PUFsecurity

PUFcc – Crypto Coprocessor

Datasheet

April 2022

产品说明

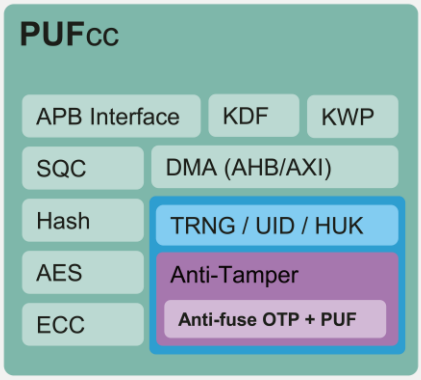
PUFcc 是一种新颖的高安全性加密协同处理器。与传统的安全 SoC 设计（具有安全核心或分立加密组件的嵌入式 HSM）相比，PUFcc 可以帮助客户更轻松地采用硬件信任根 (HRoT)，有效防止安全漏洞，在不占用处理器核心或操作系统之效能的优点下，快速提高系统的安全级别。

PUFcc 的安全边界是基于硬件物理隔离，没有纯软体安全设计的弱点，因此非常可靠。PUF 是天生自带保护能力的静态熵源，适合 SoC 架构师将其应用在密钥生成和管理程序来构建系统的密钥层次结构。此外，PUFcc 的加密引擎可以执行各种安全操作，例如密钥交换、安全启动或 TLS （公共密钥验证和签名）、身份验证（MAC）或密钥包装（同样基于 PUF 天生的随机性），并将所述包装的密钥存储到外部内存。

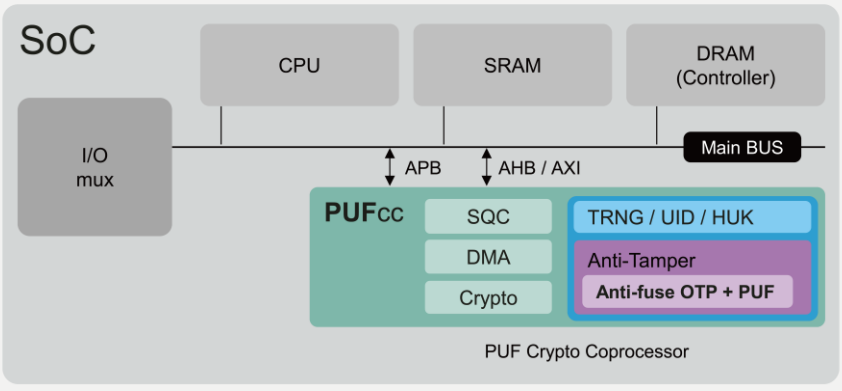
产品特征

- 加密引擎集合，由私钥密码、信息验证码、哈希加密引擎和密钥派生功能组成，经 NIST CAVP 认证并符合 OSCCA 标准
- 钥匙包装功能，有助于输出钥匙供外部使用
- 公钥协处理器，支持所有椭圆曲线加密算法功能
- 四组 256 bits PUF 指纹，具有自我检测功能，可作为唯一的身份识别（UID）或信任根密钥使用
- 标配 8k-bit OTP 搭配即时硬件加密
- OTP 存储空间大小可定制
- 物理布局搭配 RTL 的全面防篡改设计
- 高质量的真随机数生成器
- 具有安全/非安全访问权限的 APB 控制接口
- 用于直接内存访问(DMA)的 AXI/AHB 接口

Crypto Coprocessor



Suggested Integration



交付项目

- 数据手册
- 发行说明
- 整合指引
- Timing .lib 文件
- LEF
- GDS Phantom 文件
- 仿真环境和基于 PUF 的硬核行为模型
- RTL：附带整合说明
- 应用说明（内存映射寄存器/FW/API）
- FW/API 参考编码
- 硬核发行说明
- 测试方法
- 测试平台

详细内容

制程可用性

- 已扩展至 6 奈米，并持续开发
- 可在全球各大代工厂量产

安全性特点

- 已通过 Riscure 认证
- 能抵御物理攻击，包括解封装、显微镜成像、探测、反向工程等

控制器/接口

- 标准 APB 控制接口
- 安全 OTP 访问控制（工厂测试、一般使用者、可读/写、只读和不可访问模式）
- 適用不同 SoC 系統架構的直接內存存取接口(AXI/AHB)

PUF-based 安全密钥存储

- 内建 8k-bit OTP; 容量可定制
- 随机扰乱数据输出时间点
- 透过与 PUF 值混成加密使密钥无法被直接读出，确保密钥存储的安全
- 每一芯片有独立个别的扰码值将各芯片存储的信息打乱
- 内部存储的值无法更改和删除

PUF-based 真随机数生成器（TRNG）

- 极速的初始化/就绪时间（<100ms）
- 高速吞吐量（超过 160 Mbits /秒）
- 极小功耗（低于 0.38 pJ /bit）
- 符合 NIST SP800-22 和 NIST SP800-90B 的 IID/重启测试标准
- 可选用符合 NIST SP800-90A 的 DRBG、可产生超过 1Gb/s 的随机数

PUF-based 唯一 ID （UID）

- 提供理想的最小熵（1）
- 不可预测的随机性和唯一性（50%汉明权重和汉明距离）
- 供芯片本身或外部 ID生成所需的天生密钥
- 终生零误码率的高可靠性
- 在不同环境下运作的高稳定性（温度：-40～175° C）

密钥派生功能引擎（KDF）

- KBKDF (CTR/FB)
- PBKDF

密钥包装加密引擎（KWP）

- 遵循 NIST SP800-38F 附录规范的关键包装引擎

公钥协处理器（PKC）

- NIST 标准的椭圆曲线
- ECDSA/ECDH/RSA
- SM2

消息认证代码引擎（MAC）

- CMAC/HMAC/CBCMAC/GHASH
- POLY1305

私钥密码学

- 支持 NIST SP800-SP38A/B/C/D/E
- 密码：AES128/192/256
- ChaCha20
- SM4
- 支持 ECB/CBC/CTR/CCM/GCM/XTS 模式

安全哈希功能

- SHA224/256/384/512
- SHA512_224/256
- SM3

软件

- 包括固件、API 和 Mbed-TLS 驱动

全面的防篡改设计

对于侵入式攻击

- 物理性隔离
- 数据加扰和改组
- 抵御电压对比攻击

对于半侵入式攻击

- 金属屏蔽
- 安全的 IP 布局
- 模拟电路保护
- 接口保护
- 输出数据检测

对于非侵入式攻击

- 地址/模式引脚和数据上的引脚保护
- 访问控制和自毁机制
- 统一电源设计
- 电源浮动检测
- 内置安全修复机制
- 能抵抗恶意入侵的 UID 和密钥存储的屏蔽保护

PUFsecurity Corporation

8F, No. 5, Tai-Yuan 1st St., Jhubei City,
Hsinchu County, 302082, Taiwan
Tel: +886-3-560-1168

Please visit our website for further information or to download and try our IPs

https://www.pufsecurity.com/ip-go