PUFsecurity

PUFrt - Hardware Root of Trust

Datasheet

April 2022

产品说明

PUFrt 是集成了所有建立信任基础所需的关键元素的硬件信任根 (HRoT)解决方案，所有安全操作（例如安全启动）都可以基于此信任根去建立。

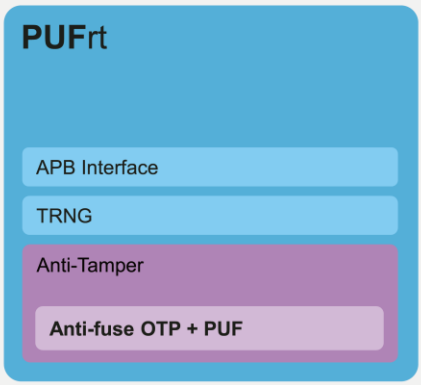
本 IP 经过 Riscure 认证并兼顾灵活性，方便客户自由添加设计所需的加密引擎，并配备了精心设计的防篡改设计来抵御各种攻击。PUFrt 可以集成到各种系统中作为基本的硬件安全信任根模块扩充到具备完整进阶功能的安全协同处理器。

PUFrt 为芯片系统提供了一个信任和安全的基础。 PUFrt 内置物理不可复制功能（PUF）来生成 1024 bits 的静态随机数，并有符合 NIST SP800-90B/SP-800-22 规范的真随机数生成器（TRNG）来生成动态随机数。可满足敏感信息和数据的加密/解密需求，并达到高水平的安全强度。此外，PUFr 也提供由 PUF 所保护的 8k-bit 安全存储空间(NeoFuse OTP)，以利保存客户的密钥或敏感信息，这使得 OTP 本身和整体系统的安全性更能抵抗物理攻击。

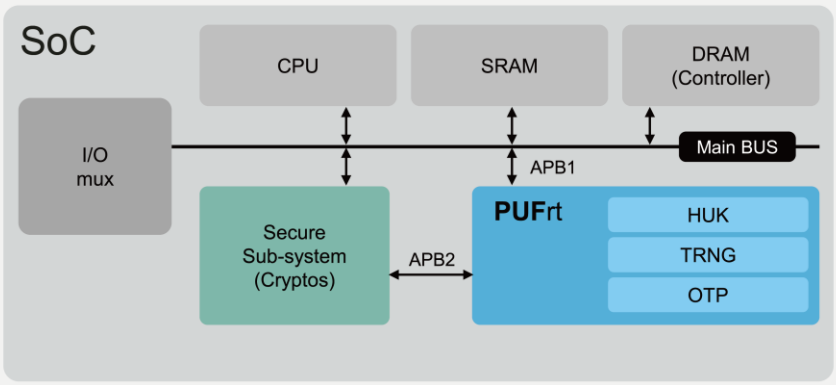
产品特征

- 四组 256-bit 的 PUF 硬件指纹，具有自我检测功能，可作为唯一的私钥、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
- 内建 PUF 健康度检测机制

Root of Trust



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
- Verilog HDL 文件（行为模型）
- Verilog HDL 文件 （FPGA）
- 应用说明
- 参考编码脚本
- 硬核发行说明
- 测试方法
- 测试平台

详细内容

制程开发进展

- 已扩展至 6 奈米，并持续开发
- 可在全球各代工厂使用

安全性保证

- 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 封装（工厂测试、一般使用者、可读/写、只读和不可访问模式）

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）

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