

U 盘加密技术在终端设备中的应用前景

曹冬华，俞海猛，丁 健，王 腾

(国电南瑞科技股份有限公司，南京市高新路 20 号 210061)

摘 要：在我国智能电网不断优化和完善的进程中，对于终端设备的功能优化需求亦在不断提高之中，U 盘的程序升级运用可以有效的方便现场工程人员进行程序的更换，而随着 U 盘升级的普遍运用，对于设备升级文件的保护措施也成为了终端设备厂家关注的重点，普通 U 盘只能作为升级程序的一种传输介质，没有保护信息安全的功能，加密 U 盘就可以很好地对文件传输过程进行监督和对信息进行保密，终端程序升级以及终端设备信息的导出必须采用加密 U 盘配合输入正确的操作密码才能执行相应的操作。本文简单论述加密 U 盘的加密方式的分类以及终端设备的具体信息，阐述了加密 U 盘对终端设备进行升级的整个通讯逻辑。

关键词：U 盘；加密技术；终端设备；AES 算法

0 引言

在传统的终端设备升级过程中，现场维护人员通常是通过 U 盘设备对现场设备进行维护，由于 U 盘设备具有体积小、容量大、操作简单携带方便以及支持热拔插的优点，可以为现场维护人员的设备维护减少大量的工作量，极大地提高工作效率，但 U 盘在广泛运用的同时，也为用户带来的极大地安全隐患，因为 U 盘存储文件以及程序升级的整个过程是完全透明的，一旦丢失，存储的所有数据和信息都将任意读出。为此，需要一种既高度安全又安全使用的 U 盘用来存储用户敏感数据，加密 U 盘很好的做到了这一点。

加密 U 盘作为普通 U 盘的升级版，能够将升级文件有效的进行保密，将 U 盘的 AES 算法加密与终端设备的界面密码解密结合在一起，既能保证现场终端升级流程的快速性又能有效地保证终端设备厂家知识产权的安全性，现场工作人员只有在设备中输入正确密码才能完成升级和终端设备信息的转出操作，这样可以有效的避免误升级操作的产生。

1 加密 U 盘与终端设备的通信机制

1.1 终端升级机制

加密 U 盘与终端设备的信息交互通过 USB 接口进行，U 盘加密机制以图 2 为例，首先将加密 U 盘连接电脑设备，将需要存储的终端升级程序进行存储，终端设备升级程序通过 NANDFLASH 存储

芯片存入 U 盘设备，存储文件经过硬件加密结合 AES 加密算法对存储文件进行加密存储。



图 1 U 盘加密机制

终端设备的解密机制以图 3 为例，终端重启识别到 USB 接口有加密设备申请对其进行升级，终端弹出输入密码提示框，现场人员只有 3 次输入密码机会，若 3 次密码都输入错误，终端将退出密码输入界面跳转至终端应用界面执行日常功能操作，若在 3 次允许范围内密码正确输入，加密 U 盘中的密文文件将转换为明文文件对终端设备进行本地升级。

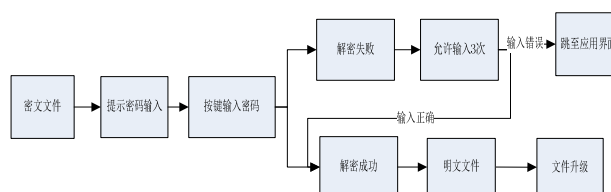


图 2 终端解密机制

2 U 盘加密架构

如图1所示，加密U盘由USB接口与控制器、程序与密钥存储器、Flash存储器、电压转换电路、时钟电路等模块组成，共同完成与主机通信、用户口令认证、AES加密存储数据、密文存储等功能。USB 接口与控制器主要完成与主机U S B 接口的通讯工作以及固件程序的执行；程序及密钥存储器用

于存储用户固件程序以及存储密钥和算法参数; Flash 存储器用来存放用户信息数据、软件和敏感数据, 密文存储; 电压转换电路将从 USB 总线上获取的 +5 V 电压转换为 +3.3 V。

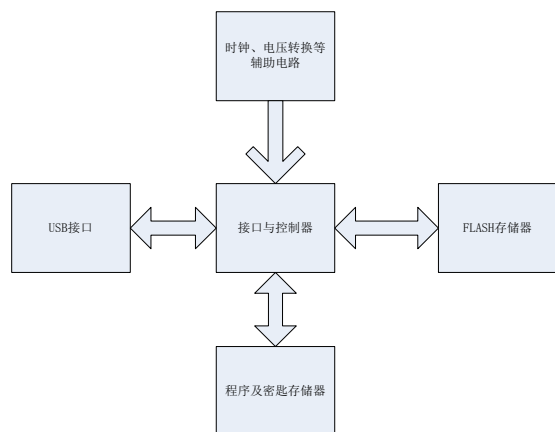


图3 加密U盘整体结构图

在加密部分, 本方案采用 AES 算法来对 U 盘进行 U 盘设备的加密, AES 是一个迭代的, 对称密钥分组的密码, 他可以使用 128、192 和 256 位密钥, 并且用 128 位分组加密和解密数据, 对称密钥密码使用相同的密钥加密和解密数据。通过分组密码返回的加密数据的位数与输入数据相同。迭代加密使用一个循环结构, 在该循环中重复置换和替换输入数据。

3 AES 算法介绍

3.1 AES 算法结构介绍

AES 使用 128、192 和 256 位密钥, 用 128bits 分组加密和解密数据。对称密钥密码使用相同的密钥加密和解密数据, 通过分组密码返回的加密数据位数与输入数据相同。使用循环结构迭代加密, 在该循环中重复置换 (Permutations) 和替换 (Substitutions) 输入数据。

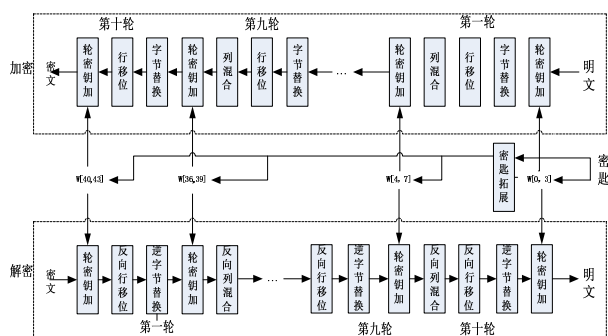


图4 AES 加密和解密

图2给出了 AES 算法的总体结构。加密和解密算法的输入是一个 128 比特的分组, 分组是一个字节方阵, 被复制到状态数组, 这个数组在加密或解密过程中的每一步都会被更改。直到最后一步结束后, 状态数组将被复制到输出矩阵。类似地, 128 比特的密钥也被描述为一个字节方阵。然后, 密钥被扩展成为一个子密钥的数组。每个字是 4 字节, 而对于 128 比特的密钥, 子密钥总共有 44 个字, 矩阵中字节的顺序是按列排序的。比如, 128 比特的明文输入的前 4 个字节占输入矩阵的第 1 列, 接下来 4 个字节占第 2 列, 以此类推。

3.2 AES 算法步骤介绍

AES 算法主要包括: 字节替换、行移位、列混合和轮密钥加四个步骤。

字节替换 (Substitute Byte)。使用一个表 (被称为 S 一盒) 对分组进行逐一字节替换。S 一盒是 AES 定义的矩阵, 把 State 中每个字节的高 4 位作为行值, 低 4 位作为列值, 然后取出 S 一盒中对应行列的元素作为输出。这个步骤提供了 AES 加密的非线性变换能力。S 一盒与有限域乘法逆元有关, 具有良好的非线性特性。为了避免简单代数攻击, S 一盒结合了乘法逆元及可逆的仿射变换矩阵建构而成。

行移位 (Shift Row)。每一行都向左循环移位某个偏移量。在 AES 中 (区块大小 128 位), State 的第一行维持不变, State 的第二行循环左移 1 个字节。同理, State 的第三行及第四行分别循环左移 2 个字节和 3 个字节。经过 Shift Row 之后, 矩阵中每一列, 都是由输入矩阵中的每个不同列中的元素组成。行移位就是将某个字节从一列移到另一列中, 它的线性距离是 4 字节的倍数。

列混合 (Mix Column)。每列的四个字节通过线性变换互相结合, 对每列独立进行操作。每列的四个元素分别当作系数, 合并后即有限域中的一个多项式, 接着将此多项式和一个固定的多项式相乘。此步骤亦可视为有限域之下的矩阵加法和乘法。矩阵的系数是基于在码字间有最大距离的线性编码, 也是基于算法执行效率的考虑。Mix Column 函数接受 4 个字节的输入, 输出 4 个字节, 每一个输入的字节都会对输出的四个字节造成影响。因此, Shift Row 和 Mix Column 两步骤为这个密码系统提供了扩散性。经过几轮列混和变换和行移位变换后, 所

有的输出位均与所有的输入位相关。

轮密钥加(Add Round Key)。在每次的加密循环中，都会由主密钥扩展产生一组轮密钥(通过 Rijndael 密钥生成方案产生)，这个轮密钥大小会跟原矩阵一样，该步骤就是轮密钥与原矩阵中每个对应的字节做异或运算。轮密钥加变换非常简单，却能影响 State 中的每一位。密钥扩展的复杂性和 AES 的其他阶段的复杂性，确保了该算法的安全性。

3.3 AES 算法模块介绍

AES算法主要分为三大模块，即密钥扩展，数据加密和数据解密。

密钥扩展。使用 Rotword()函数将数组中左端第一个数字移至数组的末端，而原来在它之后的数字依次前移一位，即对数组中的数字实现循环左移一位的运算。由于数组中的 4 个数字已合并为一个数字，在程序的实际执行过程中是进行数字的循环移位运算，而不是做数组的循环左移运算，这样可以大大简化运算过程，很大程度提高了运算效率。

数据加密。依据 S 置换表，使用 SubByte()函数对状态矩阵 State[4][4]中的数字进行置换。使用 ShiftRow()函数对状态矩阵 State[4][4]中的各行数据进行循环移位运算。循环移位遵循以下规则，状态矩阵 State[4][4]中的第一行数据位置不变，第二行数据循环左移一位数字，第三行数据循环左移两位数字，第四行数据循环左移三位数字。

数据解密。依据 S 置换表的逆表，使用 InvSubByte()函数对状态矩阵 State[4][4]中的数字进行置换，置换方法与 SubByte()函数相同。使用 InvShiftRow()函数对状态矩阵 State[4][4]中的各行数据进行循环移位运算。AES 的解密算法和加密算法不同。尽管密钥扩展的形式一样，但在解密中每轮交换步骤的顺序与加密中的顺序不同。其缺点在于对同时需要加密和解密的应用，需要两个不同的软件或固件模块。

4 方案的可行性分析

该方案中需要在终端设备硬件上添加解密芯片来进行加密文件的解密以及终端设备的升级，传统的U盘升级全部采用明文升级，这种升级方式虽然操作简单，但是整个文件升级的过程都是透明化的，这种升级方式对于升级文件的保密以及终端设

备的维护是极为不利的，一旦U盘设备丢失，就意味着升级文件以及与工作相关的信息丢失甚至为他人所用。加密U盘的运用将有效避免上述问题的发生，加密U盘与终端设备的文件传输完全采用密文传输，不会出现传输过程中信息泄露的情况，U盘设备即使丢失也能有效地保证存储文件的安全性。

U盘加密以及终端设备机密技术的运用虽然会增加终端设备以及U盘设备硬件的成本花费，软件开发上也增加了难度，但是考虑到现场终端设备升级文件的安全性以及各终端厂家现场升级的流程规范性，这笔小投入将会收到巨大的回报。

5 结束语

U 盘设备是现场工程人员常用的现场终端设备维护工具，U 盘设备对终端设备的升级可以在极短的时间内对终端设备进行程序更新以保持现场设备的正常运行，U 盘加密机制的引入可以较好的保证现场升级文件的安全性和现场维护流程的规范性，为电力用户用电信息采集系统建设的“安全性、可靠性”作出贡献。

参考文献：

- [1] 郎荣玲,戴冠中.高级加密标准(AES)算法的研究[J].小型微型计算机系统,2003,24(05):905-908.
- [2] 卡哈特(Atul Kalate). 金名(译).密码学与网络安全[M]. 北京:清华大学出版社,2005:9.
- [3] 易青松,苏锦海,岳云天,等.基于CY7C68013安全U盘的硬件设计[J].计算机工程与设计.2007,28(06):297-299.

作者简介：

曹冬华(1987-)，男，助理工程师，学士，从事用电专业方向研究工作；

俞海猛(1988-)，男，助理工程师，学士，从事用电专业方向研究工作；

丁 健(1988-)，男，助理工程师，学士，从事用电专业方向研究工作；

王 腾(1988-)，男，助理工程师，学士，从事用电专业方向研究工作。