在设置产品 ID 时，为了防止其他人设置相同的产品 ID，ROCKEY-ARM 采用了种子的方式来生成产品 ID，即开发商输入产生产品 ID 的种子（种子长度最大为 250 字节），ROCKEY-ARM 会在锁内部根据该种子产生相应的产品 ID，而且是不可逆的。只有生成者才知道什么样的种子能生成自己的产品 ID，这样其他人即使获得了产品 ID，但由于不知道产生产品 ID 的种子，因此无法设置相同的锁，大大增强了安全性。

HID：为硬件 ID。每个 ROCKEY-ARM 内部都有一个唯一的硬件 ID，这个硬件 ID 是在 ROCKEY-ARM 出厂时烧 入的，即使是厂家也不能修改，而且这个硬件 ID 具有唯一性。当开发者需要给特定用户加密时，则

外壳加密工具可绑定 HID，通过检查这个 ID 来确认加密的唯一有效性，提高了安全性。绑定加密锁 A 的 HID，加密文件。加密文件使用加密锁 A 可以打开，其余任何一把 ROCKEY-ARM 加密锁都打不开。若绑定的 HID 不是加密锁 A 的，加密锁 A 虽对文件可以加密，但是使用加密锁 A 无法打开文件，只有 HID 为绑定的 HID 的那把锁才能够打开文件。

后台定时检测：选择此项后，应用程序在运行时，将按设置时间检测 ROCKEY-ARM 是否存在，防止加密锁被拔出后程序还能运行。在“时间间隔”的输入框中填写检查 ROCKEY-ARM 的间隔时间。在程序运行过程中，若将锁拔出，到检测时间，运行的文件自动暂停，弹出提示信息（外壳加密工具设置的时间间隔大于等于 60 秒，低于 60 秒无法加密文件）。

信息标题：找不到锁时弹出的提示框的标题，默认的设置是“错误” 。

找不到锁的提示信息：在其后设置提示信息，在未插入锁而打开程序或程序运行中拔锁等情况下，弹出的提示信息会与设置的文字相一致，默认的设置是“找不到指定的加密锁”。

2. 加密不同类型文件，在配置选项栏会对应添加的文件类型来显示 PE 外壳选项、DATA 保护选项、.NET 外壳选项或 JAVA 外壳选项。下面对这四种类型分别介绍：

PE 文件：若添加文件类型为 PE，在配置选项栏会相应的显示 PE 外壳选项。加密 PE 类型文件时，若启用数据文件保护选项，加密后 PE 文件不依赖于加密锁，但是可用该加密后的 PE 播放器文件对应打开加密后的 data 文件，这样真正保护的目标是 data 文件。若不启用数据文件保护，加密后 PE 文件依赖于加密锁，这样真正保护的目标是 PE 文件。绑定其余 PE 选项信息如：反调试、检查父进程、指令替换和启用区块对齐后，加密文件时 ，不容易看出区别，在这里不做细述。

Data 文件：若添加文件类型为 Data，在配置选项栏会相应的显示数据保护选项。对数据文件加密，在算法选择处可选择 3DES/RC4 算法对文件加密 。对 Flash/PDF/音频/视频等 data 文件进行外壳加密时，想要加密文件正常播放，就必须由该外壳工具也对这些文件对应的播放器工具如：Flash 播放器/Adobe/暴风影音等 PE 类型文件加密，加密 PE 类型文件时要启用数据文件保护，使用这些加密后的 PE 播放器才能正常播放加密的 Flash/PDF/音频/视频等数据文件。

.Net 文件：若添加文件类型为.Net，在配置选项栏会相应的显示.NET 外壳选项。算法选择处可选择 3DES/DES 两种不同算法对文件进行加密。对方法列表选项处，单击  ，出现类似如图所示的“选择需要加密的函数”窗口：

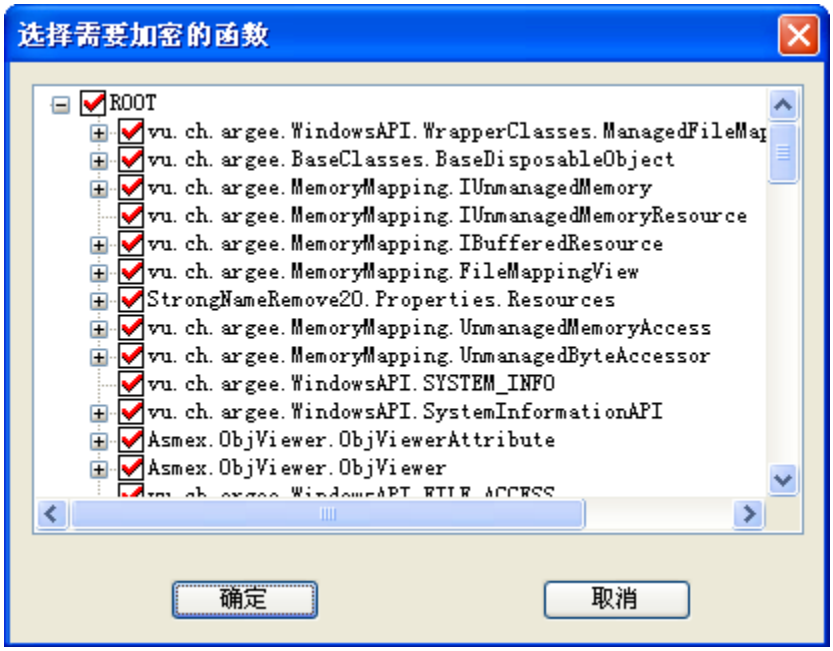

图 26 选择加密函数

当所有函数全选时，在方法列表处显示“全部加密”，若有函数未选中，在方法列表处显示“部分加密”，若在加密.net 文件过程中失败，外壳加密工具会自动备份原文件，备份文件以.rybak 为后缀。

Java 文件：若添加文件类型为 Java，在配置选项栏会相应的显示 JAVA 外壳选项，对 Java 保护选项。可根据需要设定 “反调试”，这样在 Java 程序运行时会检测运行的环境；“JAVA 运行时选项”处有 Java.exe 和 Javaw.exe 两种不同选择，它们都只是一个 Java 包装程序，区别是前一个运行 Java 程序会出现一个命令行窗口，后一个则没有；“加密算法”选项中可选择 RC4 和 3DES 两种不同算法。

由于使用 Java 保护外壳对 Java 程序保护后，原程序格式已被破坏，要运行就必须先解密，而解密的功能是由我们选择的包装程序完成的如：Java.exe 或者 Javaw.exe。

JAVA 程序加密后的运行方法：

1. 运行桌面程序

首先插入绑定的加密锁，点击“开始”——“运行”，然后输入 cmd，在命令行窗口中输入<加密后生成 java.exe 所在路径> -jar <加密后的 Java 程序所在路径>。例如我们加密了一个 example.jar，选择“Java 运行时”为 Java.exe，选择输出路径在“C:\protect\enc_example.jar”，那么在“C:\protect\” 目录下会产生一个 Java.exe，要运行这个 Java 程序，我们只要输入命令：“C:\protect\java.exe”-jar “C:\protect\enc_example.jar”。

2. 运行 WEB 程序

以 tomcat 为例，首先选择需要加密的 class 文件进行加密，然后放到网站的 classes 目录中。 在 tomcat 的安装目录中找到 bin 目录，然后在 bin 目录中找到 setclasspath.bat 文件，使用文本编辑器打开，然后在里面查找 set _RUNJAVA=“%JRE_HOME%\bin\java” 语句， 把它替换成：set_RUNJAVA=<加密时生成的 Java.exe 或 Javaw.exe 所在路径>，例如加密时生成 C:\protect\java.exe，则设置为：set _RUNJAVA=“C:\protect\java.exe”。最后运行 startup.bat 启动 tomcat，此时加密的类就能被正确加载了。

当运行加密后的 java 文件时提示“系统无法执行指定的程序”，说明缺少了 Microsoft Visual C++运行库，可直接安装 Framwork 2.0 解决该问题。

4.3.9.2 加密绑定信息的文件

绑定信息设置完成后，对文件开始加密，文件加密成功后，在显示栏会有绿色的圆框显示加密成功，同时在状态栏 2 也会显示 Result：success，窗口界面显示如下图，

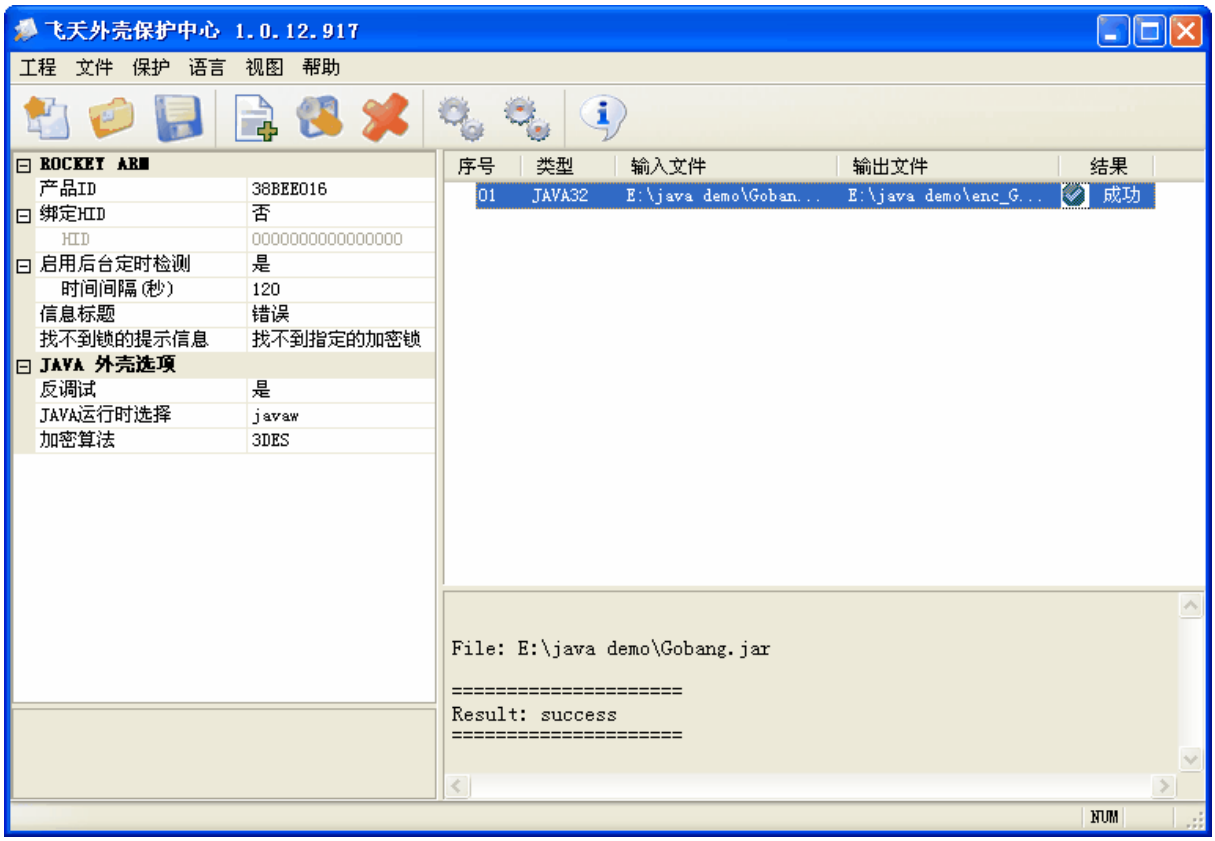

图 27 加密文件

若文件加密失败，在显示栏会有红色的圆框显示加密失败，在状态栏 2 也会显示 Result：failed，在状态栏 2 会有提示错误码，有利于查找错误。

第5章 ROCKEY-ARM 工程向导工具

下载到 ROCKEY-ARM 系列加密锁内的可执行文件，是通过 Keil uVision4 工具进行编译的。为了方便用户创建工程，我们提供了一个工程向导工具（ARMProjWizard）。使用 ROCKEY-ARM 向导工具，就可以很轻松的创建一个项目，不需要用户对 Keil 集成环境进行过多的配置。本章的内容将重点介绍如何使用 ROCKEY-ARM 来创建工程。

双击 ARMProjWizard.exe 工具，弹出 ARM 工程向导的界面，如图所示：

图 28 ARM 工程向导

在工程名称中填入相应工程的名称，点击 ... 按钮，选择要保存路径，如图所示：

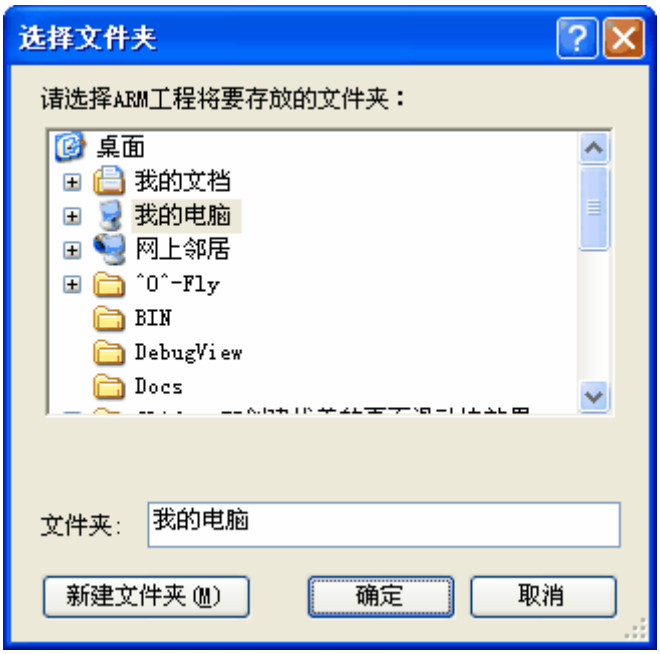

图 29 选择文件夹

选定好相应路径后，点击确定按钮，然后再点击图 28 界面上的创建工程按钮，则就在保存路径下，创

建了一个所设定好的工程，此时，工具提示是否打开工程目录，如图所示：

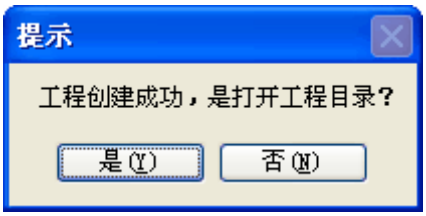

图 30 提示信息

点击是，则自动打开在相应路径下创建好的项目目录，如图所示：

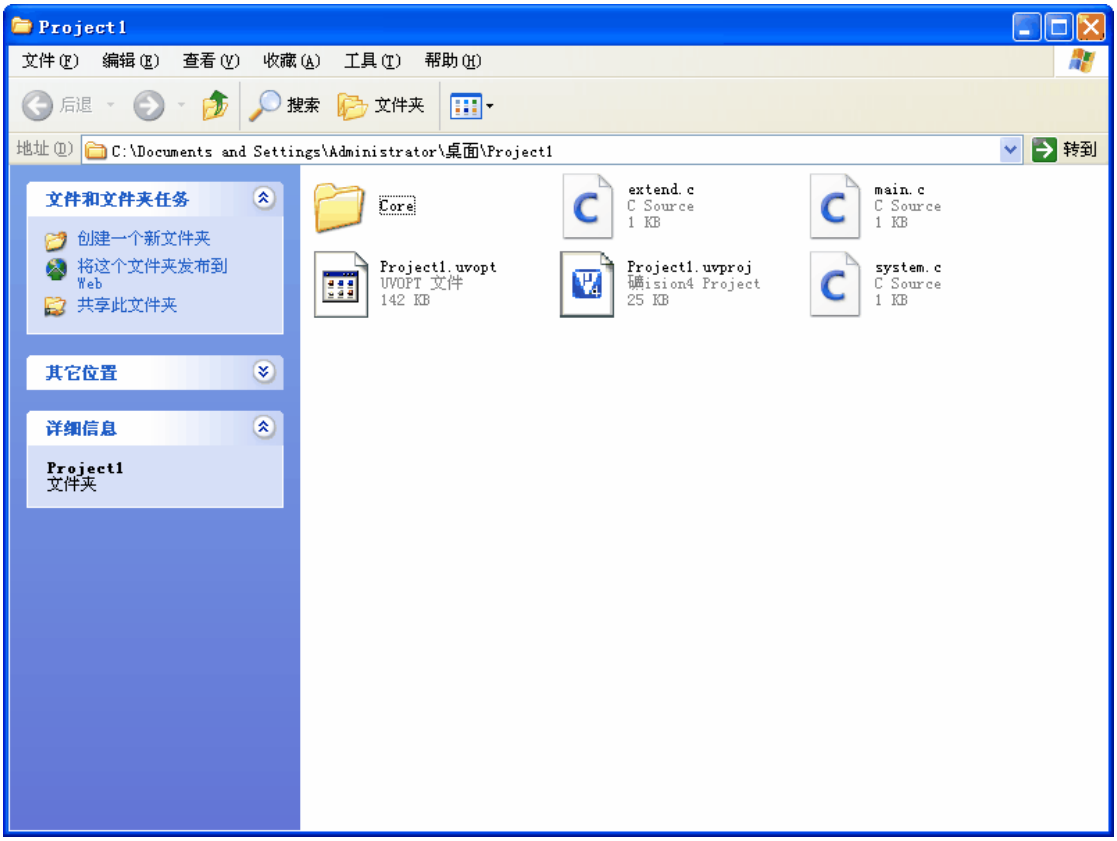

图 31 工程目录

在没有安装 Keil uVision4 工具的主机上，也是可以使用 ROCKEY-ARM 工程向导工具来创建工程的，但是无法将工程文件打开。双击.uvproj 文件，则可以将此工程打开，并按照软件需要，编写锁内的可执行文件。编写好的代码程序经过编译后，就会在工程目录下生成一个与工程名称相同的.bin 格式的文件，将此文件通过集成编辑工具中提供的可执行文件的下载功能（详见 1.3.1 可执行文件的下载），将可执行文件下载到锁内，并测试其运行（详见 1.3.1 可执行文件的运行）