OpenGCC

边缘计算 Edge Computing CONSORTIUM

CIEC2023

2023计算产业生态大会

COMPUTING INDUSTRY ECOSYSTEM CONFERENCE 2023

凝心聚力 共赢计算新时代

北京香格里拉饭店

2023.12.13-14

OpenGCC

边缘计算 Edge Computing CONSORTIUM

CIEC2023

机密计算：现状与展望

冯登国

边缘计算产业联盟ECC

研究背景

数据是数字时代的基础性战略资源与关键性生产要素。随着国家数据战略的深化，数据要素呈现出加速整合与互联互通的趋势，数据安全需求凸显

2020.04
国务院在要素市场化配置体制意见中明确提出加快培育数据要素市场

2021.03
《国家十四五规划和 2035 年远景目标纲要》“推动数据赋能全产业链协同转型，同时强化数据资源全生命周期安全保护”

2021.05
国家发展改革委、中央网信办、工业和信息化部、国家能源局联合印发（发改高技〔2021〕709号）文件，东数西算工程正式启动

2022.10
国务院关于数字经济发展情况的报告，指出要全面加强网络安全和数据安全保护，推动构建网络空间命运共同体

《数据安全法》、《个人信息保护法》于2021年落地实施，如何平衡数字经济发展与重要数据安全、个人隐私保护已成为迫在眉睫的现实挑战

数据安全法
2021年9月1日起实施

个人信息保护法
2021年11月1日起实施

当前数据安全呈现出三大主流发展方向

数据传输安全

- ✓ 数据通信安全，已有很多成果，相对比较成熟
- ✓ 但仍需创新发展，以适应技术进步和实际应用需求

数据存储安全

- ✓ 数据资产安全，已有很多成果，相对比较成熟
- ✓ 但仍需创新发展，以适应技术进步和实际应用需求

数据使用安全

- ✓ 运行态数据安全或流动数据安全，发展中遇到的一个难题，也是一个前沿发展方向
- ✓ 需要加快创新研究和实用化进程

数据使用安全需求迫切

云计算、大数据等新型应用场景的发展迫切需要对使用中的数据进行保护

- 针对云应用的每种攻击模式（包括虚拟机逃逸、容器逃逸、固件损坏和内部威胁）都使用了不同的攻击技术，但它们的共性是被攻击对象都是使用中的代码或数据
- 传统的保护数据在传输或存储中的安全措施无法处理云场景下敏感数据在使用中的数据安全

移动、物联网等设备数量的不断扩大迫切需要对使用中的数据进行保护

- 对于在移动设备、边缘设备和物联网设备上进行的数据存储和处理，实际进行数据处理的地方往往在远端且通常是难以确保其安全性的地理位置，因此，在执行过程中对数据和应用程序提供保护变得越来越重要
- 由于个人信息存储在移动设备上，移动设备制造商和操作系统提供商需要证明：它们访问个人数据的过程是受到保护的，即确保在共享和处理个人信息的过程中，设备供应商或第三方无法观察到这些个人数据，同时还要确保这些安全防护符合监管要求

数据使用安全受到高度关注

工业界和学术界已发现了多起影响深远的基于内存数据的攻击手段，这些攻击都极大地增加了人们对使用中的数据安全的关注

- 2017年黑客利用名为Triton的恶意工具攻击了位于沙特的一家炼油厂，致使其紧急关闭，分析人员在其中发现了从内存中提取用户口令或其它认证凭据的恶意程序，其目标是关闭工业控制系统的正常服务功能并对其造成物理损坏
- 以熔断（Meltdown）和幽灵（Spectre）为代表的利用CPU微架构漏洞的侧信道攻击，打破了操作系统内核与用户层、应用和应用之间的隔离

2021年，一项全球范围的有关数据隐私保护和安全调研表明（这项调研是由Futurum Research和IBM合作进行的，涉及360多位具有影响力的专业人员）

- 77%的企业认为，传统的安全模型不再适用于如今的计算环境
- 94%的企业认为，数据在使用中所受风险越来越高，必须受到保护
- 92%的企业认为，云服务提供商需要从技术上为客户提供无法访问其机密数据的有效保证

数据使用安全是当前数据安全中最为薄弱的环节

数据保护通常涉及数据的3种不同状态

- ✓ 传输时的数据（data at transit），其安全保护措施主要有加密、隐藏、SSL/TLS、IPSec、VPN和HTTPS等
- ✓ 存储时的数据（data at rest），其安全保护措施主要有加密、访问控制、安全数据库、数据容灾备份等
- ✓ **使用中的数据**（data in use），其安全保护包括其在内存、处理器中进行计算时的形态的机密性和完整性保护

数据使用安全：最为核心的技术是密态计算技术

- **机密计算（CC），+可信执行环境（TEE）**
  - ✓ 性能高，但可信赖性有待于提高，一种现实的密态计算技术
- **同态加密（HE）**
  - ✓ 可信赖性高，性能低~高，而全同态加密离实用化还有距离，一种理想的密态计算技术
  - ✓ 基于机密计算的全同态加密（FHE）方案设计和实现是一个重要研究方向
- **安全多方计算（MPC）**
  - ✓ 可信赖性高，性能低~中，有待于提高
- **联邦学习（FL），+差分隐私（DP）**
- **外包计算**
- **零知识证明**
- **密文检索**

……

机密计算定义（Confidential Computing）

CCC定义：机密计算是通过在基于硬件的可信执行环境(Trusted Execution Environment，TEE)中执行计算来保护使用中的数据，TEE则是提供一定级别的数据完整性/机密性和代码完整性保证的环境

IBM定义：机密计算是一种云计算安全技术，它在处理过程中将敏感数据隔离在受保护的CPU飞地（Enclave）中

微软定义：云计算中的下一个重大变革，对现有的静止和传输中数据加密的基线安全保证的扩展，对计算过程中的数据进行的硬件加密保护

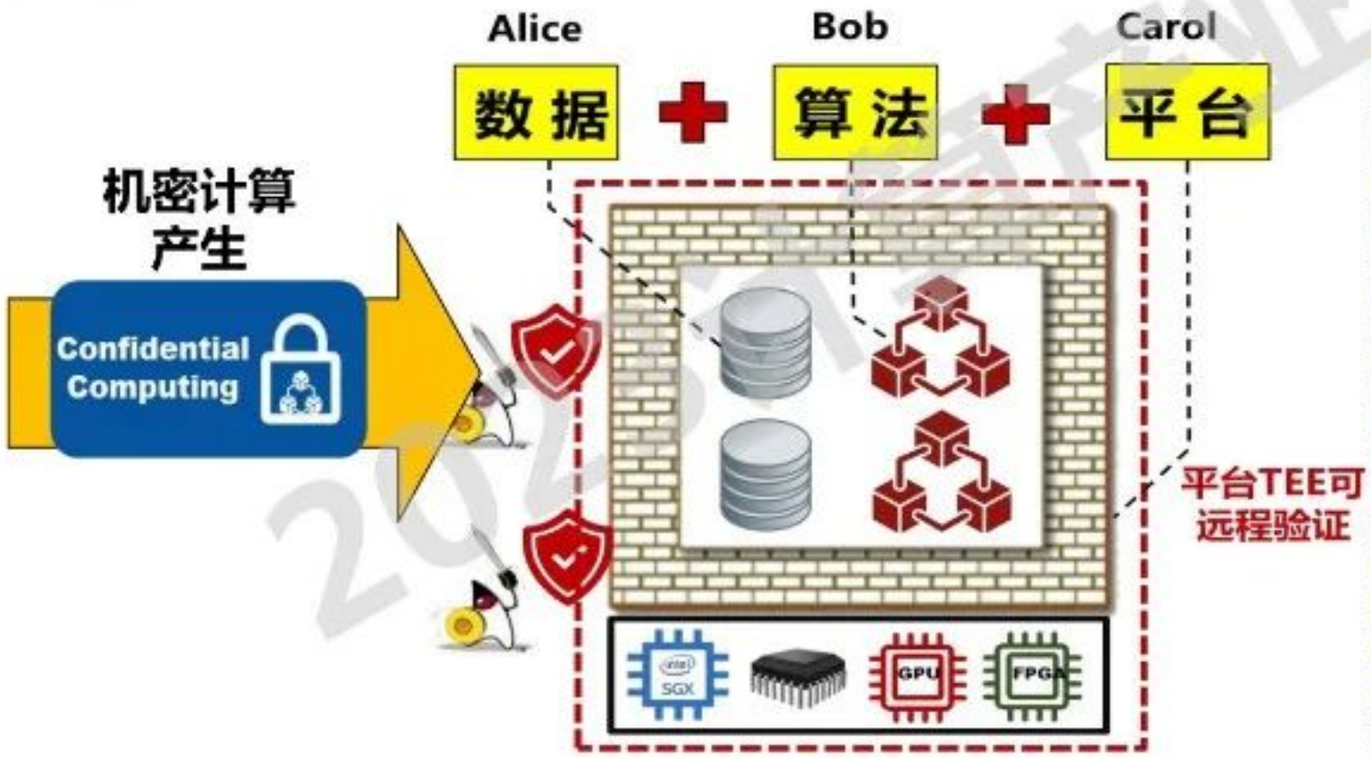
IEEE定义：机密计算使用基于硬件的技术，将数据、特定功能或整个应用程序与操作系统、Hypervisor或虚拟机管理器以及其他特权进程相互隔离

我认为：机密计算是一种**保护使用中的数据安全**的**计算范式**，它提供硬件级的系统隔离，保障数据安全，特别是多方参与者下数据使用中的安全

机密计算是目前最为现实的一种数据使用安全技术，本质上是一种密态计算技术

安全问题

- 如何确保海量数据应用场景下“数据可用不可见”，提高数据共享流通安全性
- 如何有效保障多方参与者(数据所有者、平台所有者、数据使用者等）相关利益和数据隐私
- 能否信任机密计算平台TEE硬件以及系统软件栈，保障数据和程序的机密性/完整性



主要特点

- 基于硬件信任且可远程证明和验证的可信计算方式
- 数据、算法、平台三者完全独立的安全计算模式
- 与可信计算、隐私计算形成安全互补
- 学科交叉性强，涵盖体系结构、系统安全、密码技术、人工智能等领域，需要协同创新发展

机密计算研究现状

机密计算的研究主要包括两个方面

- ✓ 一是自身研究，包括信任模型、安全架构、安全机制、TEE构建技术、平台安全服务框架等
- ✓ 二是应用研究，根据需求与使用特点，将机密计算应用分为系统与平台基础应用和技术领域结合应用两大类

机密计算应用

系统与平台基础应用 → 使用机密计算技术构建一个通用的隔离执行环境，作为机密工作负载与敏感数据保护的基础系统与平台来应用，可以为各种安全敏感应用提供机密计算功能，能够适配不同的硬件设备与平台环境，**典型代表**如**机密服务器、机密虚拟机、机密容器等**

技术领域结合应用 → 深入分析机密计算的功能特点与优势，将其与其它技术或者应用领域进行深度结合，开发一些新的计算模式，支撑一些新的安全服务，提升计算或者交互的安全与效率，同时使用户能对其计算环境和敏感数据保持控制权，**典型代表**如**机密人工智能、机密多方计算、机密区块链、机密数据库**等

1、信任模型

目前机密计算信任模型扩展研究，主要集中在以下两个方面

- ✓ 一是解耦CPU厂商与平台的强绑定信任建立通用证明框架
  - 解耦机密计算证明服务，建立不依赖于可信第三方的TEE间证明框架，消除机密计算硬件供应商的限制，从而解耦CPU厂商与平台的强绑定关系，实现不同技术路线TEE（Intel SGX， AMD SEV，ARM Trustzone等）之间相互认证。代表方案有Opera、Mage、Apache Teaclave等
- ✓ 二是面向不同TEE架构，建立机密计算应用的兼容性信任
  - 通常采用虚拟化技术、二进制兼容等技术路线，实现TEE的跨硬件平台的兼容移植、安全迁移。例如：vSGX方案(采用虚拟化技术在AMD SEV架构上运行SGX程序)，还有谷歌Asylo项目、亚马逊Nitro Enclaves等

2、安全架构

- **现有的机密计算安全架构根据其安全边界和受保护对象，可分为以下四种类型**
  - ✓ 系统级TEE安全架构
  - ✓ 应用级TEE安全架构
  - ✓ 异构TEE安全架构（外设TEE保护安全架构）
  - ✓ 密钥保护安全架构

- 就保护边界而言，系统级TEE的安全边界大于应用级TEE，攻击面也要相应的更大一些
- 就保护对象而言，系统级/应用级TEE都是保护程序代码执行环境，异构TEE保护的是GPU、FPGA等异构外设计算环境，密钥保护架构则是保护平台的机密数据

典型机密计算技术路线的安全能力比较

比较项	Intel SGX	Intel TDX	AMD SEV	ARM TZ	ARM CCA	KeyStone
体系结构	X86	X86	X86	ARM	ARM	RISC V
系统保护层级	进程	虚拟机	虚拟机	进程/secure OS	虚拟机	进程/虚拟机
数据完整性	支持	支持	支持(嵌套分页)	支持(系统隔离分区)	支持(系统隔离分区)	支持(内存保护)
数据机密性	支持	支持	支持	不支持	不支持	支持(内存保护)

- **目前机密计算技术路线中X86体系相对比较成熟，ARM和RISC V体系也在跟进发展，系统级“飞地”方案受到了更多关注，是未来重要发展方向**
  - ✓ 进程级Enclave方案虽然TCB小，但存在大量侧信道攻击面，系统级Enclave方案TCB较大，对机密计算应用的兼容性，扩展性支持更好
  - ✓ 这些代表性技术路线安全能力上差异较小，在机密性和完整性保护实现技术方面存在较大差异
  - ✓ 机密计算应用方面，X86技术路线重点应用在云服务器，而ARM、RISC V技术路线侧重于嵌入式和移动智能终端，但ARM 64位机密计算服务器也在不断改进

3、安全机制

- **机密计算安全机制主要包括：平台安全启动、度量、证明、隔离、可信存储、内存加密等，目前已有很多成熟方案**

4、TEE构建技术

现有的机密计算TEE构建技术根据其核心组件的性质，可分为以下四类方案

1. 基于离散芯片的TEE构建方案

- 该方案构建的可信执行环境位于一个独立的硬件安全芯片或者安全协处理器中，与主机环境是物理隔离的
- 代表性工作有TPM/TCM可信芯片、安全协处理器等

2. 基于指令集扩展的TEE构建方案

- 该方案构建的可信执行环境与主机环境使用相同的物理处理器，但是通过对处理器指令集进行扩展，可以确保两个环境之间的隔离
- 代表性工作有ARM TrustZone/CCA、Intel SGX/TDX等

3. 基于软件的TEE构建方案

- 该方案不再依赖硬件安全特征来保护可信执行环境，而是依赖系统软件或者虚拟化模块来维护类似的安全性与隔离性，灵活性增强，安全性相对减弱
- 代表性工作有VSM、open-SGX模拟器等

4. 基于异构可信的TEE构建方案

- 该方案将可信执行环境的边界从通用CPU处理器扩展到GPU、FPGA、SSD、NPU等异构设备，使得安全隔离保护的范围得到扩展，计算过程不仅受到CPU TEE的保护，还受异构TEE（如GPU TEE）的保护
- 代表性工作有HETEE、SGX-FPGA、IceClave、TNPU等

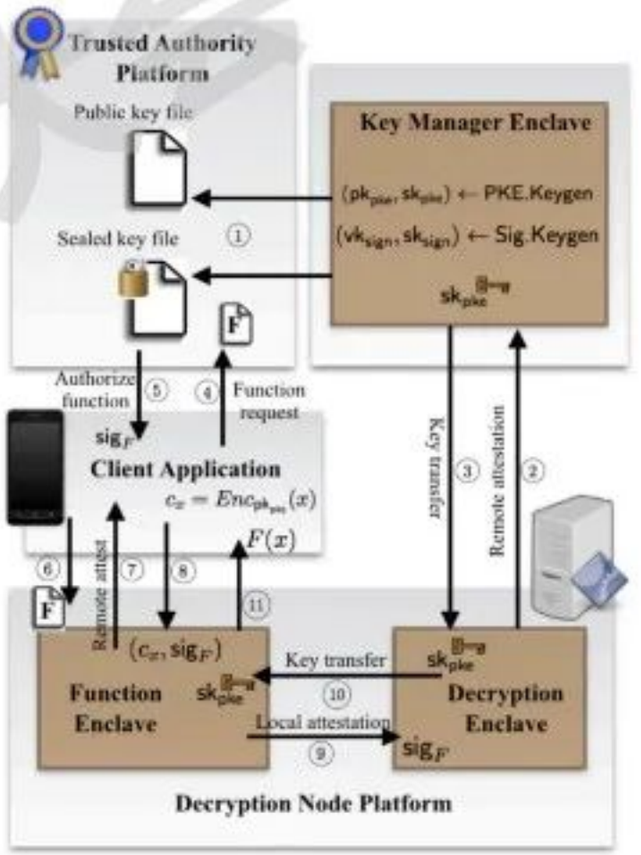
5、平台安全服务框架

目前的机密计算平台安全服务框架主要是在基础机密计算安全服务上增强应用安全性，扩展机密计算平台的易用性和兼容性，形成通用的服务框架标准

基础安全服务	安全性增强	机密云服务	框架标准
• 密钥管理 • 远程证明服务 • 完整性和信任 • 安全存储	• Aditya等人提出一种TEE应用**安全编程模型JE**，通过注释Java程序编译安全飞地应用程序 • Fortanix、MesaTEE使用**内存安全语言Rust**重写SGX SDK来增强机密计算应用安全性	• 谷歌云(Google Cloud)推出**机密虚拟机服务**，保障虚拟机用户和内存数据的机密性 • Anjuna等多项目整合了包括AWS、Azure等公/私有云的机密计算服务，增强机密计算应用**跨平台部署能力** • 国内阿里云等已开展**机密计算云服务商业化**，为云用户提供更高等级数据保护能力	• 国内也有机构正在开展机密计算平台服务框架标准的制定

6、应用实例

- **可将“可信执行环境”视为“困难问题”。例如，如果有一个对称密钥在SGX Enclave中、永远不会泄露，而且Enclave中只包含加密代码、没有解密代码，我们就得到了一个单向函数：可以加密、不能解密**
  - ✓ IRON方案
    - 基于Intel SGX构建函数加密，高性能
    - 利用普通的公钥密码算法，基于SGX安全假设
    - 实现函数加密功能
  - ✓ PoS方案
    - 基于Intel SGX构建公钥密码和标识密码，高性能
    - 利用对称密码算法和HASH算法，基于SGX安全假设
    - 实现类似于“公钥密码”和“标识密码”功能



IRON方案

- **当然，这些方案有效的前提是：“可信执行环境”真的做到安全、万无一失**

机密计算未来展望

一是机密计算实用化研究更加重要

- 机密计算的基础方法和关键技术的实用化和创新研究十分重要，可为机密计算的发展和进步提供理论基础和科学方法
- 机密计算的理念必将导致传统的安全体系结构、安全模型、安全策略、安全措施等的变革和创新，也必将催生一批新型安全技术
- 在机密计算环境中，安全体系结构与模型、安全机制的轻量化设计及其安全性证明、侧信道防护方法与形式化分析、安全监管策略与方法等都是值得进一步研究的问题
- 应积极推进机密计算技术创新研究，进一步发展和完善机密计算技术体系

机密计算未来展望

二是机密计算标准化需求更加迫切

- 机密计算缺乏标准的实现方法，不同公司实现方式不一样，所以，机密计算应用会使专业安全人员面临技术困惑，这也是CCC开发统一开源SDK的因素
- 机密计算标准应包括：算法与协议标准，应用接口规范，软硬件加速技术规范，平台功能规范，平台服务框架标准，安全管理框架标准，基于机密计算的应用标准，检测评估标准
- 应大力推进机密计算标准规范的研究与制定，加快构建机密计算标准体系

机密计算未来展望

三是机密计算协同发展更加紧密

- 协同发展、交叉研究是机密计算领域的一大特色，需要机密计算硬件(如CPU、FPGA)、密码技术（如SM2/3/4、同态加密）、隐私机制（如差分隐私、联邦学习）、安全协议(如TLS、安全多方计算）、可信计算机制(如硬件信任根、远程证明)、VM和OS安全、容器和微服务安全等的协同支持才能变得更有效、更安全
- 密码技术有很多，在机密计算环境中，尤其要关注新形态密码技术（如同态加密、可搜索加密、函数加密、属性加密）和抗量子公钥密码技术（如NIST推荐的CRYSTALS-KYBER、CRYSTALS-Dilithium)
- 应强化不同领域学者的深度开放合作研究，积极构建机密计算协同发展机制

机密计算未来展望

四是机密计算应用将更加深入

- 机密计算依托基于硬件支持的可信执行环境（TEE）构建隔离的“安全飞地”，为敏感数据和代码执行提供安全保障，是计算效率约束条件下解决“使用中或运行态或流动”数据安全的重要而现实的技术途径
- 机密计算试图破解数据保护与利用之间的矛盾，可应用于电子政务的跨部门数据安全共享、金融行业的联合风控、医疗领域的医学、药物和基因研究、商业领域的联合营销等
- 机密计算应用仍存在很多问题，如跨场景、多样性、大规模、高安全，需加强机密计算应用研究以及基于机密计算的应用解决方案研究
- 应加速“产学研用”深度融合，全力打造具有韧性的机密计算应用生态体系