从根源解决芯片安全弱点

以 PUF-based 硬件安全信任根构建芯片内完整安全边界

PUFsecurity

产品白皮书

October 2021

John Chou
邹定宇

前言

在 19 世纪，荷兰的密码学家奥古斯特·克尔克霍夫 (Auguste Kerckhoff) 发表了克尔克霍夫原理，指出：「即使系统中除密钥之外的一切都是公共知识，密码系统也必须是安全的。」芯片安全中最关键的元素是根密钥(Root Key)或硬件唯一密钥(Hardware Unique Key; HUK)。根密钥不仅是保护每个芯片的基础，也是整个系统和相关服务的信任链起点。因此，必须从设计之初就充分考虑密钥的生成、存储和使用的方式。

随着物理不可复制功能 (PUF) 的发明，我们现在可以在硬件级别创建一个独特的、天生的、不可复制的密钥。而后续该思考的问题是，“我们如何保护这把钥匙？”若是没有做好保护密钥的安全机制，就好比将你的密钥随意扔在抽屉里一样，破坏了安全边界形成安全漏洞。一个系统的安全级别取决于该系统安全中最弱的环节，在大多数情况下，系统的安全弱点往往是存储在不甚安全的 eFuse 中的密钥。无论密钥本身的复杂程度如何，不安全的存储都会立即危及整个系统的安全性。

此外，我们知道软件可以在产品出厂后持续更新，但硬件更新相对困难且成本极高。因此，在一开始所选择的硬件安全部署质量是至关重要的。 PUFrt 是结合 PUF 和 anti-fuse OTP 的硬件信任根 IP，在完整防篡改设计的保护下，提供不可复制的密钥和安全的 OTP 存储，从制造阶段起即提供硬件安全防护。

以 eFuse 做密钥存储的风险

eFuse(熔丝)和 anti-fuse OTP(反熔丝内存)是现代芯片设计中最常见的密钥存储选项。 eFuse 的原理是透过熔断金属或聚合物的方式将密钥编程到 OTP 内存中，这会留下可见的痕迹。 而 anti-fuse 的编程方式是根据量子穿隧原理在单晶体氧化层形成导电路径，因此表面上没有可见的痕迹。 图 1 为 eFuse 和 anti-fuse OTP 在电子显微镜下的比较。储存在 eFuse 中的“0”和“1”数据很容易识别，因为在编程为“1”的单元中有一个明显的开口。 而如图 1 的右图所示，无论存储的数据如何， anti-fuse 单元看起来并无显著差异。

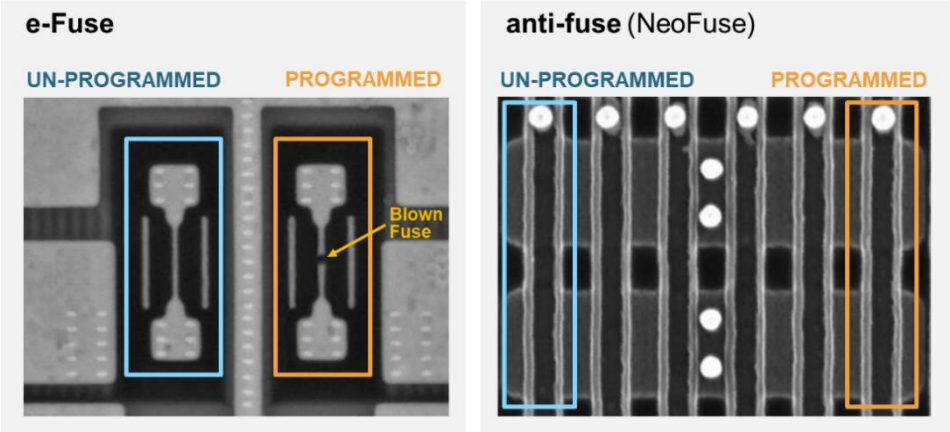

图 1. e-fuse 与 anti-fuse OTP 在电子显微镜下的俯瞰图

不安全存储造成的漏洞

以 ARM 核搭配 Crypto Cell-312™ (CC312) 是当今最常见的设计组合之一。当设计人员都着重于 CC312 提供的安全功能时，但却往往忽略了密钥存储的安全。 我们经常可以看到，ARM CC312 与 eFuse/anti-fuse 搭配使用，可是针对密钥注入和存储程序却没有额外的保护(如图 2 所示)，造成密钥仍暴露在安全边界之外，成为攻击者有机可乘的安全漏洞。这样的安全问题来自于两个层面，一是储存在 eFuse 中的数据容易被窥探破解；二是当访问权限控制没有被考虑时，任何人皆可轻松获取储存在 OTP 中的机密。尽管 CC312 被认为是一款设计精良的门锁，但将钥匙存放在不安全的地方无异于将钥匙留在门锁中供任何人开启一样。

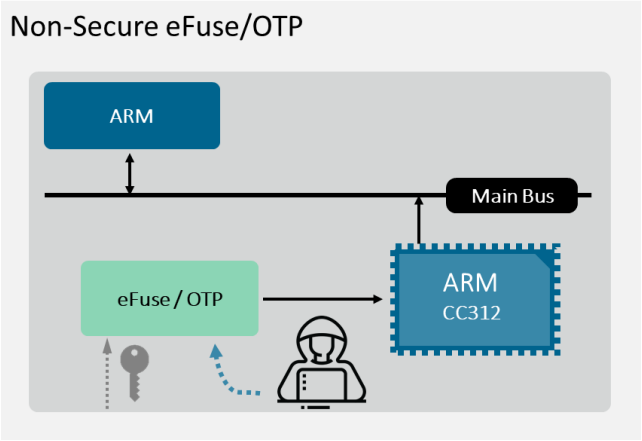

图 2. 不安全的信任根

以抗攻击设计强化的安全防护

虽然 eFuse 中的数据可见性问题可用 anti-fuse OTP 解决，但严格来说这样的安全防护仍然不足。为了实现身份识别并仅将机密数据的访问权限开放给获得授权的用户，在 OTP 控制器设计中还必须考虑访问权限控制。

为了进一步保护芯片设计中的 anti-fuse OTP，防篡改设计也是不可或缺的。良好的防篡改设计运用电路布局(Layout)和数字设计(RTL)打造一个可对抗各种类型的攻击，如在写入数据时对数据进行加扰、或是纳入毛刺检测电路等等的保护外壳。我们将在未来的白皮书中更详细地讨论防篡改设计的主题。

将 anti-fuse OTP、访问权限的控制器和防篡改外壳相结合，建立了一个安全的硬件信任根 (Hardware Root of Trust; HRoT)，即可对抗所有前述所讨论的漏洞。 凭借精心设计的防篡改外壳和权限控管的双 APB 接口，安全 HRoT 与安全子系统，CC312 等，能相辅相成，为芯片设计实现完整的安全边界。熵码科技所开发的 dual-APB RoT IP--PUFrt，即是专为 ARM CC312 和其他 ARM 用户的需求所开发。更详细的说明及其功能详见图 3。

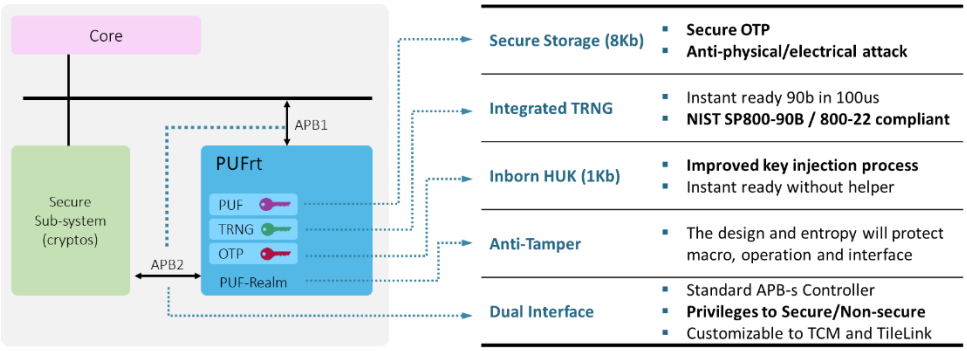

图 3. PUFrt 模块示意图与其重要特点

以 PUFrt 实现完整安全边界

PUFrt 建立在 力旺电子的 anti-fuse OTP (NeoFuse) 和量子穿隧 PUF (NeoPUF) 技术之上，并以 PUF 天生密码加密保护 anti-fuse OTP。PUFrt 利用 NeoPUF 完美的随机性自芯片内部生成每个设备的唯一密钥(Hardwre Unique Key; HUK)，大幅简化了密钥配置的程序。真随机数发生器 (TRNG) 具有数字和仿真设计，结合了静态和动态熵源以实现其卓越的性能。PUFrt 还对数据和地址进行了混淆处理，并结合模拟与数字设计了抗攻击安全防护层，以充分保护密钥存储。此外，PUFrt 还配备了一个权限控管控制器和两个 APB 接口。图 4 即示意了 PUFrt 和 ARM CC312 整合使用的范例。 APB1 将 PUFrt 连接到 BUS 总线并使用 JTAG 进行 OTP 测试，

APB2 将 PUFrt 集成到 CC312 中，为 CC312 中的加密功能提供安全存储和高质量熵源。APB1 将在测试后被禁用，以维持安全边界的完整性。

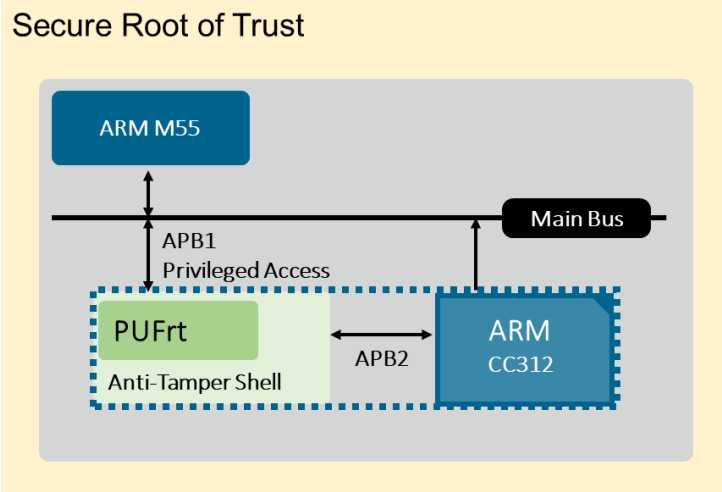

图 4. 结合 PUFrt 延伸 ARM CC312 的安全边界

总结而言，双 APB 接口的 PUFrt 能与 CC312 无缝集成，并为密钥存储提供完整的抗攻击防护。此外，PUFrt 中的 TRNG 能为 CC312 提供高质量的熵以执行各种安全功能。透过集成 CC312 和 PUFrt，ARM Cortex-M55 可以在推向市场之前实现安全信任根、安全存储和安全系统。这种应用可推及 AIoT 到 HPC 等多项领域。

结论

谈到芯片安全性，设计人员通常会想到 ARM Crypto Cell 312 等加密子系统解决方案。然而，如何为系统生成可信赖的根密钥、以及如何安全储存该密钥的问题仍然未解。 PUFrt 就如同一幅完整拼图所缺失的部分。利用 PUF 的天生密码(芯片指纹)作为密钥来加密存储的任何机要信息，再加上全面的抗攻击设计，使其成为能抵御各类潜在攻击的完美方案。 凭借其精心规划的架构，PUFrt 可以轻松导入芯片取代不安全的 eFuse，其权限控管控制器更为设计人员节省设计时间。总结而言，PUFrt 整合解决方案不仅完成了 IC 的安全边界，且能帮助 CC312 对整体 SoC 的性能表现达到极致发挥。

PUFsecurity

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

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