# PLib

## Private Library

# 目录

# 1 简介

PLib 为私有库，主要目的有三个：

- 防止程序被读出，杜绝各种破解方式
- 方便中间方案商保护知识产权，可以将其核心算法固化再提供给终端客户二次开发，而不会泄露核心代码
- 加入版权保护信息，方便维权

# 2 主要特征

- 操作简单，安全可靠
- 不影响程序的运行性能
- PLib 分为 ICODE 和 DCODE 保护区：ICODE 为指令区，DCODE 为数据区
- ICODE、DCODE 保护区各自独立设置，可只打开一个或全部打开保护功能
- ICODE、DCODE 空间不允许重叠（任何对重叠部分的访问都视为非法）
- 擦除版权保护信息时，会擦除 PLib
- 全片擦除时会跳过 PLib

# 3 工作原理

MCU 在运行程序时，指令通过 IBUS 读取，数据通过 DBUS 读取。一般 MCU 在设计时都使用单个 FLASH，其指令、数据一起存入 FLASH 中，IBUS、DBUS 都可以访问 FLASH。因此，如果以读取数据的方式（例如调试器、用户程序、木马程序等）将 FLASH 内容输出（通过串口、USB 等接口），则程序无法保密。

对于需要保护的程序段（仅指令），如果切断 DBUS 的访问路径，使其可以执行却不能被读取，便可达到既不影响执行又不会泄密的功能，因此，设计 PLib ICODE 区域，可有效保护需要执行的程序段。而 PLib DCODE 区域，则是为了固定程序中的定义的常数，防止对其进行擦除。

- 对于 PLib ICODE，只允许 IBUS 读取，禁止所有写入；禁止 DBUS 读写和调试器读写
- 对于 PLib DCODE，只允许 DBUS 读取，禁止所有写入；禁止 IBUS 读写和调试器读写
- 默认为不开启 PLib（即设定区被擦除，出厂状态）。如果启用了 PLib 后，将 PLib 设定区擦除（回到关闭 PLib 状态），会先执行整片擦除，从而防止 PLib 泄露
- 非法读，将返回 0xFF
- 非法擦除、编程，将置位 PGERR，并产生 Hardfault

# 4 FLASH 划分

MCU 的片内 FLASH 划分如下：

| 地址 | 物理分配 | 逻辑分配 | | 说明 |
|---|---|---|---|---|
| | | 未启用 PLib | 启用 PLib | |
| 0x0800_0000 | MAIN | USER | USER | USER 空间受读保护位（加密位）控制 |
| | | | PLib ICODE | 启用后只执行 |
| | | | USER | |
| | | | PLib DCODE | 启用后只能数据方式读取 |
| | | | USER | |
| 0x1FFF_xxxx ~ 0x1FFF_F7FF | INFO | BOOT | | 出厂固化，用户不可擦写；读保护开启后仍可读 |
| 0x1FFF_F800 | | OB | | 通用选项字 |
| 0x1FFF_FC00 | | PLOB | | PLib 选项字 |

# 5 PLib 设定

PLib Option（选项区）的基地址位于 0x1FFF_FC00，根据不同型号，其大小为 0.5KB 或 1KB，为了程序的兼容性，建议仅使用 0.5KB。

PLib 选项区的组织结构如下：

PLib Option byte

| Address Offset | [31:24] | [23:16] | [15:8] | [7:0] |
|---|---|---|---|---|
| **0x000** | nPLDKEY | PLDKEY | nPLIKEY | PLIKEY |
| **0x004** | nPLib_IPST[15:8] | PLib_IPST[15:8] | nPLib_IPST[7:0] | PLib_IPST[7:0] |
| **0x008** | nPLib_IPEND[15:8] | PLib_IPEND[15:8] | nPLib_IPEND[7:0] | PLib_IPEND[7:0] |
| **0x00C** | nPLib_DPST[15:8] | PLib_DPST[15:8] | nPLib_DPST[7:0] | PLib_DPST[7:0] |
| **0x010** | nPLib_DPEND[15:8] | PLib_DPEND[15:8] | nPLib_DPEND[7:0] | PLib_DPEND[7:0] |
| **…** | | | | |
| **0x040 ~ END** | Copy Right info, eg:<br>Copy Right By FLASHCHIP!<br>PLib Function: BLDC Driver<br>PLib Version: 0.01<br>Public date: 2022/05/21 | | | |

PLib 选项说明：

| 选项字 | 说明 |
|---|---|

| | |
|---|---|
| **PLIKEY** | PLib ICODE 保护字，0xFF 或 0x00 = 不保护 |
| **PLDKEY** | PLib DCODE 保护字，0xFF 或 0x00 = 不保护 |
| **PLib_IPST[15:0]** | PLib ICODE Page Start，不能设为 0x00 |
| **PLib_IPEND[15:0]** | PLib ICODE Page End，不能设为 0x00 |
| **PLib_DPST[15:0]** | PLib DCODE Page Start，不能设为 0x00 |
| **PLib_DPEND[15:0]** | PLib DCODE Page End，不能设为 0x00 |

注：

1. n*为相应字段的反码，只有反码和原码互补，该选项字才装载。
2. 前 64 Byte 在写入时，由硬件处理反码；>64 Byte 的地址，在写入时，硬件不会自动插入反码
3. 未擦除前，不允许写入任何值。这样可防止版权信息被填全 0
4. KEY 不为 FF/00 且反码正确，则至少开启了版权保护，擦除版权信息时，会全片擦除
5. KEY 不为 FF/00 且反码正确，并且 Page Start/Page End 正确设置，则相应保护区开启
6. Page End >= Page Start 为有效设置，否则无效

# 6 PLib 状态

PLib 新增的寄存器位于 FLASH 控制器内，列表如下（所有位皆为只读）：

| Offset | Register | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **0x30** | FLASH_PLOBR | | | | | | | | | | | | | | PLDEN | PLIEN | PLERR |
| **0x34** | FLASH_PLIPST | PLIPST[15:0] | | | | | | | | | | | | | | | |
| **0x38** | FLASH_PLIPEND | PLIPEND[15:0] | | | | | | | | | | | | | | | |
| **0x3C** | FLASH_PLDPST | PLDPST[15:0] | | | | | | | | | | | | | | | |
| **0x40** | FLASH_PLDPEND | PLDPEND[15:0] | | | | | | | | | | | | | | | |

PLERR：PLib 选项字（0x000~0x010）非互反，该位置 1。

PLIEN：PLib ICODE 使能状态

PLDEN：PLib DCODE 使能状态

PLIPST：PLib ICODE 起始页

PLIPEND：PLib ICODE 结束页

PLDPST：PLib DCODE 起始页

PLDPEND：PLib DCODE 结束页

在 PLib 允许后，对 PLib ICODE/DCODE 进行擦除或写入，会产生 PGERR。

# 7 PLib 选项字的编程与生效

PLib 选项字的操作方式和 Option Byte 是一样的，只是其地址不同。在装载 Option Byte 时会一同装载 PLib 选项字。

**解锁 PLib（移除 PLib 保护）：**

1) 等待 FLASH->SR.BSY=0
2) unlock FLASH
3) unlock OPT
4) 置位 FLASH->CR.OPTER
5) 将 PLib Option 基地址 0x1FFF_FC00 写入 FAR
6) 置位 FLASH->CR.STRT，开始擦除（会先擦除整个 FLASH，再擦除 PLib Option）
7) 等等 FLASH->SR.BSY=0
8) 置位 FLASH->CR.OBL_LAUNCH，或复位 MCU，使 PLib Option 重新装载生效

上述步骤和擦除 Option Byte 基本一致，只多了第 5)步。

**启用 PLib（开启 PLib 保护）：**

1) 确保需要保护的指令和数据已经分别写入 PLib 的 ICODE、DCODE 区域
2) unclock FLASH
3) unlock OPT
4) 置位 FLASH->CR.OPTPG
5) 按 FLASH 编程操作方法，将 ICODE、DCODE 起始和结束的页地址分别写入 PLib Option 的相应地址
6) 按 FLASH 编程操作方法，将 0xFF/0x00 以外的值写入 PLib Option 的 PLIKEY 打开 ICODE 保护；将 0xFF/0x00 以外的值写入 PLib Option 的 PLDKEY 打开 DCODE 保护
7) 置位 FLASH->CR.OBL_LAUNCH，或复位 MCU，使 PLib Option 重新装载生效

**PLib ICODE、DCODE 开启保护后，只有解锁 PLib 才能将其擦除，其它任何方式（页擦除、整片擦除、去读保护、编程）均不能改写其内容。**

# 8 用户程序设定

# 9 版本历史

| Date | Revision | Author | Changes |
|---|---|---|---|
| 2022/6/6 | 0.10 | Dick Hou | 初版 |
| | | | |

# 10 -