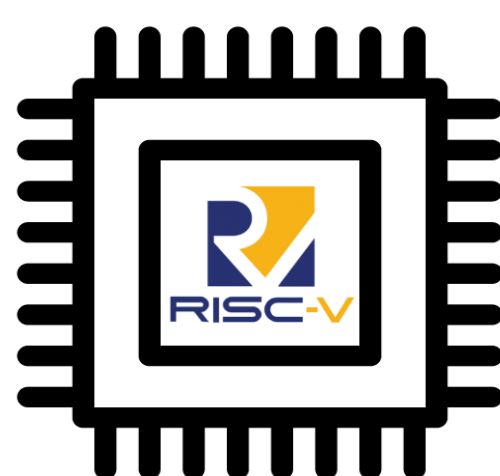




经过CC EAL7认证的RISC-V安全芯片

• RISC-V 处理器

- RV64IMACZifenceZicr
- MMU
- Instruction 和 Data Caches



• 交互接口

- NFC
- ISO-7816
- GPIOs



• 控制流完整性的延伸:

- 检测代码执行过程中的不正常序列
- 由于物理攻击, 如激光、电源/时钟故障、温度、探测或其他原因造成的问题



• 阻止来自硬件的攻击

- Active Shield
- PVT
- Laser
- EM
- Light Sensors



• 指针和返回地址堆栈的保护扩展:

- 防止存储在内存中的指针被改变或伪造
- 防止在内存中已经暴露在堆栈的返回地址被伪造或复制和重复使用



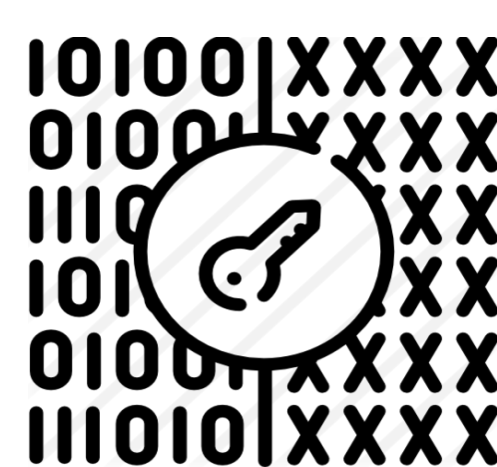
• 发展支撑

- Debug over two wire JTAG (IEEE 1197.7)
- Full IDE provided with :
 - C, C++ compilers
 - Assemblers
 - Linkers
 - libraries
- CC EAL7正式认证的内核管理核心代码
- 编译器修改, 在将指针存储到内存之前生成额外的指针"加密"指令, 在从内存读取指针时生成"解密"指令。



• 客户指南

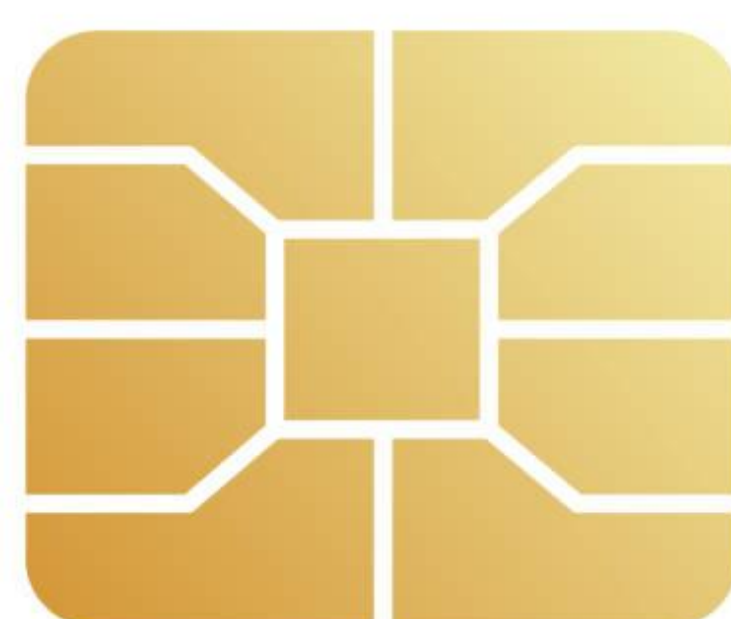
- 对指针值和情景加密
- 对指针值和情景进行解密, 如果是伪造的, 会进行进一步捕获
- 情景是提供的额外操作符, 所使用的密钥被存储在仅可写入的CSR中。



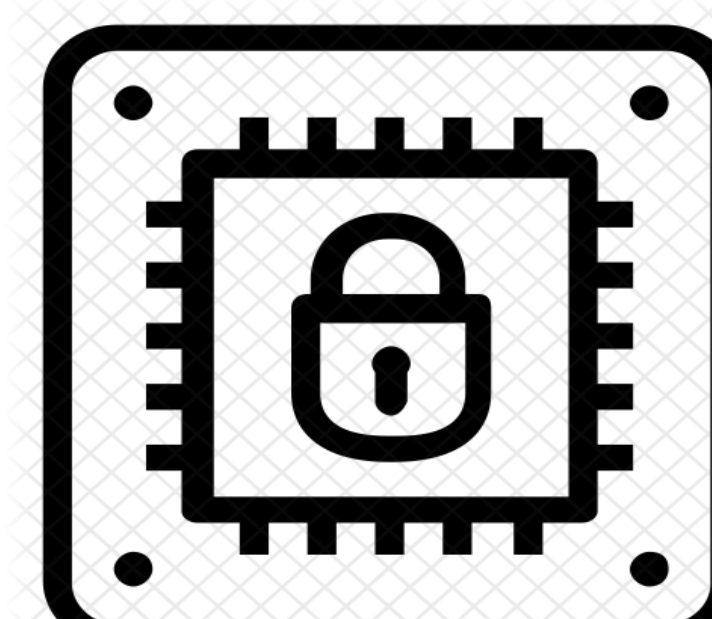
应用 / 目标市场



汽车行业



智能卡片



ROT / HSM

Cortus 非常欢迎大家积极咨询关于您的申请及需求的问题

法国区域联系人
Michael Chapman
michael.chapman@cortus.com

大中华区联系人
Zhongwei Xu 徐中伟
MP: +86 13918555536

有任何问题和商务合作需求
请扫描本二维码添加微信

