



**赛题答疑邮箱**

[zhengwenbin.zwb@alibaba-inc.com](mailto:zhengwenbin.zwb@alibaba-inc.com)

**平头哥企业命题专项奖设置**

一等奖1队，奖金10 000元二等奖3队，奖金5 000元

**赛题：基于开源E902处理器构建双核TEE安全解决方案**

**赛题描述：**

随着物联网(IOT)的高速发展，信息安全问题突显，可信执行环境（Trusted Execution Environment，TEE）是保障信息安全的有效手段，因此在RISC-V处理器上构建TEE的安全能力是眼下最热门的话题。本赛题旨在利用平头哥开源的RISC-V处理器（E902）设计一个支持TEE的最小系统，为RISC-V处理器构建TEE的安全原型。双核TEE安全架构中，其中一个E902核心用作安全核，运行安全世界程序，另一个E902核心用作非安全核，运行非安全世界程序。通过双核方案实现CPU在物理上的隔离，保证非安全核无法访问安全世界的资源，包括内存和MMIO。E902安全核和非安全核之间的通信需要用到mailbox设备，安全世界的mailbox属于安全设备，非安全世界的mailbox属于非安全设备。系统从安全核上启动，完成安全配置后才能启动非安全核。

**参考建议：**

在E902非安全核后面接一个地址访问防火墙，比如IOPMP，用于约束非安全E902核对内存、MMIO的访问。

**提交内容：**

1）作品展示，包括技术创新、项目内容和后续工作

2）设计报告：

* 项目背景
* 系统架构和安全方案，包含处理器、内存、I/O和调试的隔离方案，安全启动流程，以及关键模块的描述
* 功能仿真、FPGA测试结果
* 总结
* 参考文献和团队介绍

3）设计代码：

* SoC平台代码
* 安全启动代码
* TEE/REE软件栈

**参考平台：**

SoC平台可参考开源的无剑平台（<https://occ.t-head.cn/development/chip>），FPGA开发平台可选择Xilinx FPGA。

**评分标准：**

|  |  |  |
| --- | --- | --- |
| **评分级别** | **功能实现** | **得分** |
| 基础任务 | SoC至少包括基础双核E902+存储（SRAM）+IO(2个串口) | 30 |
| 每个E902核分别运行独立的软件程序，并从串口输出打印信息 | 30 |
| SoC实现BootROM，实现安全启动机制，比如: BootROM->TEE Code ->REE Code | 20 |
| 中级任务 | BootROM实现从安全串口加载程序 | 10 |
| SoC实现Mailbox，双核E902通过Mailbox建立核间通信 | 10 |
| SoC实现IOPMP，通过IOPMP来控制E902非安全核的对内存(SRAM)、MMIO(如串口)的访问权限 | 10 |
| 高级任务 | SoC实现Crypto加解密模块，实现硬件AES、RSA加解密算法，用于加速对程序的解密和验签，并通过IOPMP控制Crypto引擎的访问权限 | 20 |
| 设计报告 | 设计报告应详细阐述技术方案，尤其需要突出如何实现中、高级任务的技术要点，报告应结构清晰、逻辑流畅、详略得当。 | 10 |
| 技术路线 | 在实现中、高级任务时，应于现有的常规技术路线进行对比。如果在技术路线上有成功的改进或突破，可以根据技术路线的先进性判别得分。 | 10 |
| **总分** |  | 150 |

评分标准：

1. 所有任务，功能每实现一项，即可得到该项所有分数
2. 如果未完全实现某项功能，根据技术报告的内容酌情给分