RISC-V 晶片設計不可或缺的安全協同處理器

PUFsecurity

White Paper

August 2021

Authors:
Sam Chung,
Sean H. Wu,
Evans Yang

前言

连网应用带动了大量连网装置需求与信息流需求。根据 Juniper Research 的最新报告，IoT 连网设备将在 2021 年达到 460 亿个，并在 2030 年达到 1250 亿个。要有效执行连网应用功能与处理大量数据与信息流，每个装置都需要处理器核心，而在此庞大市场商机之下，开放指令、低成本 RISC-V 架构提供了芯片设计者在 X86 及 ARM 之外的另一个新选择。

大量的连网装置与信息流也给攻击者更多的攻击机会。连网应用安全越来越受到重视，如何有效执行装置身份认证、确保信息传输与数据储存的安全成为连网装置必要的安全功能。RISC-V 在安全功能方面的规范仍在持续发展制定中，如何提供 RISC-V 芯片设计者容易使用、有效的安全解决方案去强化芯片安全功能并提升应用安全成为新兴课题。

实现物联网应用安全功能，系统芯片需要的设计考虑

一般而言，在考虑系统芯片安全设计时，需考虑几个要件，包括：

1. 可信任执行环境 (TEE)：透过硬件强制隔离程序代码、数据和储存内存
2. 信任根 (Root of Trust)：作为唯一 ID 和证书，以及私钥和安全保存
3. 安全启动 (Secure Boot)：阻止非授权认证程序的启动
4. 数据储存安全：取用控制权限管理、并对数据读取与储存进行混淆与加密
5. 信息传输安全：信息传输前以私钥加密，以密文形式传输
6. 在线安全更新：更新档案以加密形式传送并阻挡失效版本的安装

要达到这些功能设计，芯片设计架构中除了 CPU 外，通常还需要密钥储存单元搭配各种密码算法来协助 CPU 执行应用服务所需的相关安全功能，如认证、数据加解密、完整性确认等功能。同时需要有独立的安全运作环境或可信任的执行环境来有效区隔安全功能与一般非关安全功能的运作，以及抗攻击设计来避免执行安全运作时遭受攻击。

因此，要有效防止恶意攻击、提升芯片运作的安全性，有经验的设计工程师会采用具备硬件安全信任根以及抗攻击设计的安全协同处理器 (secure co-processor) 来协助 CPU 执行应用服务所需的各项安全功能。

硬件加速的安全协同处理器不会占用到主 CPU 的运算能力，可高效的执行上述安全相关的功能，让宝贵的 CPU 运算资源去处理其他需高效能运算的工作。机密信息只经由被信任的安全协同处理器来处理，更加符合安全原则。这种功能上的分离简化了设计流程与复杂度并且提高了系统性能。

安全协同处理器常见的问题

当前市场上可分为两大处理器应用体系，分别是 ARM 和 RISC-V。在 ARM 应用体系中，ARM 提供了 CC312 与其 CPU 整合的安全协同处理器进行各项安全运算；RISC-V 生态系则尚在发展中，目前没有对应的安全协同处理器，因此 RISC-V 的使用者需自行开发设计或使用第三方 IP 来完成前段所提的安全功能。若要自行开发，是否有适合的安全开发团队与能力是公司马上面临的一大课题，接踵而来的如上市时程压力、所开发的安全功能是否能通过认证机构认证、遭遇技术问题时的解决能力、以及所对应的投资成本等，都是 RISC-V 使用者在决定是否自行开发前需要仔细考虑的。相对来说，如果有良好第三方能提供安全协同处理器 IP，就可大幅减少以上这些自行开发的难题。

目前市场上的安全协同处理器多半缺少硬件信任根的整合，没有完整安全边界 (secure boundary)，功能也不够全面。譬如有的协同处理器是硬件加解密算法不够完整，或没有抗攻击能力，或没有通过第三方认证单位的安全认证；而有些是不提供安全密钥存储空间，造成安全协同处理器执行安全功能时需跨越安全边界取得密钥(想象一下您把家里金库上锁后将钥匙放在大门外的概念)；又或是虽有存储空间，然芯片的密钥、身分必须在测试过程时一一写入芯片内，造成密钥暴露外泄的风险；或是所有产品共享相同密钥、身分造成装置与应用服务管理的安全风险。

以上种种的不足，都有可能成为 IoT 设备最后的安全漏洞，被黑客利用做为重大攻击的跳板。因此，即便是小小的 IoT 设备，传输的是一般不起眼的寻常数据，一旦设备出现安全隐忧，遭黑客利用攻击之后，都可能造成巨大的损失。类似的事件层出不穷，相对知名的如 2021 年五月份，美国最大的油管运输公司(Colonial Pipeline)遭黑客攻击，造成油管供应关闭，政府一度发布紧急状态，最终支付了将近 500 万美元赎金。

熵码 PUFcc 帮助 RISC-V 实现更安全的芯片架构

针对 RISC-V 生态系中安全协同处理器不够完善且完整的情况，熵码科技提出的方案 PUFcc 就是完整解决各项安全问题的最佳选择。

PUFcc 完整的防护设计来自于多层次的设计架构，有别于纯软件安全设计的弱点，PUFcc 是基于硬件的物理隔离所设计，提供了可靠的安全边界，为系统创造了完整的可信任执行环境 (TEE)。

图 1 是 PUFcc 的设计架构，它的最底层是以模拟电路设计的硬件安全信任根(蓝色区域)。在此硬件安全信任根设计中应用了力旺电子专利技术的 NeoPUF，提供每颗芯片独一无二的芯片指纹(UID)，并由经过 Riscure 认证的抗攻击安全存储 OTP 来存放密钥，保护重要数据免受物理篡改。

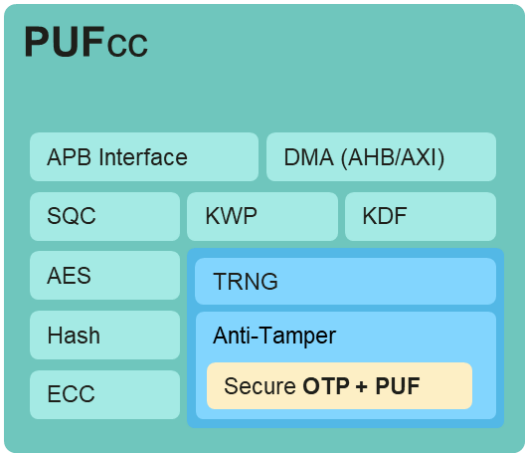

图 1: 基于芯片指纹防护信任根的 PUFcc 安全协同处理器设计架构

在硬件安全信任根之上，搭配了高速真随机数产生器(TRNG)来提供安全系统对动态随机数的需求并用于保护加密算法引擎。搭配着基于 NIST 发布的标准密钥包装(KWP)和密钥产生(KDF)功能，专门用于密钥的安全使用与安全导出，可以为 RISC-V 系统架构之物理内存保护(PMP)功能快速生成多把密钥，供不同安全应用之内存的加解密程序所用，确保信息传输的安全。

此 PUF 的特性可以在装置上实现安全启动以及在线安全更新功能，也就是同一个软件在不同的 IoT 设备上都有一把独立的加密密钥——真正实现数百亿甚至千亿个 IoT 设备连网的坚若盘石之安全基础。

PUFcc 支持完整硬件加解密算法(包含国际算法及中国国密算法)，分别经过 CAVP 以及国密实验室认证。透过完整灵活的算法模块化设计，可以根据每个使用者的需求客制 PUFcc 的加解密算法模块。例如，使用 SM4 替换 AES，使其可以完整支持目前甚至是未来 RISC-V 的安全需求。

最后，在以上安全功能面之外，PUFcc 在数字与模拟设计上皆加入了防窜改设计来提供使用者完善的安全协同处理器架构。不仅如此，为了降低芯片在系统层级的复杂度，PUFcc 支持 APB 标准协议接口，用于 PUFcc 寄存器命令处理；至于高速内置 DMA 模块的接口，则采用 AXI4 接口，可快速取得储存于系统内存中的大量数据。除硬件 IP 外，PUFcc 还提供标准的软件内容，包括 Linux bare-metal firmware 和 high-level API，以缩短软件开发部署时程。

PUFcc 与 RISC-V 结合之优势

PUFcc 可搭配 RISC-V 处理器，扮演 RISC-V 系统芯片架构内的安全协同处理器，提升芯片系统运作安全性，补足 RISC-V 设计生态系的安全解决方案缺口。经过实际设计验证，PUFcc 藉由提供芯片指纹抗攻击保护设计来强化芯片硬件信任根与密钥储存。完整保护系统运作的安全边界，提供可信任安全环境、安全启动以及数据储存安全等功能，同时支持各种硬件加解密算法，且又能提供不同内存区域不同密钥的 PMP 保护与管理机制，实现 IoT 连网装置应用不可或缺的信息传输安全与在线安全更新。采用 PUFcc 的 RISC-V 系统芯片设计架构如图 2 所示。

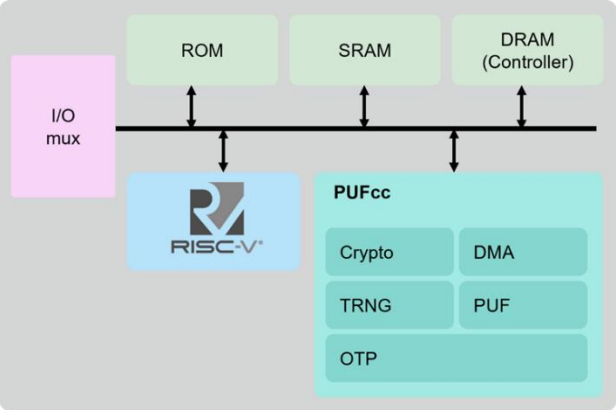

图 2: 使用 PUFcc 的 RISC-V 系统芯片设计架构

为实现物联网应用安全，熵码科技以芯片指纹技术为基础强化芯片信任根的安全，开发出具完整安全边界保护的安全协同处理器 PUFcc，可以为 RISC-V 使用者提供了一个可快速导入的芯片安全设计解决方案，帮助实现 IoT 连网应用所需的大量组件装置零接触部署(Zero Touch Deployment)，PUFcc 提供的各种硬件加速安全功能与管理机制可以满足零信任运作(Zero Trust)的云端应用安全需求，适合应用于 IoT 设备生态的 RISC-V 处理器最完美配合之安全方案。

PUFcc IP 评估套件免费下载请至: https://www.pufsecurity.com/ip-go

PUFsecurity

8F, No. 5, Tai-Yuan 1st St.,
Jhubei City, Hsinchu County,
302082, Taiwan

Tel: +886-3-560-1010
www.pufsecurity.com