# ArtInChip ArtHSM介绍

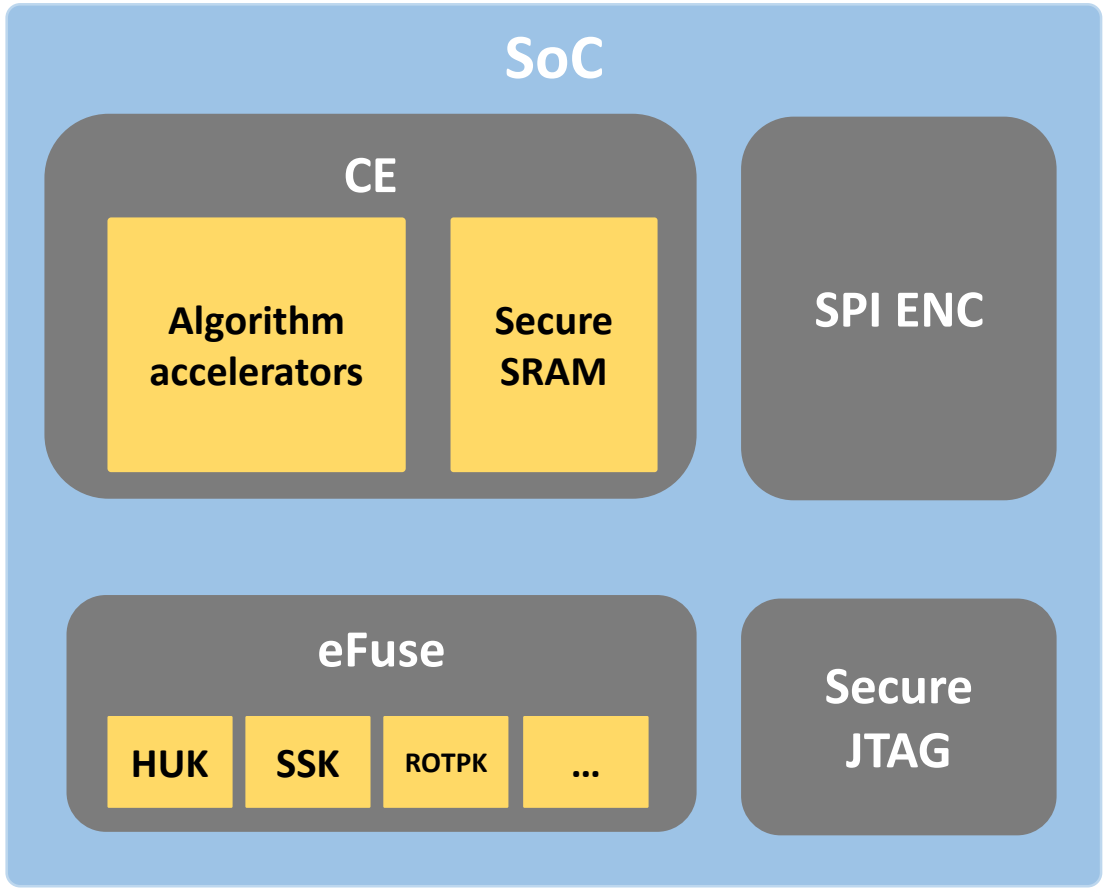
## “工业芯、匠芯创”

报告人：刘可亮

日期：2024-05-24

# ArtHSM 的安全硬件






**CE:**

- Crypto Engine
- 加密引擎

**SPI ENC**

- SPI 总线在线数据加密

**eFuse**

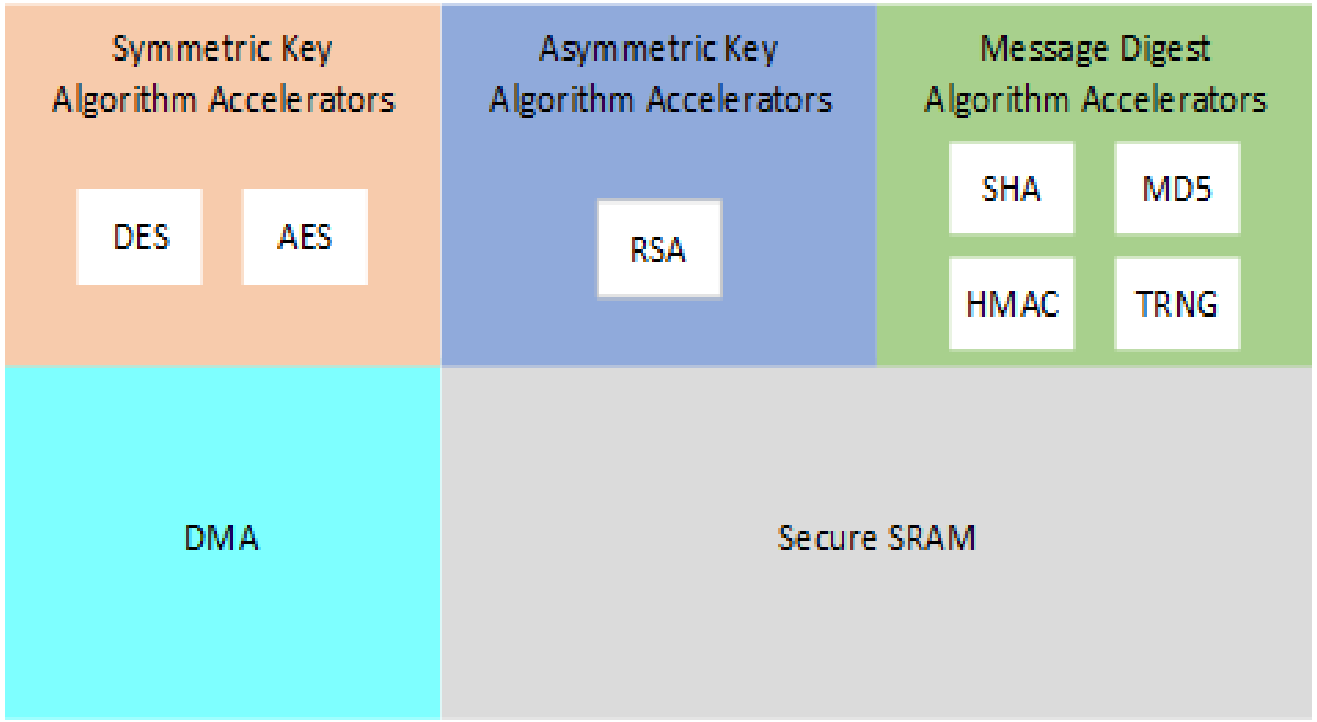
- 一次性熔断性编程模块

**Secure JTAG**

- 可安全开关的调试端口

# 模块 – Crypto Engine






- ✓ 文档章节：
  - 芯片手册：6.1
  - SDK： 8.3
- ✓ 独立的硬件模块
- ✓ 支持多路并行处理
- ✓ 对称，非对称，信息摘要等多种算法
- ✓ 内部独立DMA
- ✓ 专用Secure SRAM

# 模块 – eFuse

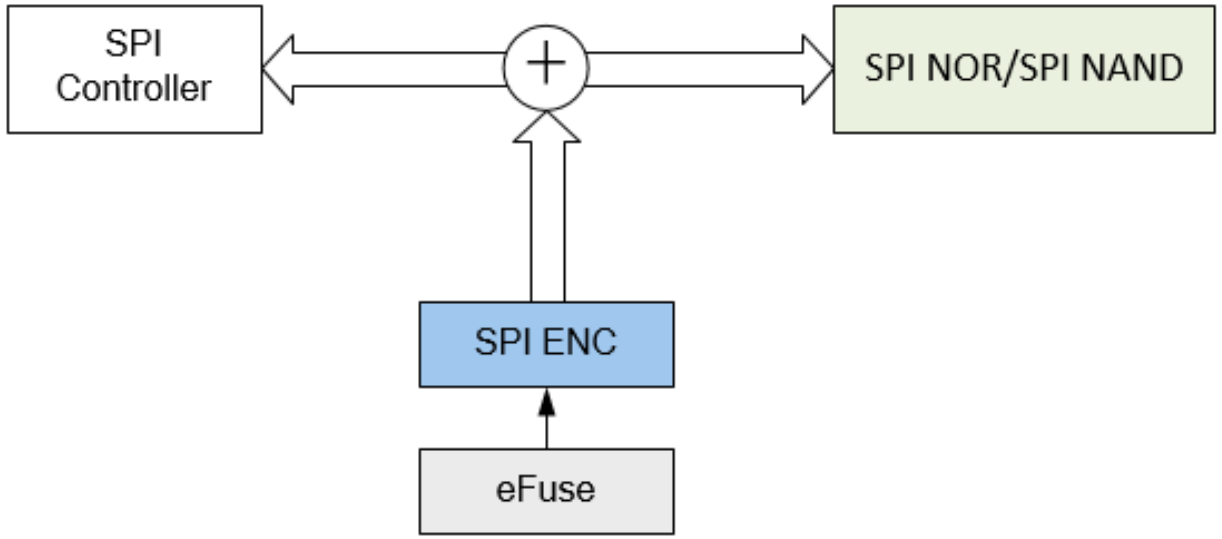


| 用途 | 位数 | 归属 | 备注 |
|---|---|---|---|
| CHIP ID | 128 | AIC | 芯片编号 |
| BROM | 64 | CSTM | BROM参数配置区域 |
| ROTPK | 128 | CSTM | 安全，RSA公钥的MD5 Hash值 |
| HUK | 128 | CSTM | 安全，连接到CE，硬件唯一密钥 |
| PSK0 | 64 | CSTM | 安全，合作伙伴密钥，4组 |
| SPI Key | 128 | CSTM | 安全，SPI ENC 对称密钥 |
| Reserved | 512 | CSTM | OEM可自定义使用 |

- ✓ **文档章节：**
  - **芯片手册：6.3**
  - **SDK：8.1**
- ✓ **CHIPID 接口：getChipID**
- ✓ **512Bit用户可用**
- ✓ **安全存储，对用户透明**

# 模块 – SPI-ENC

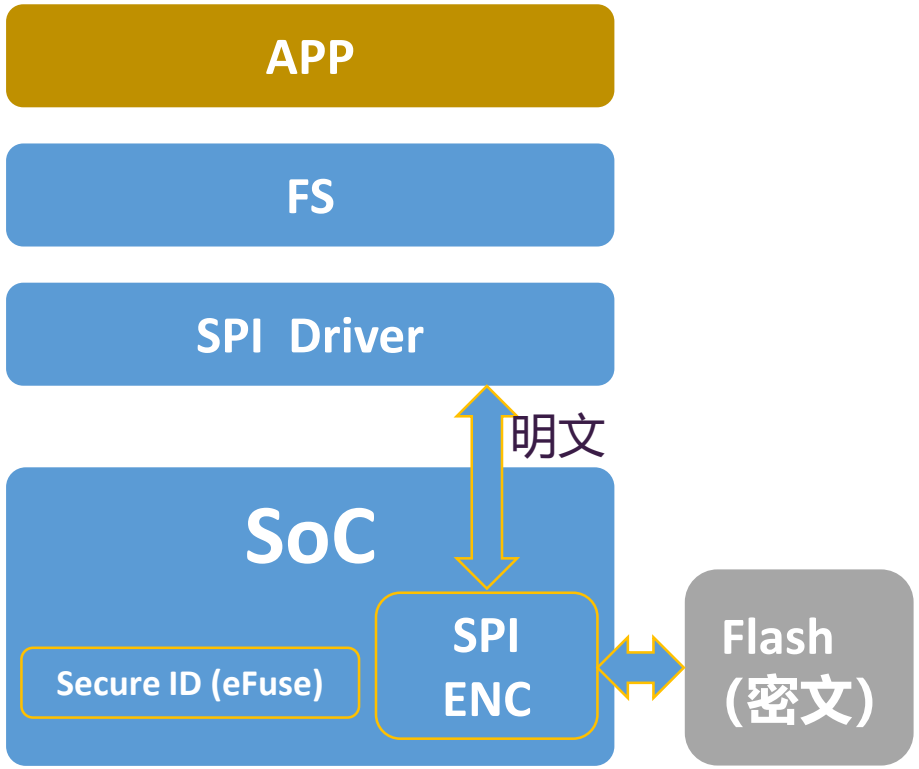





- ✓ 文档章节：
  - 芯片手册：6.2
  - SDK：8.2
- ✓ 对CPU透明的SPI数据加密方案
- ✓ SPI0,SPI1可以用
- ✓ 无额外CPU资源消耗
- ✓ 不影响SPI总线传输带宽

# 方案 – SPI-ENC

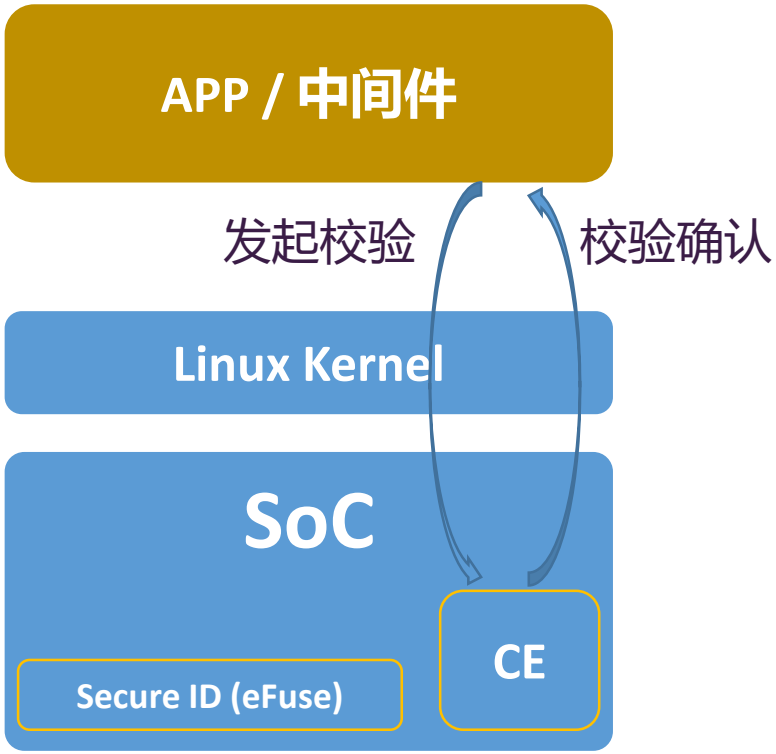





- ✓硬件级在线加密，应用无感知
- ✓ Flash读写性能无影响
- ✓支持烧写器批量烧写
- ✓eFuse需要写入SPI KEY
- ✓串口等外设要处理

# 方案 – CE+HUK

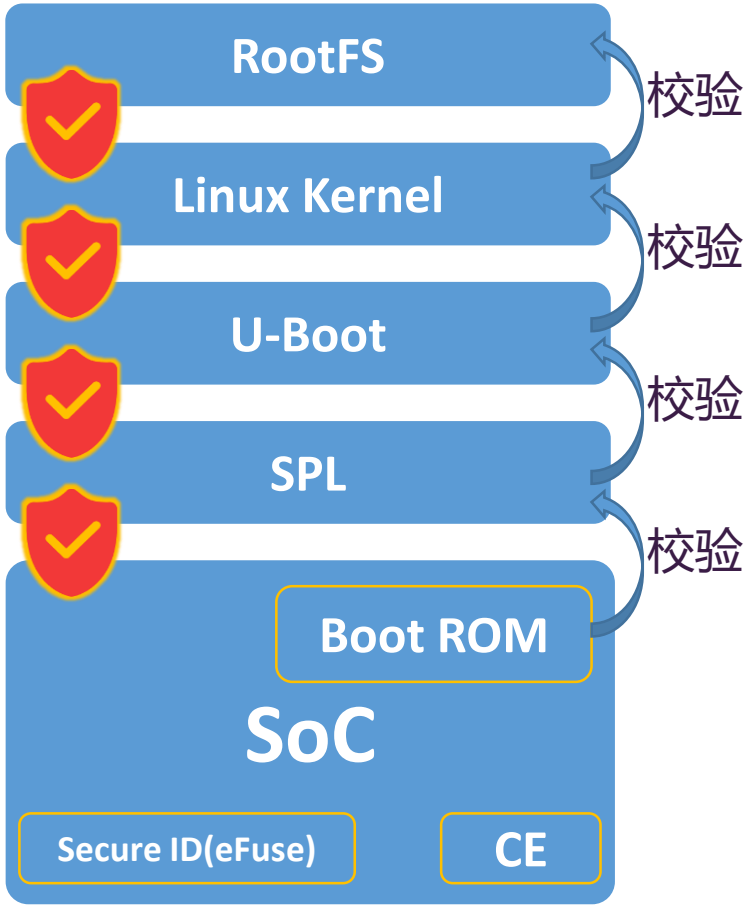





- ✓ 自由度高，可自由选择合适算法
- ✓ 可使用自带HUK，不用额外写入KEY
- ✓ 可生成和管理 自有PSK
- ✓ SDK自带openssl 硬件引擎
- ✓ 额外开发加解密逻辑

# 方案 – 安全启动

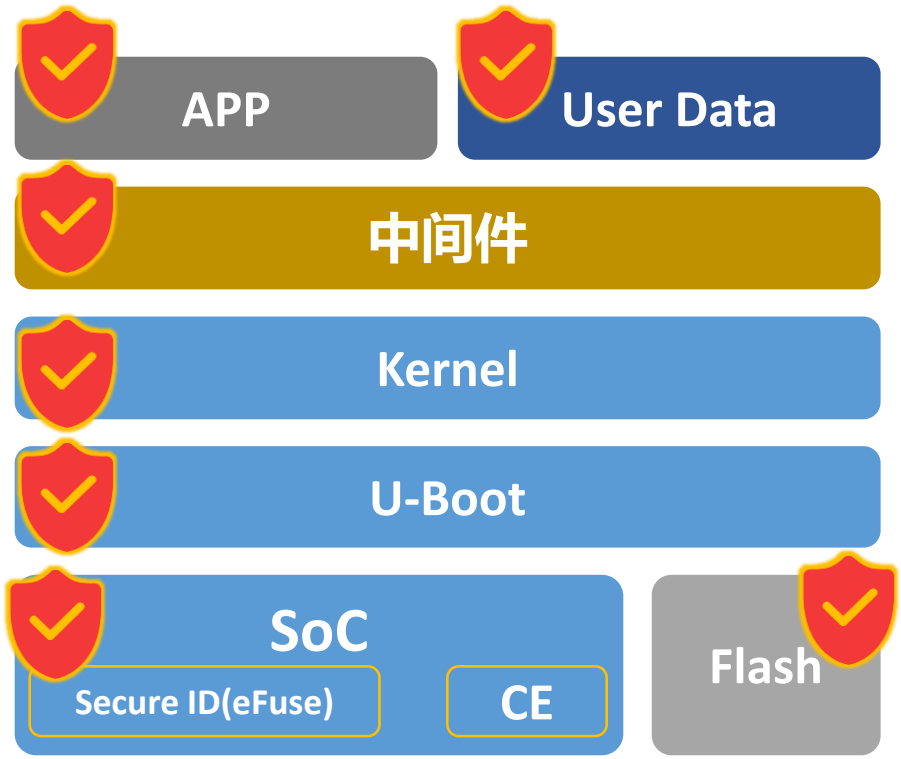





- ✓逐级校验，一种更彻底的解决方案
- ✓ 启动时校验，运行时无影响
- ✓固件加密，支持烧写器烧录
- ✓eFuse需要写入PSK
- ✓串口等外设要处理

# 应用场景及解决方案






| | 保护对象 | 相关技术方案 |
|---|---|---|
| **固件安全** | 固件防破解，篡改 | 安全启动 |
| | 固件防拷贝 | SPI-ENC |
| | | 安全启动（bootloader） |
| **版权安全** | 中间件、APP的版权 | CE + HUK |
| | | SPI-ENC |
| **数据安全** | 用户数据 | CE + HUK |
| | | SPI-ENC |
| **信息采集** | 数据统计 | CHIPID |

# 让使用更简单

Sincere Cooperation For A Win-win Situation

13726219952 | Jun.chen@artinchip.com

Luban-lite 技术交流群