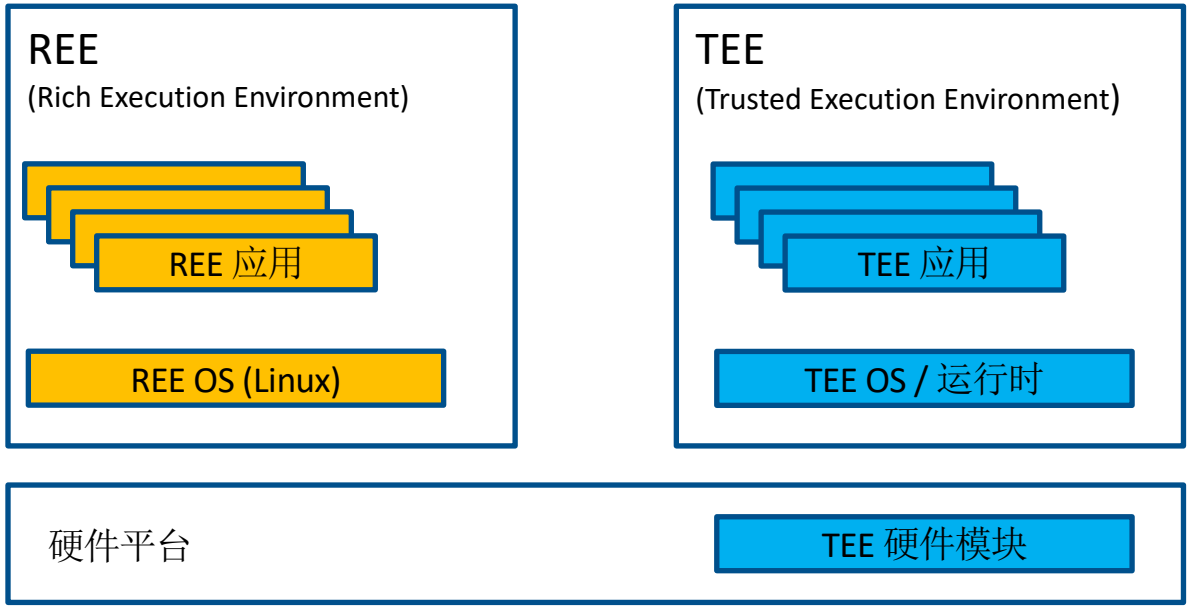
蚂蚁集团 ANT GROUP | 支付宝 | DataFun.

HYPERENCLAVE
信创TEE最佳实践

刘双 蚂蚁集团 高级技术专家

什么是可信执行环境(TEE)?



① 遗世独立

- REE复杂软件栈被排除在TEE 之外，攻击面更小
- TEE安全性依赖于自身，与REE无关

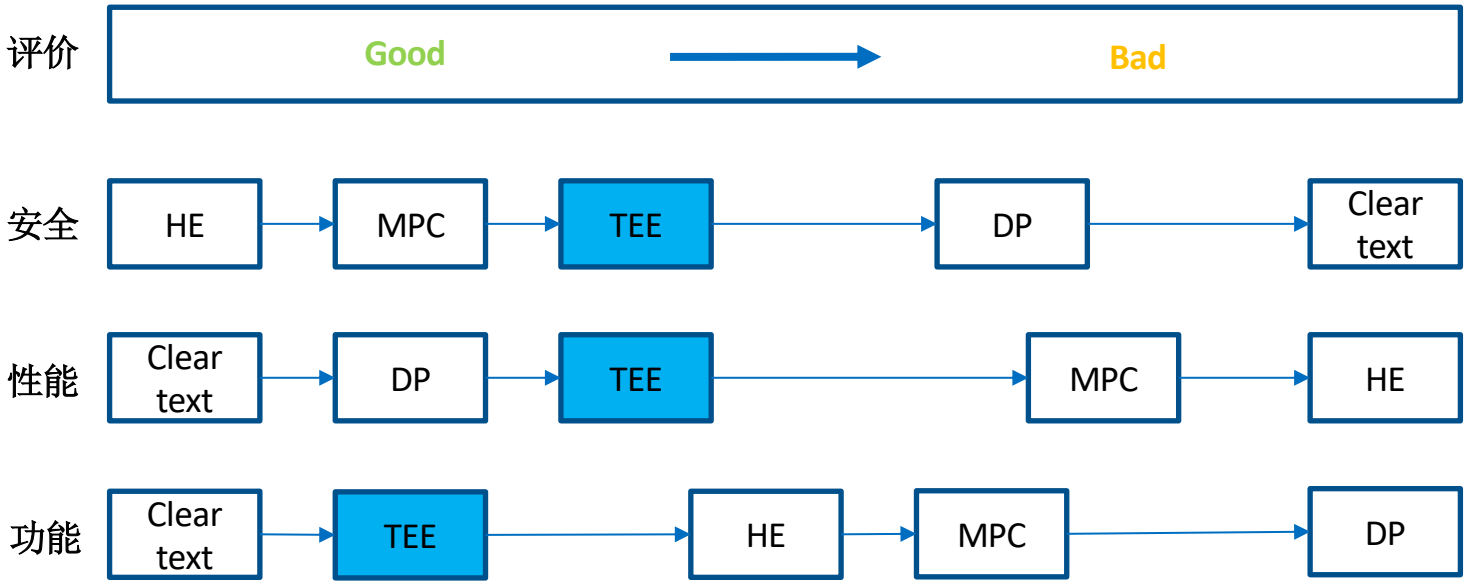
② 密不透风

- TEE硬件保证TEE与REE隔离
- TEE硬件通常对TEE内存加密

③ 清者自清

- TEE硬件可作为信任根，提供远程证明

各种隐私计算技术比较



TEE 优势是兼顾通用与性能，可单独使用也能跟其他技术有机结合

背景

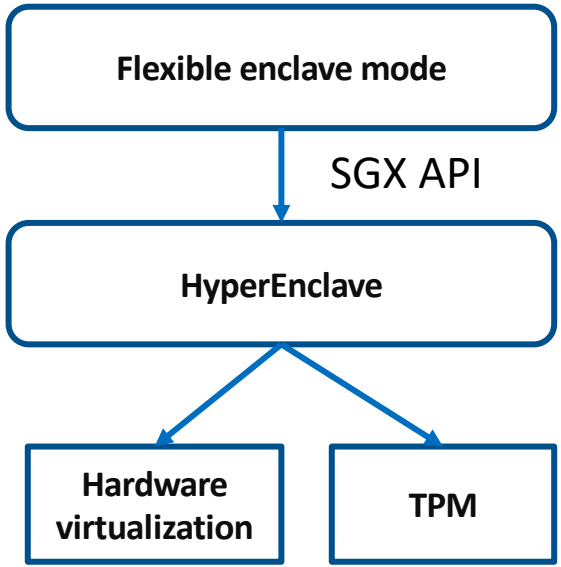
现有的TEE方案存在如下问题：

- 依赖特殊的硬件和固件修改：功能演进缓慢
- 硬件闭源：安全性无法审计
- 信任根与CPU绑定：通用性差
- 仅能提供单一TEE 应用运行模式：不灵活

TEEs	Company or Academia	Where isolation is implemented?	Root of trust	Enclave mode
TrustZone	ARM	Processor	N/A	Kernel
SGX	Intel	XuCode	CPU	User
SEV	AMD	Co-processor	CPU	Kernel
TDX	Intel	Firmware	CPU	Kernel
CCA	ARM	Firmware	N/A	kernel

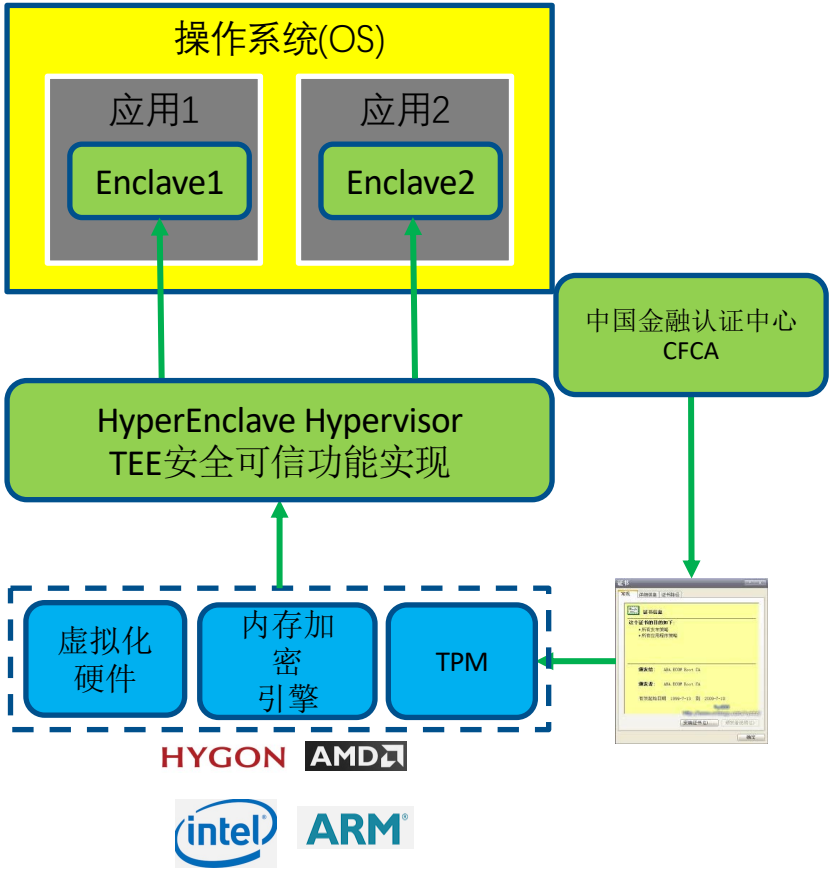
设计目标

- G1: 硬件依赖最小化，支持多平台
  - 硬件虚拟化(隔离) + TPM(可信)
- G2: 易于开发
  - 兼容现有SGX工具链和生态
  - 不修改或少量修改即可运行现有SGX应用
- G3: 支持灵活的运行模式
  - 更好的满足TEE应用对安全与性能的不同需求

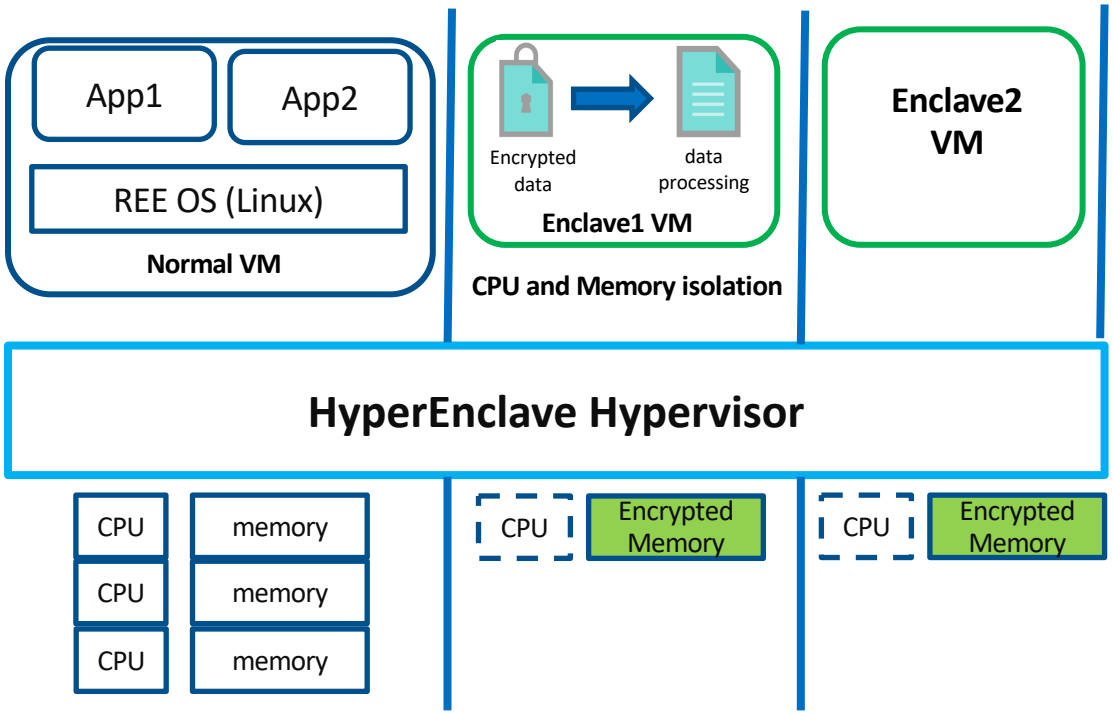


HyperEnclave 信创TEE方案

- 原生支持国产海光CPU平台，同时兼容Intel, AMD等
- 信任根构建于国家金融信息安全基础设施
- 软件生态完备：兼容SGX SDK，Teaclave Rusk SDK, Occlum 等已有TEE生态
- TEE 能力完备：隔离执行，远程证明，内存加密，数据封印
- 安全性经形式化证明和权威机构审查认证
- 已通过金融科技产品认证



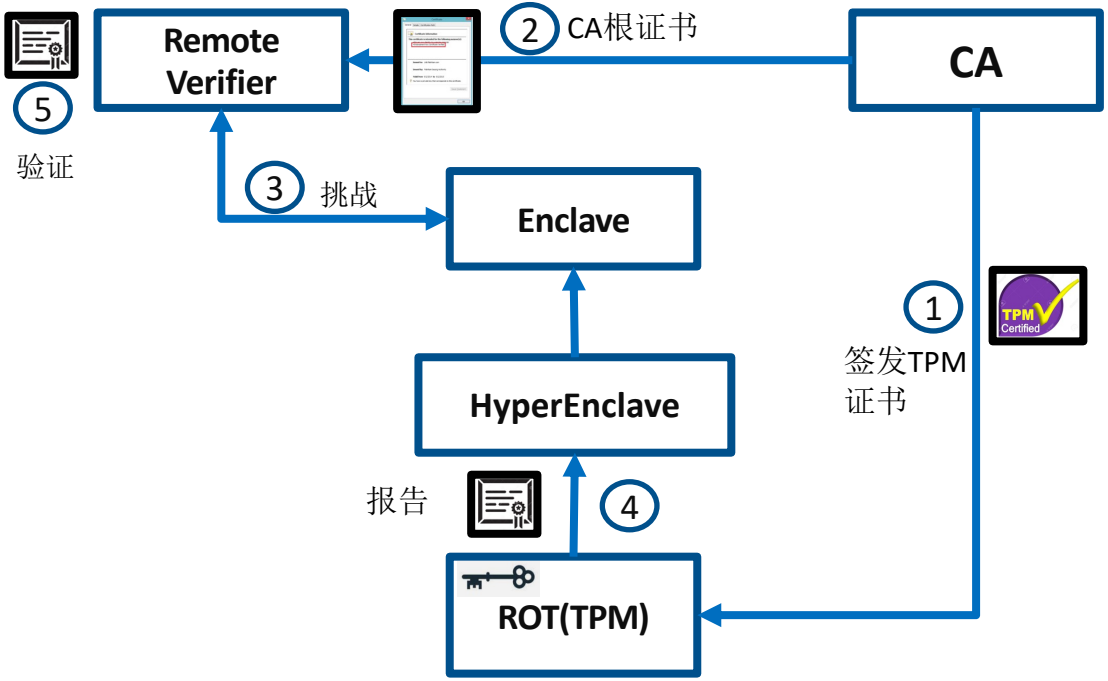
安全隔离

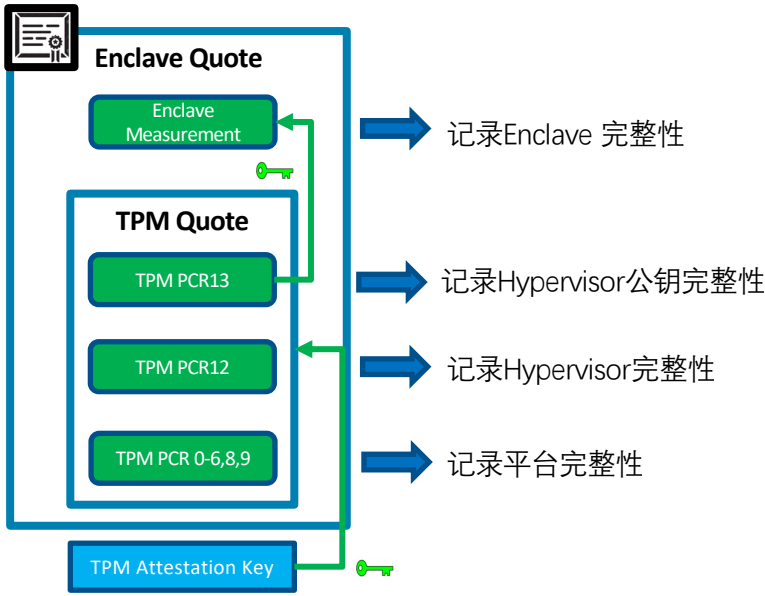


- 运行在REE上的应用负责创建对应的Enclave VM，借助该Enclave VM处理隐私数据，如：App1 对应 Enclave VM1
- HyperEnclave 基于虚拟化技术为Enclave VM提供安全隔离环境：保证Enclave VM运行时的机密性和完整性
- REE 与 Enclave VM隔离，Enclave VM间彼此双向隔离

远程证明

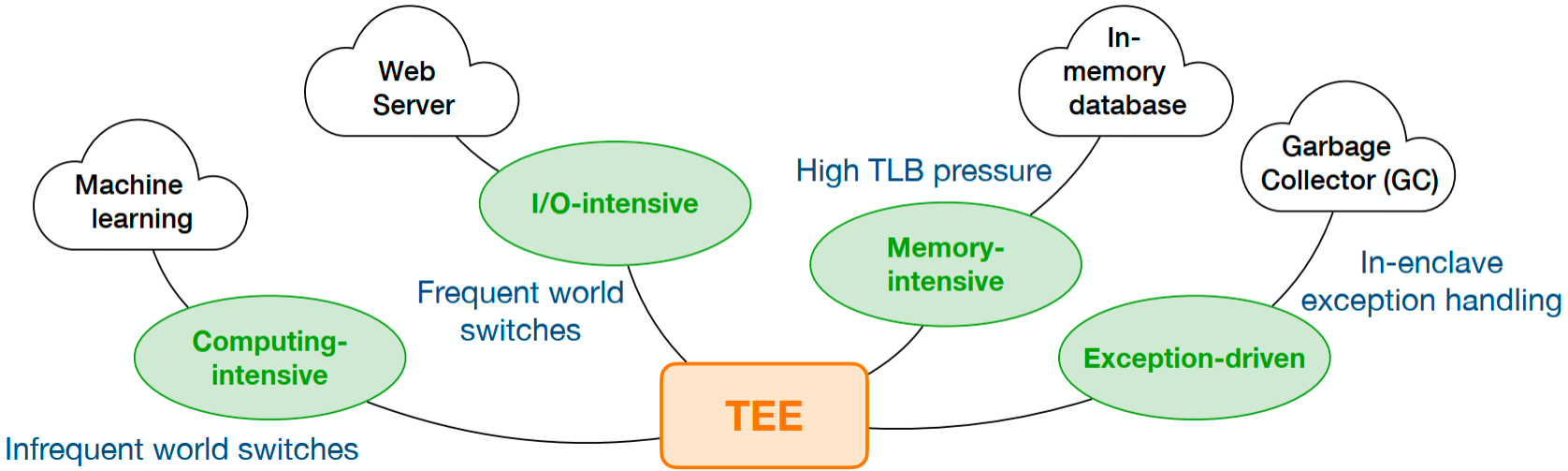
远程证明用来鉴别TEE平台和Enclave身份，确认被授权的代码运行在TEE上



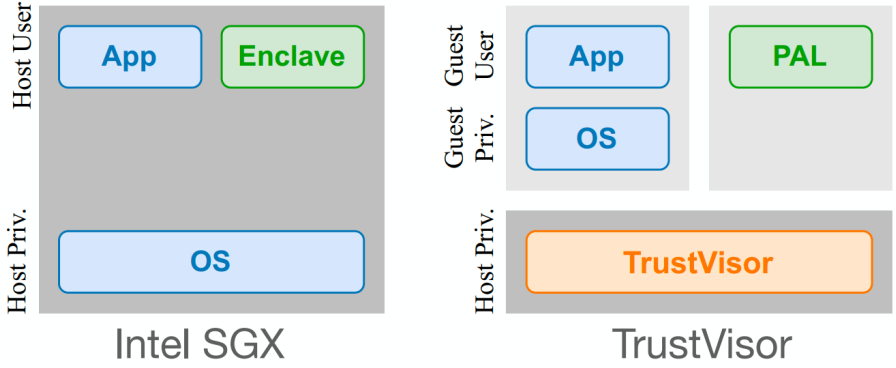


灵活的TEE运行模式

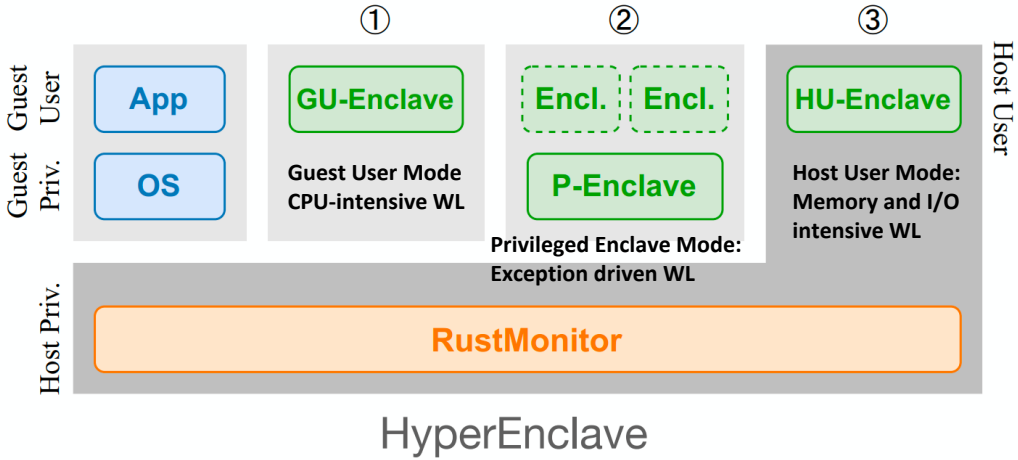
- TEE 需要提供更灵活的运行模式满足不同属性的应用场景



灵活的TEE运行模式



现有TEE如SGX，仅能提供用户态运行模式



HyperEnclave 提供3种Enclave模式

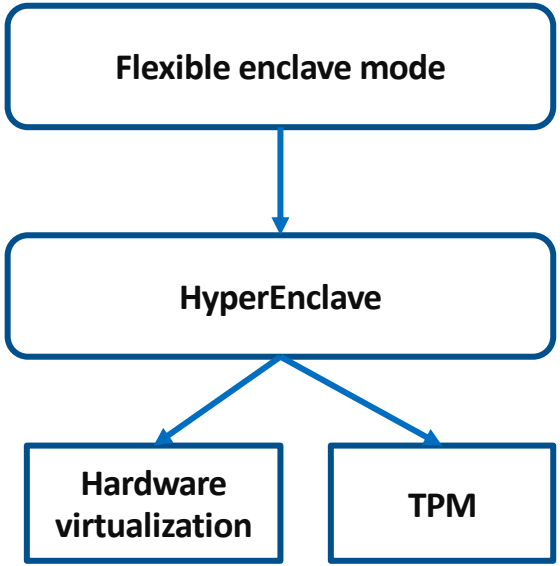
HyperEnclave SDK

- 兼容SGX SDK API
- 默认支持：
  - Rust SGX SDK
  - Occlum LibOS
- 不修改或少量修改即可运行已有SGX应用

Occlum

总结

- 硬件依赖最小化，支持多平台
  - 硬件虚拟化(隔离) + TPM(可信)
- 易于开发
  - 兼容现有SGX工具链和生态
  - 不修改或少量修改即可运行现有SGX应用
- 支持灵活的运行模式
  - 更好的满足TEE应用对安全与性能的不同需求



交流合作

- 期待与产业界，学术界伙伴们，共建信创TEE生态
- We are hiring ! 系统安全方向，虚拟化，内核等

非常感谢您的观看

蚂蚁集团 ANT GROUP | 支付宝 | DataFun.