航芯方案分享 | 智能设备防盗版解决方案

随着科技的进步与发展，身边的电子设备变得日趋智能，这些智能设备在使得人们工作与生活变得便捷的同时，产品的版权及安全性正受到威胁。为了维护设备制造商的利益和品牌价值，也为了保护消费者使用产品的质量和服务保障，智能设备的安全和防伪将变得十分重要，保护它也就是保护了自身的安全。

上海航芯智能设备防盗版解决方案采用金融级安全芯片 ACL16_S，支持多种对称、非对称、散列等密码算法，可以广泛适用于智能家居、汽车电子、医疗设备、电子烟耗材等领域。

方案特点

· 采用金融级安全芯片 ACL16_S，安全性更高

· 单芯片方案，无需外围器件，带来更低的 BOM 成本

· 每个设备采用一机一密的方式，Wafer 级根密钥预置，从源头进行密钥保护

· 支持 SPI、UART、I2C、ISO7816、SWI 单线等多种通信接口，便于与多种系统主机进行集成

· 丰富的软件库配套，易于多种平台系统集成

· 小尺寸封装支持，便于 PCB 板的硬件集成

· 支持多种低功耗模式，满足电池智能设备的续航要求

典型应用

· 硬件电路防抄板

· 原厂配件认证（电池、数据线）

· IoT 设备防伪

· 电源适配器

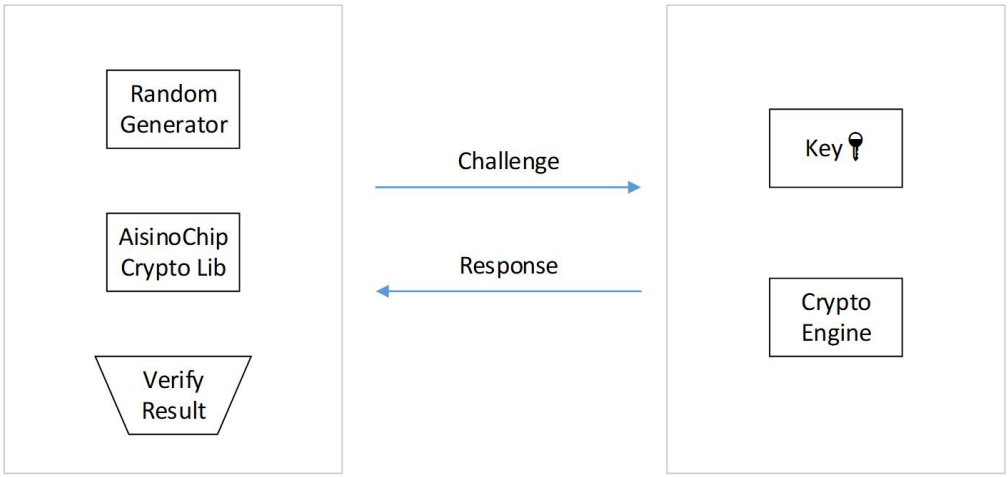
· 汽车电子

· 智能家居

· 软件 IP 保护

· License 管理

方案框图



Host：可以是系统板上的主芯片，也可以是云端的后台服务器。

Device：可以是航芯的安全芯片，也可以是嵌入航芯安全芯片的设备。

支持不同认证方式的安全芯片

	ACL16_S CSx	ACL16_S DSx	特点
HMAC 认证	●	●	对称密钥认证 认证速度快
ECDSA 认证	●	—	ECC 非对称密钥认证 认证强度高
封装	SOP8，QFN8	SOP8，QFN8	

芯片特性

· 支持 1.8V-3.3V 电压供电

· 支持 ECC 椭圆曲线算法，支持 NIST B-163 曲线和 P256 曲线

· 支持 HMAC 认证，支持 SHA-256 散列算法

· 支持 SPI、UART、I2C、ISO7816、SWI 单线等多种通信接口

· 支持客户敏感代码执行

· 支持 TSSOP8、DFN8、SOT23、WLCSP 等多种封装规格

· 动态功耗小于 3mA，待机功耗小于 1uA

安全特性

· 金融级安全芯片，符合 EAL5+安全级别

· 128 位唯一序列号

· 主动屏蔽层

· 环境异常检测模块

· 防 SPA/DPA 攻击

· 防错误注入攻击

了解更多航芯产品&方案：www.aisinochip.com