**配置文件转化为EEP数据的设计**

**下图为PC界面配置数据转化流程图：**

下载

读取

控制器\CPU

RAM

EEP

PC用户

配置文件

EEP代码

打开

保存

下面就配置文件加密处理工具及方式方法进行描述：

设计一个工具，将PC界面生成的‘配置文件’转化为E2P中写入的‘密文数据’。

**操作步骤：**

选择配置文件

自动生成密钥

生成EEP数据

1. 转化工具中可选择任意目录下的‘配置文件’载入
2. 点击‘生成密钥’，可自动生成加密算法密钥。密钥为明文可见，由四个8bit数据组成；每个数据在0～255之间；当不满意时，可人为重复点击‘生成密钥’按键再次生成新密钥。密钥组合不允许出现重复。密钥个数应为254×254×254×254 > 41亿。可满足应用周期所有密钥要求。
3. 点击‘生成密文’按键，可直接将配置文件经由步骤2生成的密钥加密为密文，并保存为EEP的\*.BIN文件，可自由选取保存路径及命名保存文件。

**加密算法：**

密钥：

|  |  |  |  |
| --- | --- | --- | --- |
| B4 | B3 | B2 | B1 |

配置文件中的源码：Y0、Y1、Y2……

加密后的密文：M0、M1、M2……

加密过程数据：Y01、Y02、……

1. 加密运算步骤一：Y0 + B1 = Y01
2. 加密运算步骤二：Y01循环左移 （B2/8的余数）次 = Y02
3. 加密运算步骤三：Y02 异或 B3 = Y03
4. 加密运算步骤四：Y03高低四位互换 ＝ Y04
5. 加密运算步骤五：Y04 – B4 = M0

配置文件中的所有原文：Y0、Y1、Y2……，均需经以上5个步骤生成各自对应的密文：M0、M1、M2……。数据对应位置顺序不做变化。

密文集合保存为\*.bin文件作为EEP的写入文件。

配置文件及密文数据中的数据定义、保存位置定义及校验和等其他请参看<E2P中数据定义.doc>