PUF security

熵码科技 执行副总 杨青松

芯片指纹：实现更安全的芯片应用与服务

大纲

- 芯片指纹技术简介
- 零信任的安全服务与需求
- 如何使用RISC-V实践安全系统单芯片?
- 如何利用芯片指纹确保供应链安全?
- 结论

PUF security

熵码携手力旺切入芯片安全市场

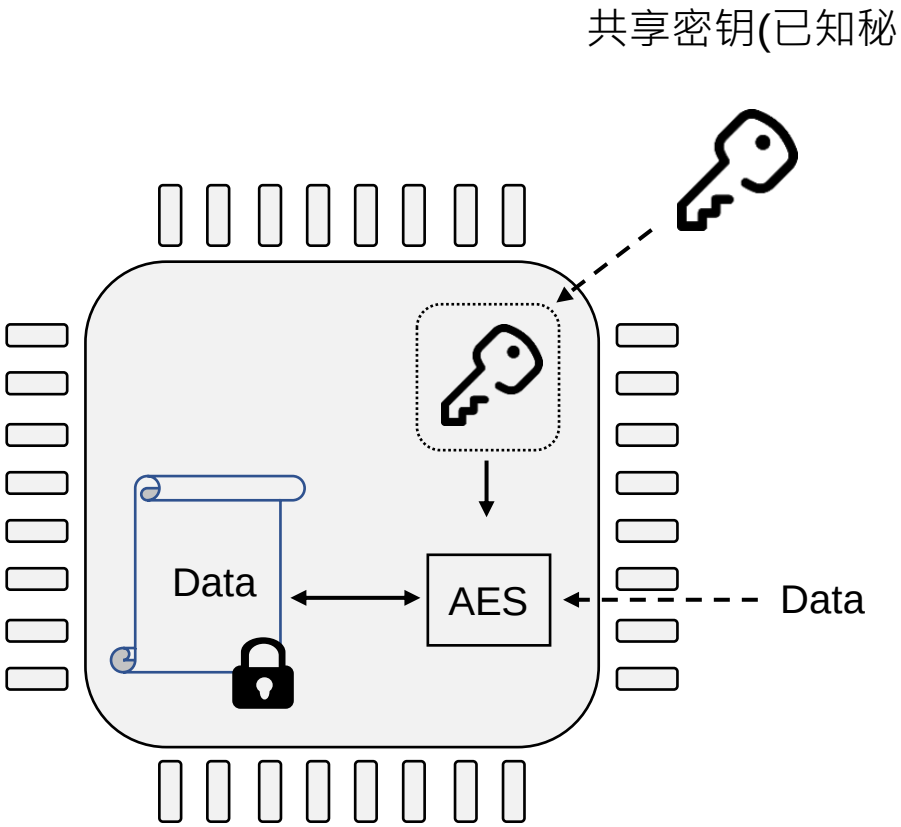
共同推广与开发...

...建立OTP PUF技术平台

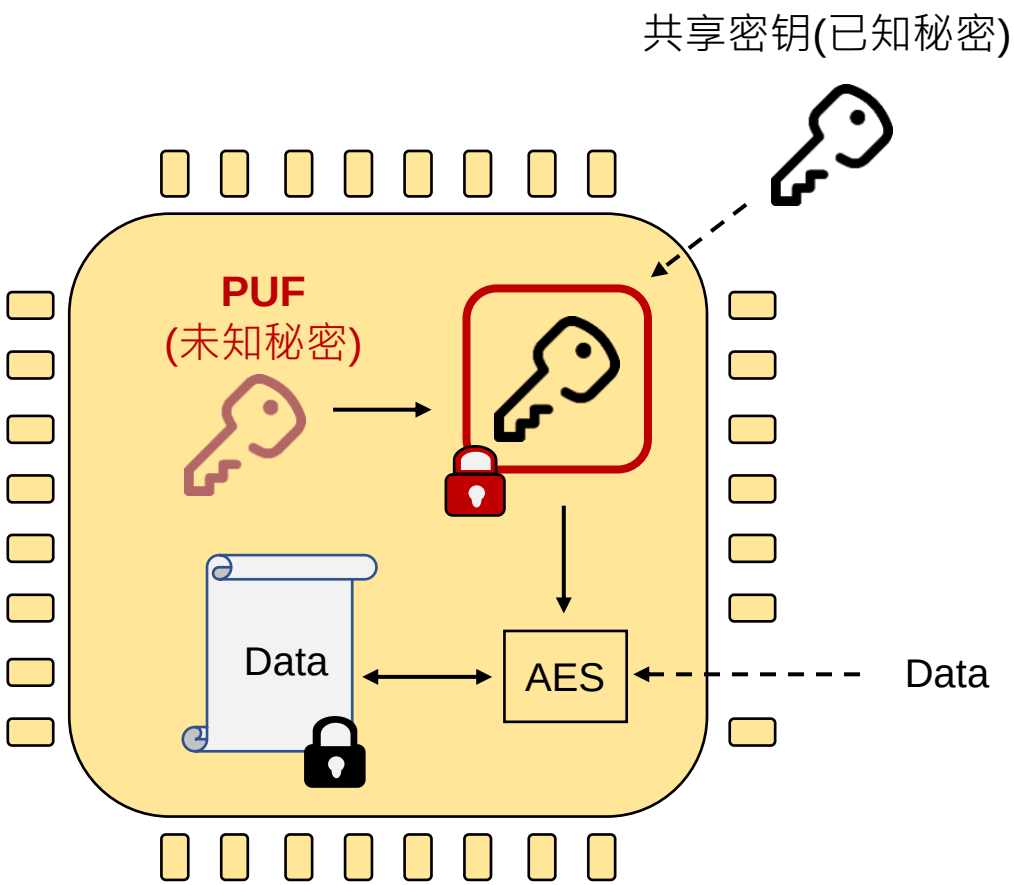
熵码科技结合力旺PUF与OTP技术，发展客制化芯片系统安全解决方案与应用服务的硅智财，为力旺电子的子公司

力旺电子为全球最大的逻辑制程非挥发性内存(Logic-Based Non-Volatile Memory, Logic NVM)与芯片安全技术开发及硅智财供货商

用未知秘密来保护已知秘密



如何保护密钥?



以**PUF** (未知秘密) 保护密钥(已知秘密)

核心技术-以芯片指纹保护的硬件信任根

密钥在安全运作当中属于已知的秘密 (common-known secret)

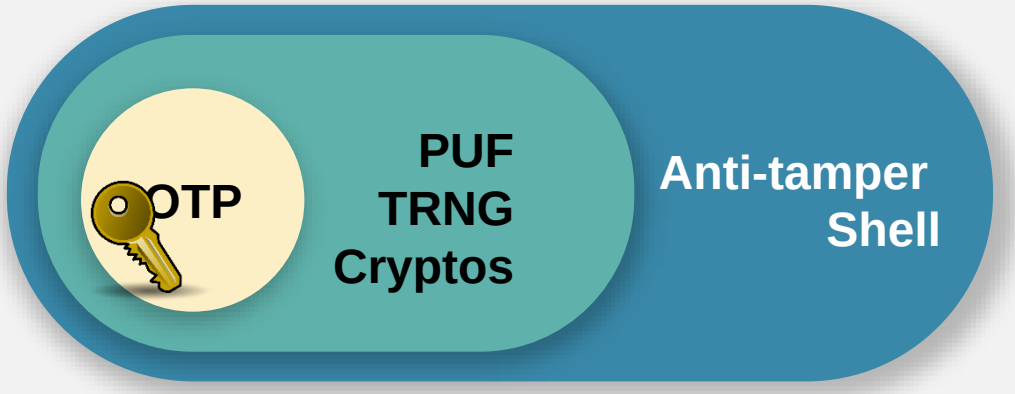
PUF是从芯片原生的指纹，属于未知的秘密 (private-unknown secret)

PUFrt

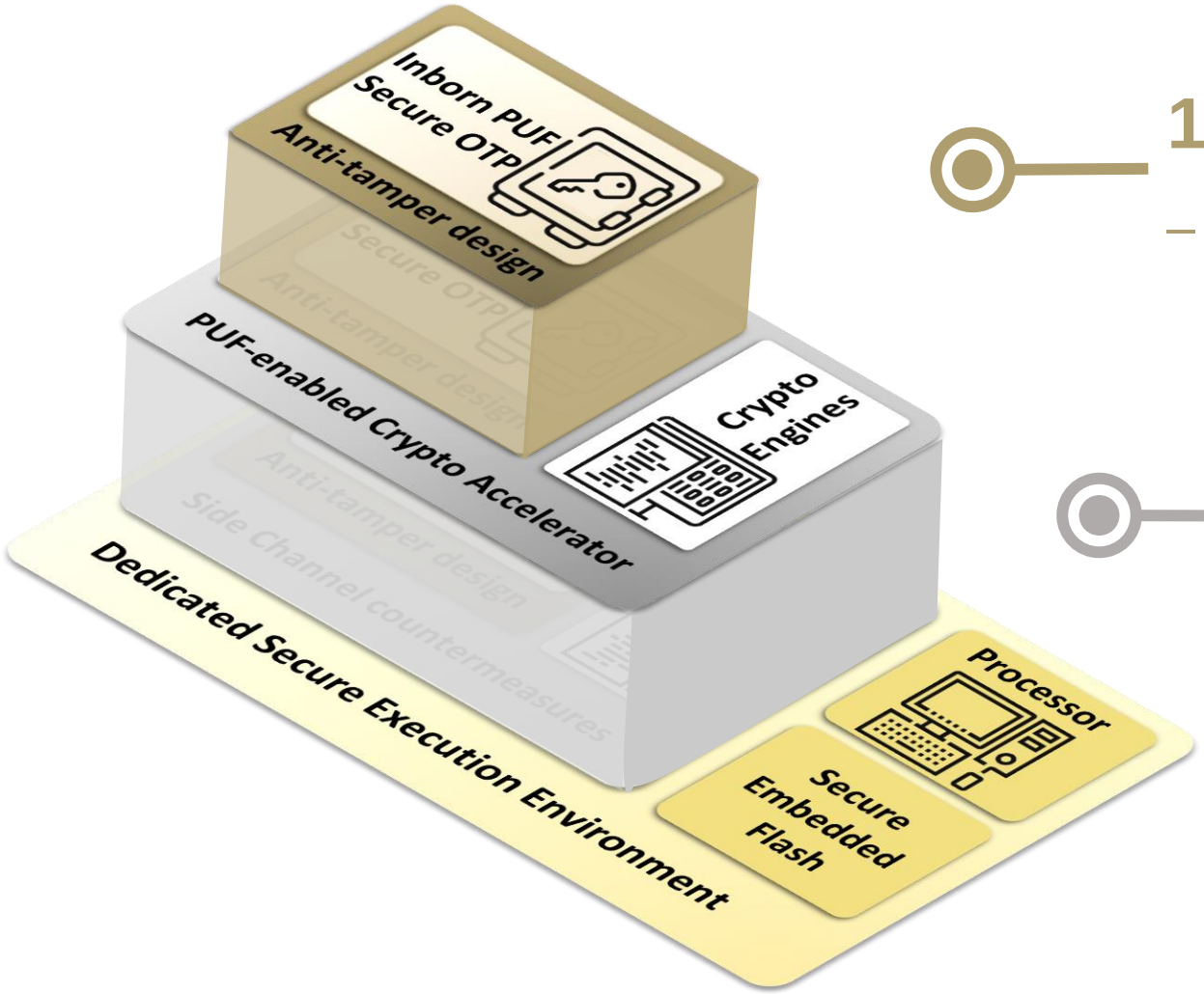
- 以芯片指纹PUF强化防护的硬件信任根(HRoT)
- 利用未知秘密(PUF)保护/产生已知秘密(密钥与随机数)，包覆物理/电性抗攻击设计强化安全防护

PUFiot

- 以PUFrt为基础的安全处理器
- 安全运作所使用的密钥与熵(随机数) 由每一芯片的PUF产生，各自与自带芯片指纹绑定



高安全性的PUFse芯片安全组件架构



1st Security Shell

- Riscure认证的物理/电性抗攻击防护

2nd Security Shell

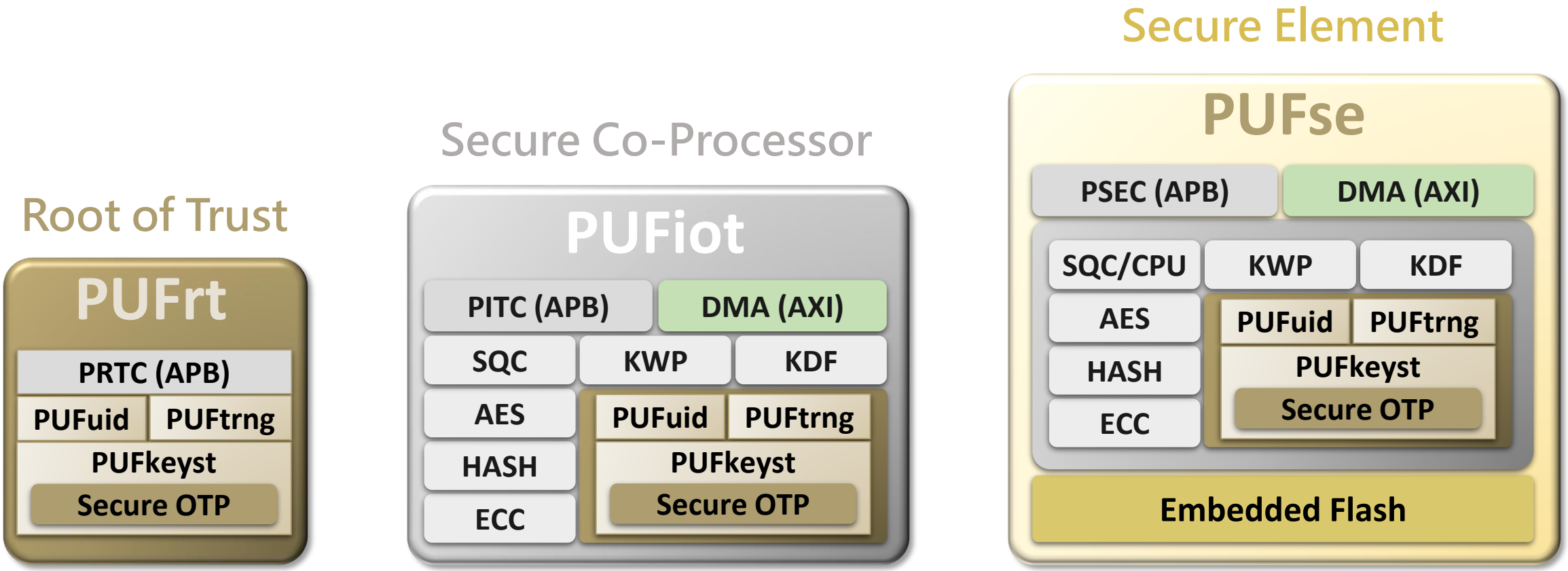
- PSA认证的安全设计架构
- NIST CAVP认证的密码算法

3rd Security Shell

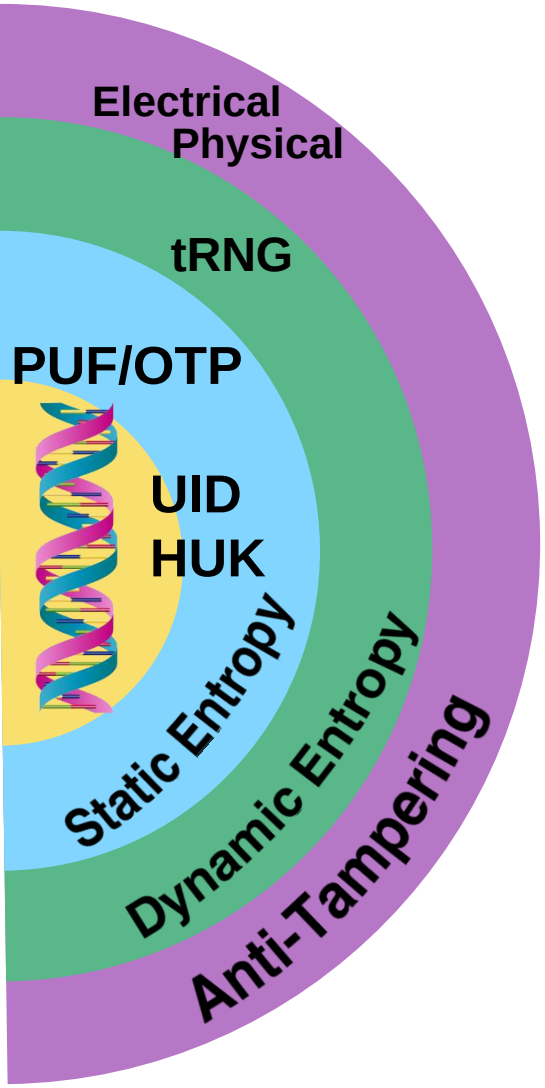
- 带有处理器的安全设计架构
- PUF-based安全嵌入式闪存

熵码产品解决方案

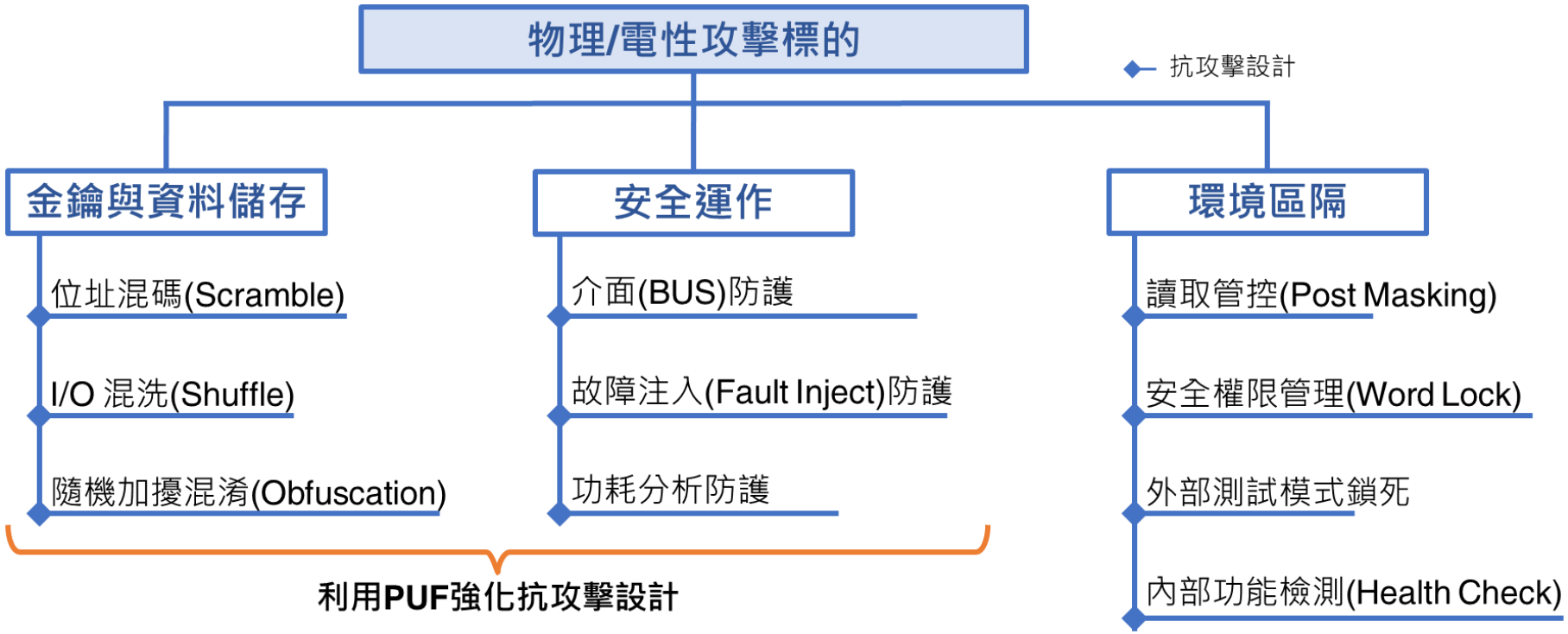
熵码利用芯片原生的PUF作为芯片指纹，开发整合性安全硅智财解决方案，以保护系统单芯片、供应链与应用服务安全



PUFrt – 抗攻击的硬件信任根

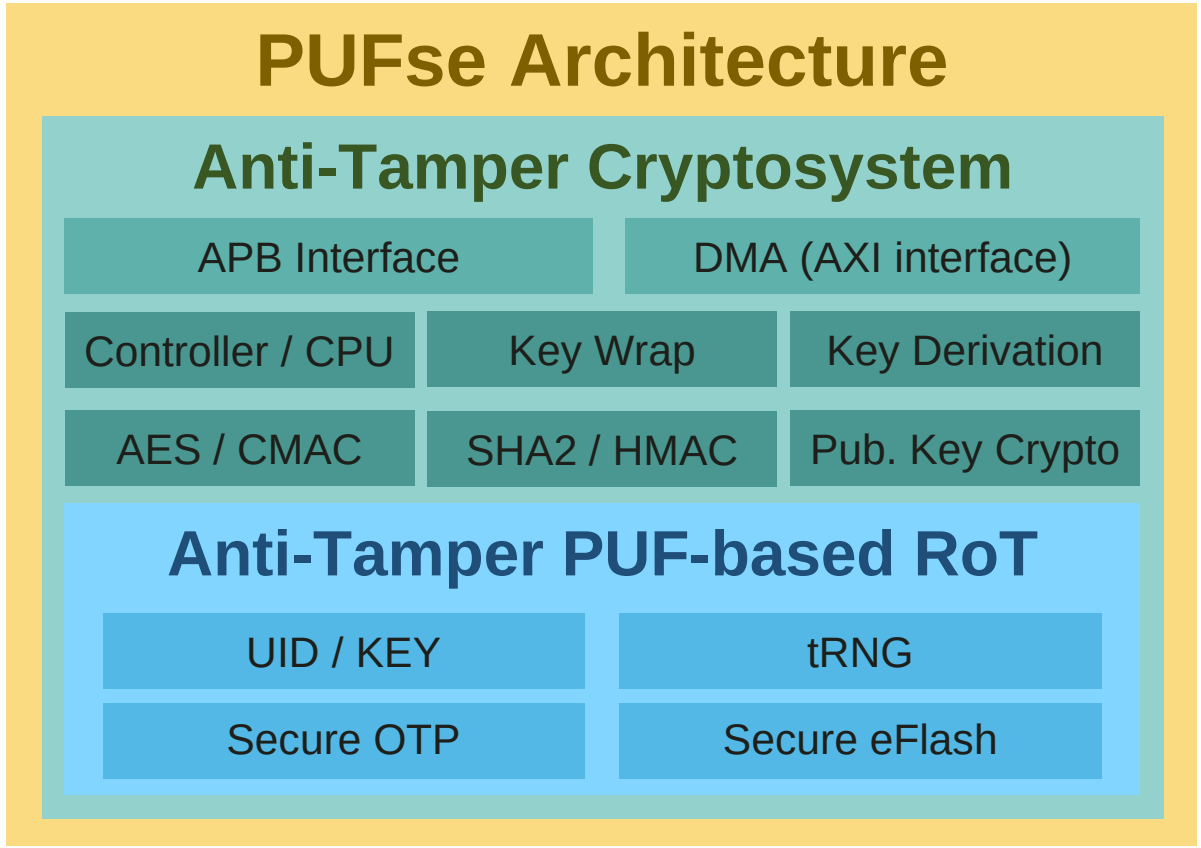


加入物理/电性抗攻击(Anti-tampering) 技术强化信任根单元；
其中数种更以PUF加强防护，共含:



PUFiot/PUFse 安全组件架构

PUFse 安全组件架构由抗攻击硬件信任根、抗攻击密码系统与CPU组成，可独立处理系统所需之基础与高阶安全功能，包含:



- 基础安全功能
  - 资料加解密
  - 完整性检查
  - 认证与签章
  - 密钥衍生/包裹
  - TLS安全协定
- PUF-enabled 进阶应用
  - 抗攻击信任根(UID, tRNG, Key Storage)
  - 全局 – 区域加解密(enc)
  - 装置注册与启用检查(sig)
  - 就地执行的实时加解密(xip)

大纲

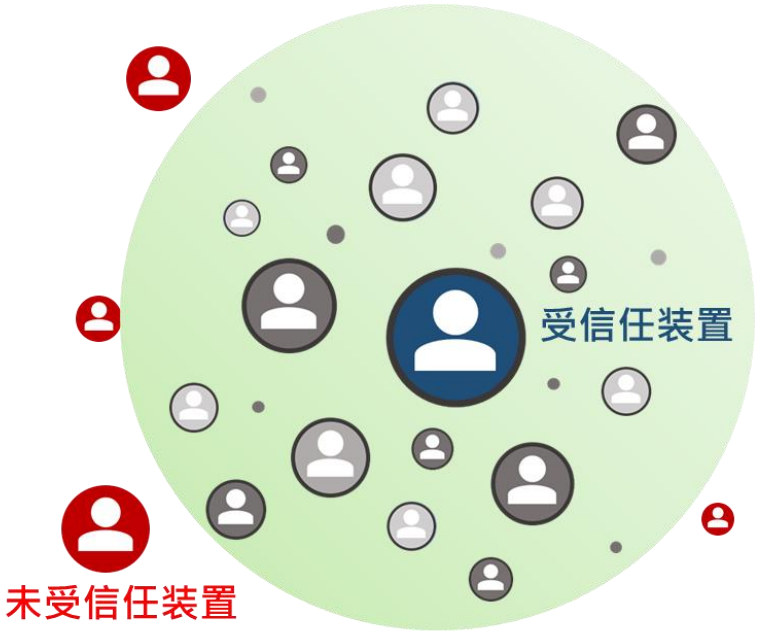
- 芯片指纹技术简介
- 零信任的安全服务与需求
- 如何使用RISC-V实践安全系统单芯片?
- 如何利用芯片指纹确保供应链安全?
- 结论

PUFsecurity

未来的安全是零信任安全 (Zero Trust Security)

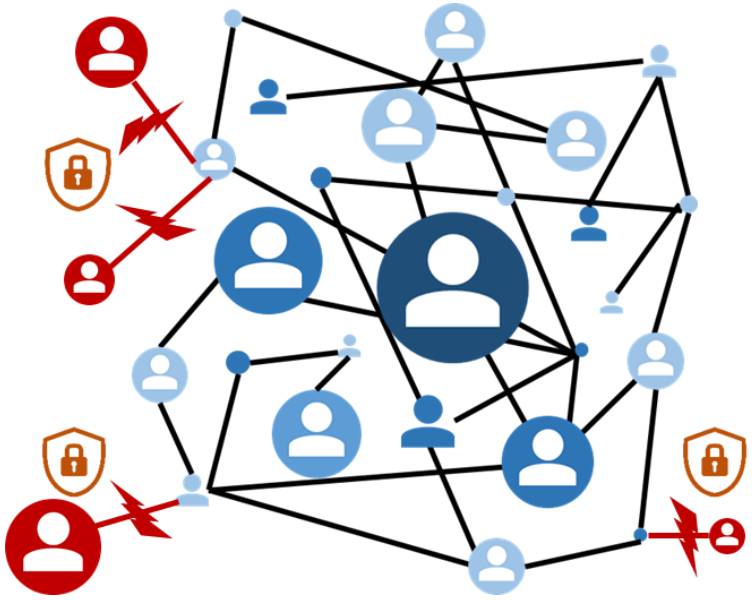
★前提是在各装置皆有其信任根(RoT)能验明正身

现行架构依靠安全网络界限(perimeter)划分
出安全区域做为信任基础



恶意装置藉由渗透进入安全界限危害系统

零信任安全 (Zero Trust Security)
每次沟通都无一例外地先行认证(Authentication)



透过认证有效阻绝恶意装置感染

PUF security

实现零接触的大量组件布署

PUF为基础 (Device eID)标准，实现零接触(Zero Touch)大量组件布署，以提升零信任(Zero Trust)连网应用安全。

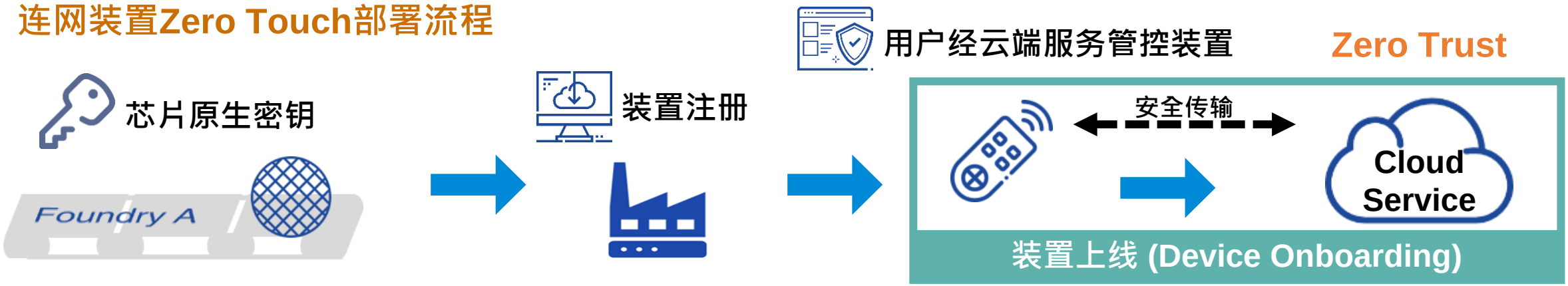
以FIDO Device Onboard规格为例，健全的连网云端生态体系需具有以下要件:

- 以唯一的密钥及数字签名维护装置所有权
- 重要参数写入信任根安全存储
- 以独立的控制器安全运行

PUF-based Device eID可以提高生产/配送供应链安全，并简化装置管理

- 从生产端即以PUF作为装置防伪的基础
- 初始化使用前能确保开通信息无法篡改/泄漏
- 装置使用时能将安全需求交由eID专门处理

连网装置Zero Touch部署流程



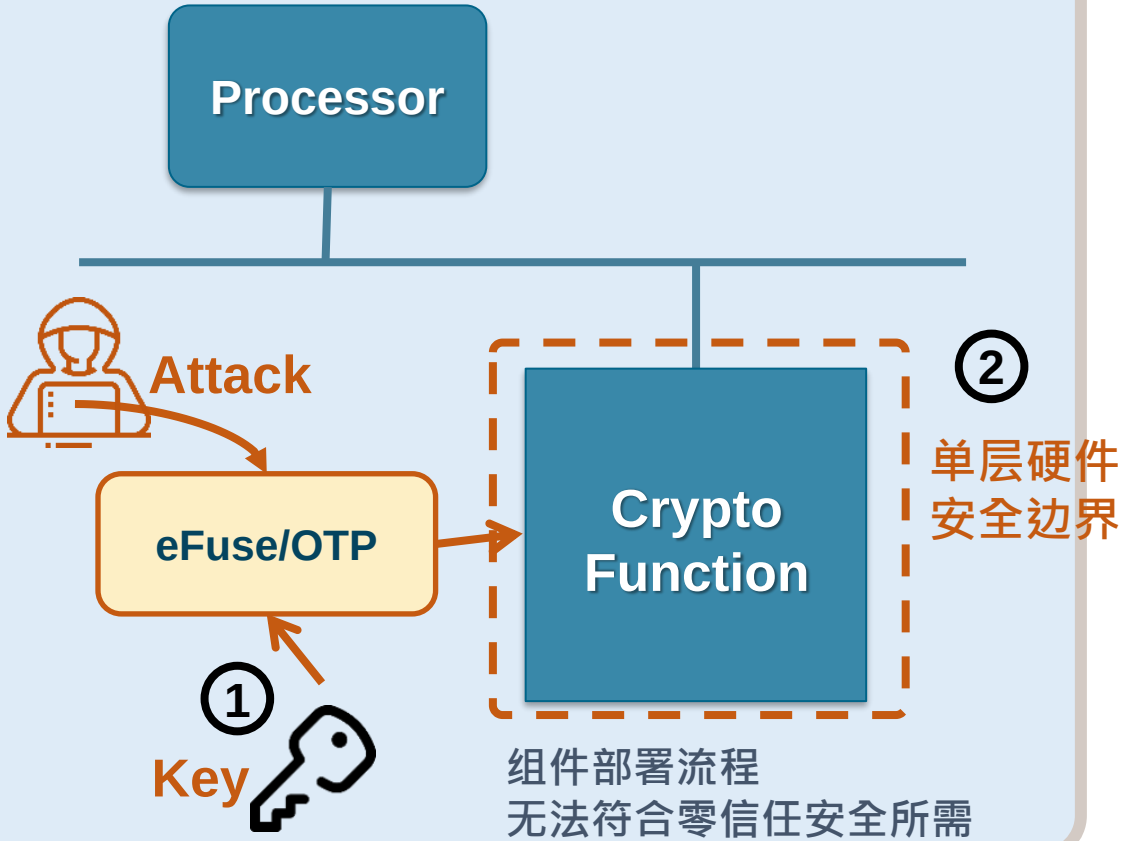
大纲

- 芯片指纹技术简介
- 零信任的安全服务与需求
- 如何使用RISC-V实践安全系统单芯片?
- 如何利用芯片指纹确保供应链安全?
- 结论

PUFsecurity

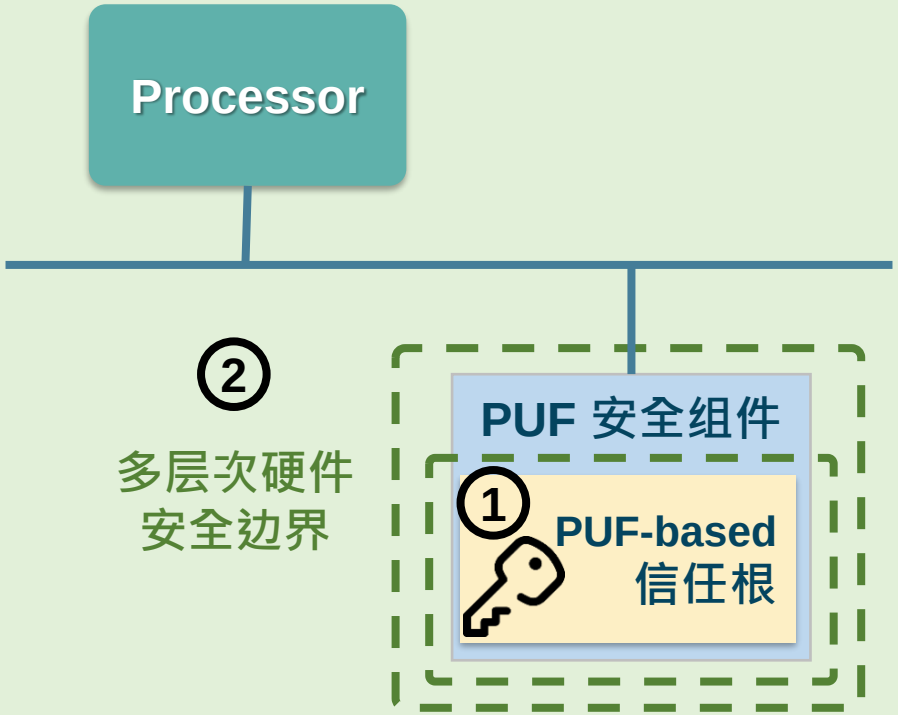
PUFiot/PUFse安全架构能满足零信任安全所需

传统作法多由外部注入密钥，暴露在硬件安全边界之外，没有抗攻击保护设计



组件部署流程
无法符合零信任安全所需

PUF-based安全组件整合信任根于安全边界内，可强化身份、密钥保护



身份、密钥由内建芯片指纹产生
层层保护于硬件安全边界内

PUFiot 成为 RISC-V 不可或缺的安全协同处理器

与Andes合作打造Secure RISC-V ecosystem，补足RISC-V体系的芯片安全缺口

RISC-V 各委员会及关注议题

軟件

- 平台
- 工具链
- 运行時長

安全部署

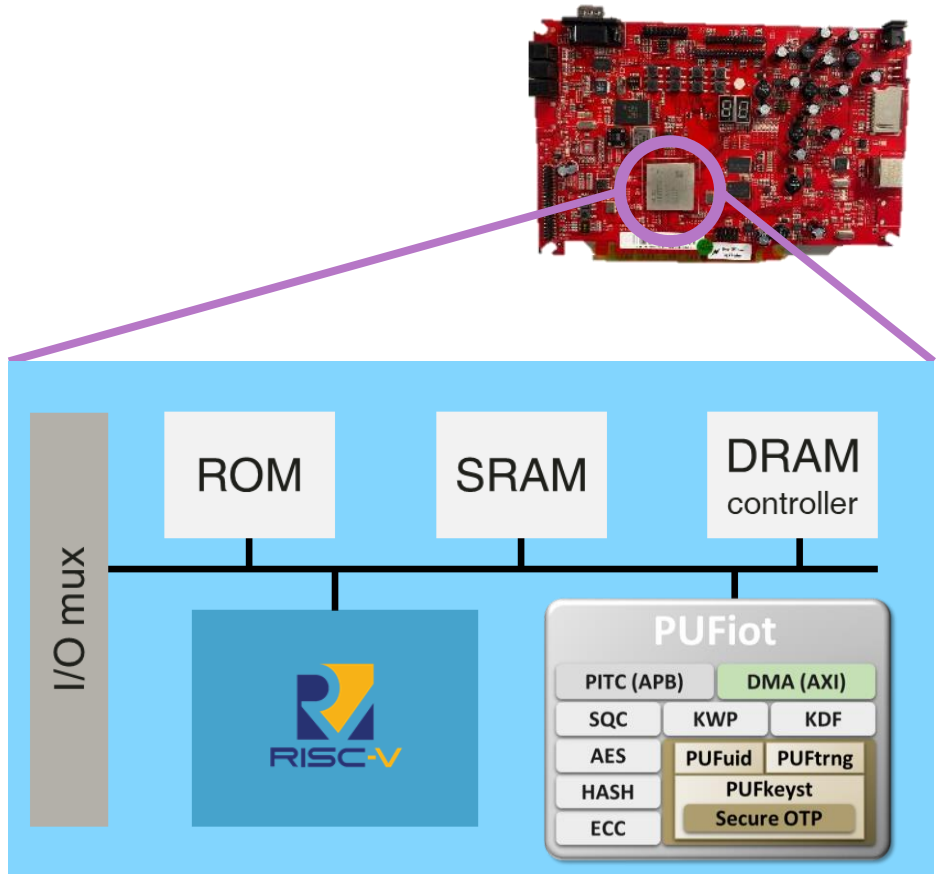
- 信任根
- 加密引擎
- 安全执行
- 物理内存保护

RASD

- 可恢复性
- 可用性
- 可维修性
- 可靠性

ISA基础设施

- 指导监督
- 指令接受



PUF security

PUFiot 已成功与 RISC-V 整合，保护AI应用

具PUFiot完整功能的Andes AE350/D25开发版，能提供AI应用所需的各式安全功能

AI 运作 \ 安全性	威胁模型 (Threat Model)	防护手段
产品激活与认证	• 韧体遭窜改/替换 • 产品未经授权、或遭仿冒	• 安全启动(secure boot) • 产品注册开通及签章认证
模型训练和部署	• 训练资料遭窃 • 模型从终端装置被窃 • 数据与模型遭窜改/替换	• 保护数据传输(in-transit) • 保护储存于终端的模型 • 完整性检查
实务使用及推论	• 未经授权/恶意使用者 • 用户数据外泄 • 模型输入/输出遭窜改	• 产品注册开通及签章认证 • 保护静止(at-rest)资料 • 完整性检查/讯息验证

PUF security

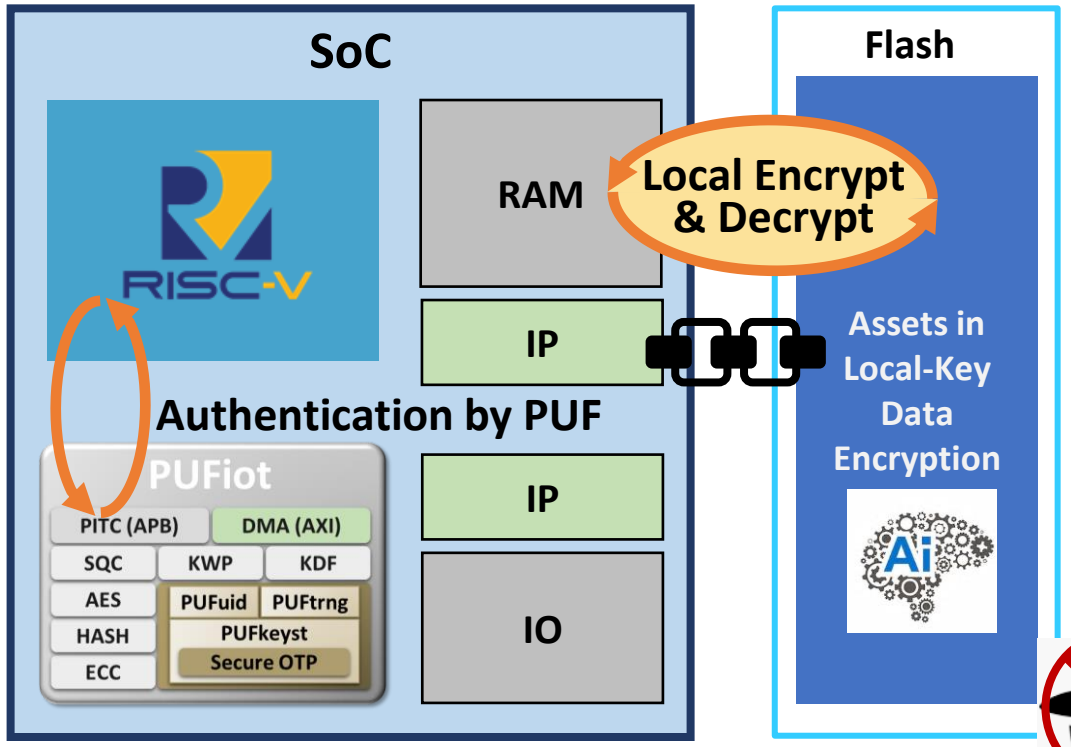
PUFiot 简单实现数据认证与保护

使用PUF作为签章(密钥)以保护芯片不被盗拷
使用芯片内嵌的PUF绑定并保护软/固件 (know-how)

利用PUF签章认证启动码(Boot code)与芯片

启动时:

1. 从PUF及映像档重新产生哈希值HASH'
2. 与事先储存保护于PUFrt内的原哈希值HASH比对
3. 若HASH' = HASH则验证成功



Flash与SoC经由PUF密钥一对一绑定，

启用全局-区域转换加密时:

1. 利用全局密钥解密信息
2. 将信息利用PUF密钥重新加密

如此Flash内资料不经PUF key(芯片指纹)无法解密

大纲

- 芯片指纹技术简介
- 零信任的安全服务与需求
- 如何使用RISC-V实践安全系统单芯片?
- 如何利用芯片指纹确保供应链安全?
- 结论

PUF security

PUF-based SE 提升芯片供应链安全

以车用电子为例，熵码与鸿海MIH平台合作Chiplet项目，提供电动车芯片安全组件

装置防伪

系统认证、防窜改

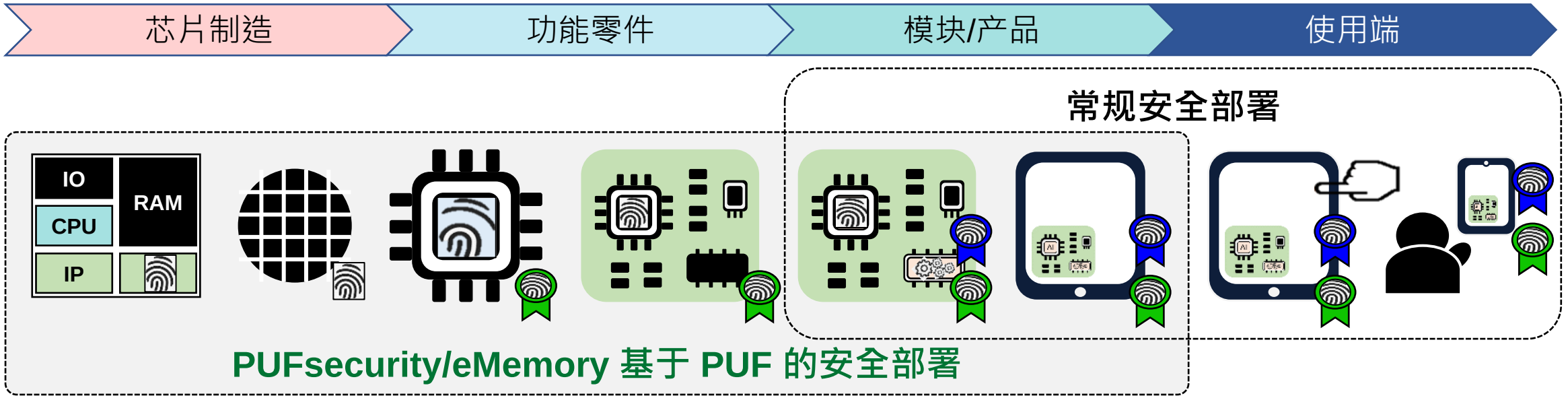
维护车用芯片供应链安全

ICT
（車用電子、晶片、半導體）
威力暘、新呈工業、廣美科技、偉詮電、榮復國際、文曄科技、百容電子、乾坤科技、阜聯電子、飆慧事業、鴻騰精密、隆達電子、台光電子、神達數位、亞弘電科技、信錩實業、喬越實業、M31、瀚薪科技、慧榮科技、強茂、瑞昱、聯發科、美隆工業、協欣電子、公信電子、聯詠科技、大毅科技、socionext、群聯、佑華科技、力旺電子、展匯科技、雷捷電子、智原、連宇、iST宜特、熵碼科技、增你強、友尚、京威先進科技

Source: 天下杂志第718期 “电动车护国群山崛起”

使用PUF-based SE保护半导体供应链安全

PUF-based SE 作为合规的eID可以用来开通芯片、设定生产过程供货商的权限、记录芯片生产履历，保护供应链安全



防反组译	反超量生产	防伪	反黑客/克隆固件

- 無須认证洁净室即可產生的低成本 HUK
- 防反组译及超量生产
- 防伪、保护FW/SW
- 用于 FW 身份验证的 HRoT 安全启动

大纲

- 芯片指纹技术简介
- 零信任的安全服务与需求
- 如何使用RISC-V实践安全系统单芯片?
- 如何利用芯片指纹确保供应链安全?
- 结论

PUFsecurity

内建PUF硬件信任根营造更安全RISC-V应用体系

3. 加固现有应用安全
落实零信任安全服务

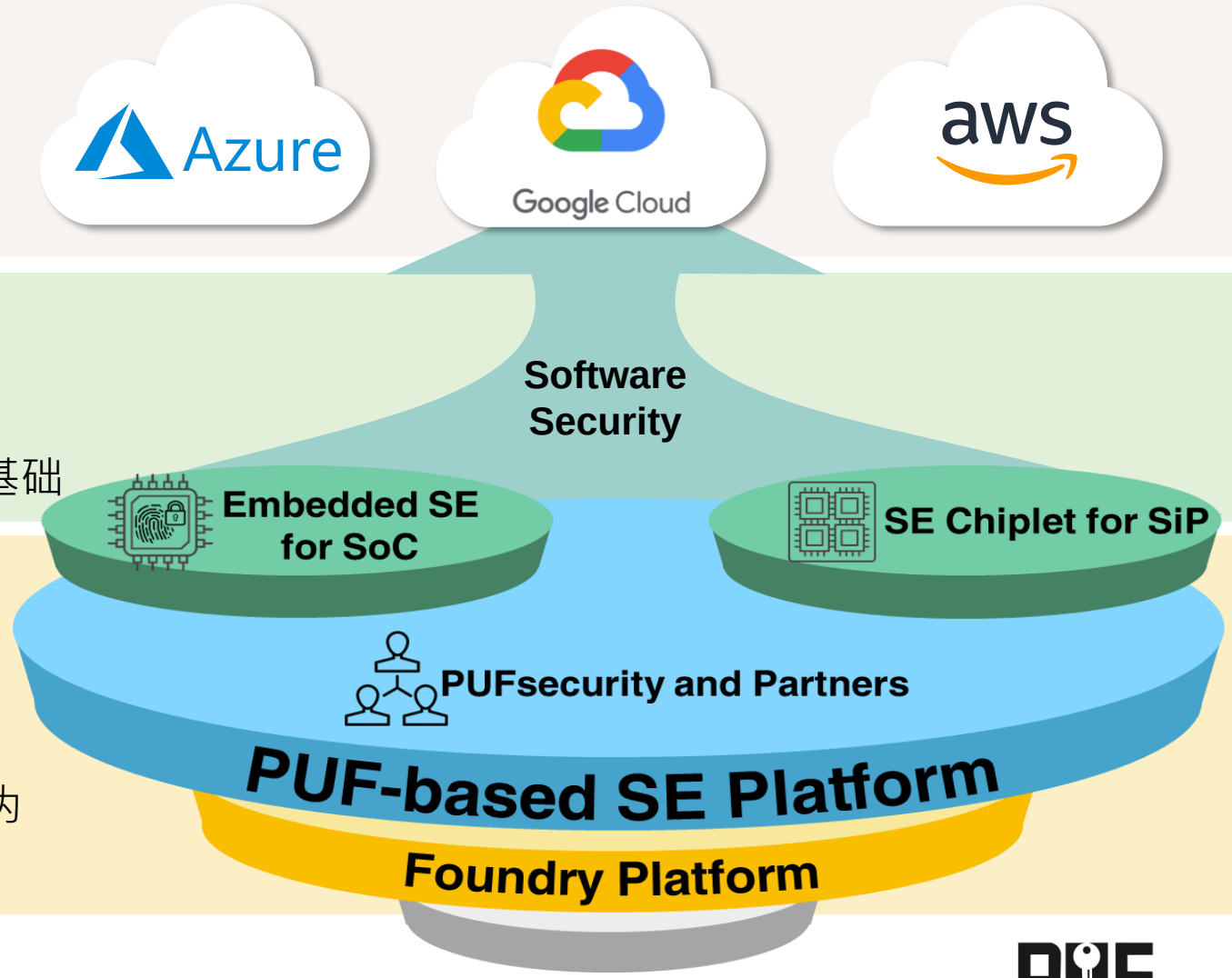
信任安全来自产品唯一身份识别

2. 硬件安全强化软件安全
简单实现零接触大量组件布署

以芯片指纹作为产品生命周期管理的基础

1. 建构芯片指纹安全运算核心
强化半导体产品供应链安全

内嵌原生芯片指纹强化运算安全与防伪



PUF security

谢谢聆听!

更多信息详见: www.pufsecurity.com

来信请至: info@pufsecurity.com