PUFsecurity

Secure OTP- Tamperpoof storage

Datasheet

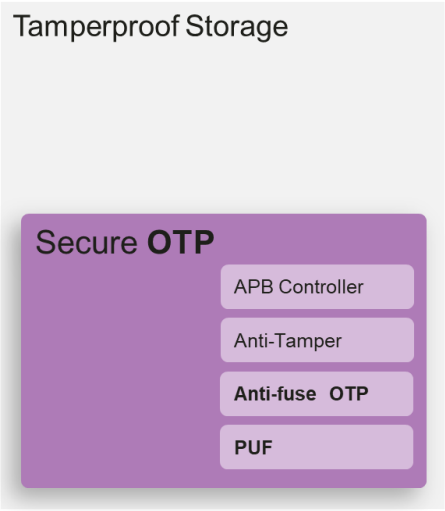
June 2022

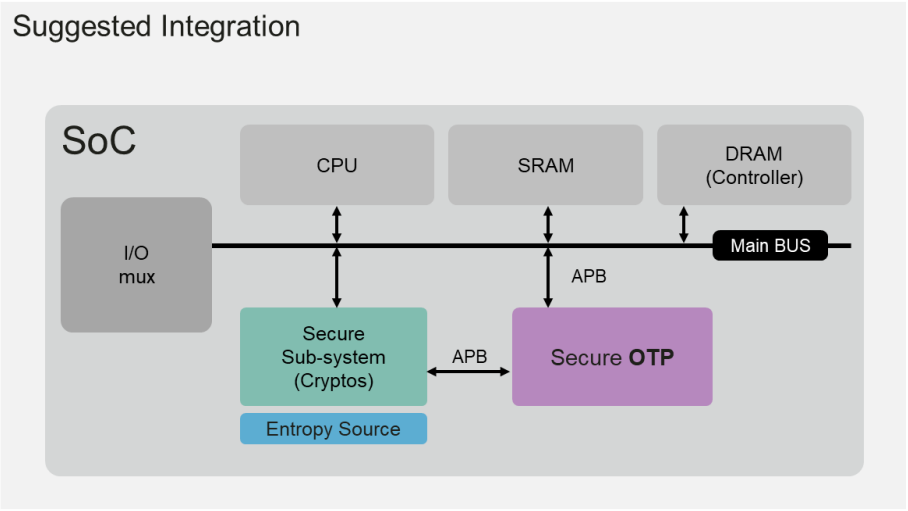
产品说明

在安全风险不断上升的压力下，物联网设备的发展潜力难免受限。而解决此问题的答案，便是创建一个完整的安全生态系统。从最安全的硬件、软件和操作系统解决方案中汲取所需，而 Secure OTP 可以成为任何芯片安全生态系统的基石，保护根密钥和启动代码等关键数据。

熵码科技开发的 Secure OTP 是一个整合了硬件核和数字 RTL 的 IP，旨在为静态数据提供安全保护。在硬件方面，Secure OTP 包括一个 1024 位的物理不可复制功能（PUF），用于物理地址扰乱和 I/O 混肴，以提高存储数据的安全性。该 PUF 属于纯硬件，能创造近乎理想的熵，不需任何辅助数据进行校正，且允许系统在几微秒内访问数据。RTL 部分则包括 OTP/PUF 控制器的胶合逻辑、防篡改功能和标准的 AMBA 接口。熵码 Secure OTP 的贴心设计不仅可随客户需求进行定制，将其功能效率极大化，更有利于工程师加速集成 Secure OTP 至各式 IC/ASIC 应用中。目前熵码 Secure OTP 有多种密度和配置可供选择，并已在各种 CMOS 技术上实现，为市场提供出色、可靠的嵌入式非易失性存储器的终极解决方案。

熵码科技在技术平台方面也具有相对的优势。通过母公司力旺电子，我们汲取了 20 多年与代工厂合作并提供高质量 IP 的经验，使我们的客户得以透过全球各大代工厂相对应的技术平台取得我们的 Secure OTP。





产品特征

- 内置即时硬件加密设计、上至 128kb 的量产 OTP（可定制）
- 结合硬件和 RTL 的全面防篡改设计
- 具有安全/非安全访问权限的 APB 控制接口
- 四组 256 位硬件 PUF 指纹，用于加扰安全 OTP 存储
- 完善的权限控管、归零和锁定机制，以加强产品生命周期的管理和保护
- 固件和 API 的软件套组

交付项目

- 数据手册
- 整合指引
- 应用说明
- 测试方法
- Verilog HDL 文件（行为模型）
- Verilog HDL 文件（FPGA）
- Hard Macro GDS
- 参考编码脚本
- 参考 FW/API

详细内容

制程开发进展

- 已实现至 5 纳米工艺，并持续发展
- 可於全球各代工厂取得

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 安全存储

- 上至 128kb 的量产 OTP; 容量可定制
- 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

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