



CIEC2023

# 网络空间的信任构建与安全计算的演进

沈晴霓

北京大学教授， ECC安全工作组主席

# 目录

01 安全与可信关系内涵

02 网络空间的信任构建

03 安全计算的演进历程

04 未来发展趋势与展望





01

---

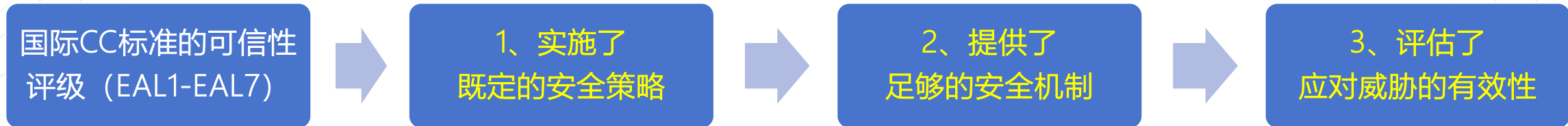
# 安全与可信关系内涵



# 安全与可信概念如何区分？

- ✓ **安全**是指采取技术和管理的安全保护手段，保护软硬件与数据不因偶然的或恶意的原因而遭到破坏、更改、暴露。
- ✓ **可信**是指如果针对某个特定的目的，实体的行为与预期的行为相符，则称针对这个目的，该实体是可信的。

| 区别        | 分级     | 声明方      | 声明依据                 | 声明结论 |
|-----------|--------|----------|----------------------|------|
| <b>安全</b> | 只分是与否  | 系统/产品提供方 | 基于系统/产品开发的安全功能作出的断言  | 绝对   |
| <b>可信</b> | 可分不同等级 | 系统/产品评估方 | 基于系统/产品安全测评相关证据作出的仲裁 | 相对   |





02

---

# 网络空间的信任构建

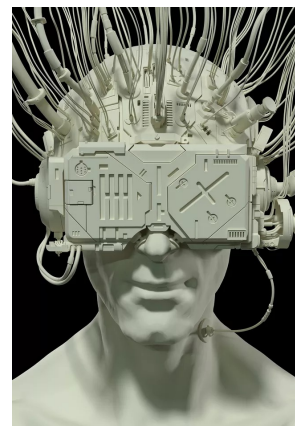


# 网络空间的组成要素是什么？

互联网是20世纪人类最伟大的发明之一

网络空间一词源自美国1984年的科幻小说《神经漫游者》

网络空间已经成为与陆、海、空、太空并列的第五空间



Neuromancer

网络空间就相当于一个国家具有主权的物理空间，涉及四大要素：

- ① **领土**：网络平台（包括：互联网、4G/5G电信网、物联网、工业互联网，以及计算系统、控制系统、通信系统等）
- ② **人口**：用户（包括：网络平台上的各种用户等）
- ③ **资产**：数据（包括：网络平台自身运行及人机交互产生的大数据）
- ④ **政权**：管理活动（包括：网络平台上的系统管理、网络管理、用户管理、数据管理等相关的活动）

# 网络空间安全威胁有哪些？

## 黑客攻击

破解或破坏某个程序、系统及网络的黑客攻击行为

为了表达不满而未造成破坏性的攻击行为，不构成国家安全

窃取商业机密、扰乱国家政治、经济秩序的攻击行为，不同程度涉及国家经济/社会安全

## 网络犯罪

借助互联网进行的、有组织的犯罪活动

借助互联网实施的金融诈骗、音视频盗版等，及非法药物合成、提取和流转

借助互联网实施人口贩卖、濒危物种走私、洗钱等非法交易

## 网络恐怖主义

针对信息及计算机系统、程序和数据发起的恐怖袭击，影响到政府或社会利益

利用计算和互联网进行恐怖主义活动，以达到一定政治目的

互联网成为恐怖主义沟通交流、理念宣讲、人员招募和激进化培训的最重要场所

## 网络战

网络战的主体包括国家行为体，也包括非国家行为体

最大威胁是对军事设施直接打击；对金融、能源和交通民用设施攻击

网络间谍通过植入恶意软件从敌方获取情报；信息战通过信息披露来影响敌方思想和行为

## 信任的评估方 由谁来担任？

- 1、权威的可信第三方机构
- 2、对等的中间人或同行
- 3、用户自己

## 信任评估的依据 应该包括什么？

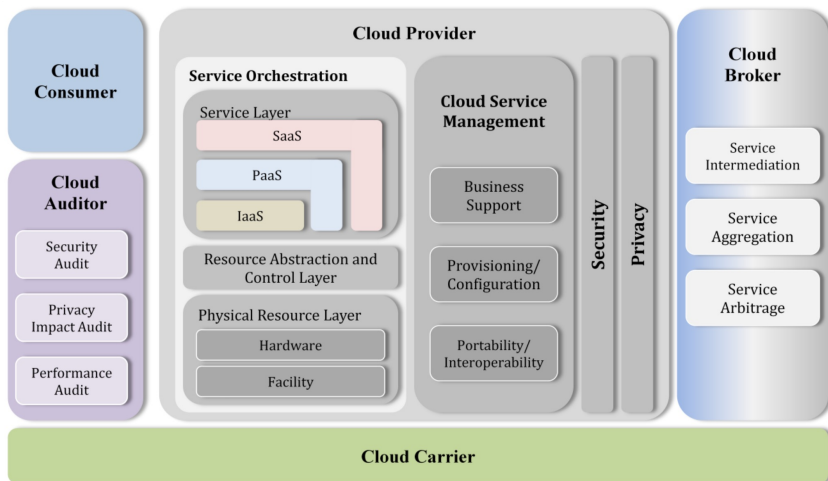
- 1、行为的合规性
- 2、行为的透明性
- 3、行为可追责性

## 信任的边界和 基本假设是什么？

- 1、信任的边界是指难以被攻击的安全硬件/软件
- 2、可证安全假设  
(安全模型、NP困难问题)

# 网络空间的信任如何构建?

示例：云服务的信任评估方来自：1) 云用户 (CC) 自己评估 (直接信任) 2) 由他人(CA, CB, Peers)评估 (间接信任)



CC: Cloud Consumer, CA: Cloud Auditor, CB: Cloud Broker, CSP: Cloud Service Provider

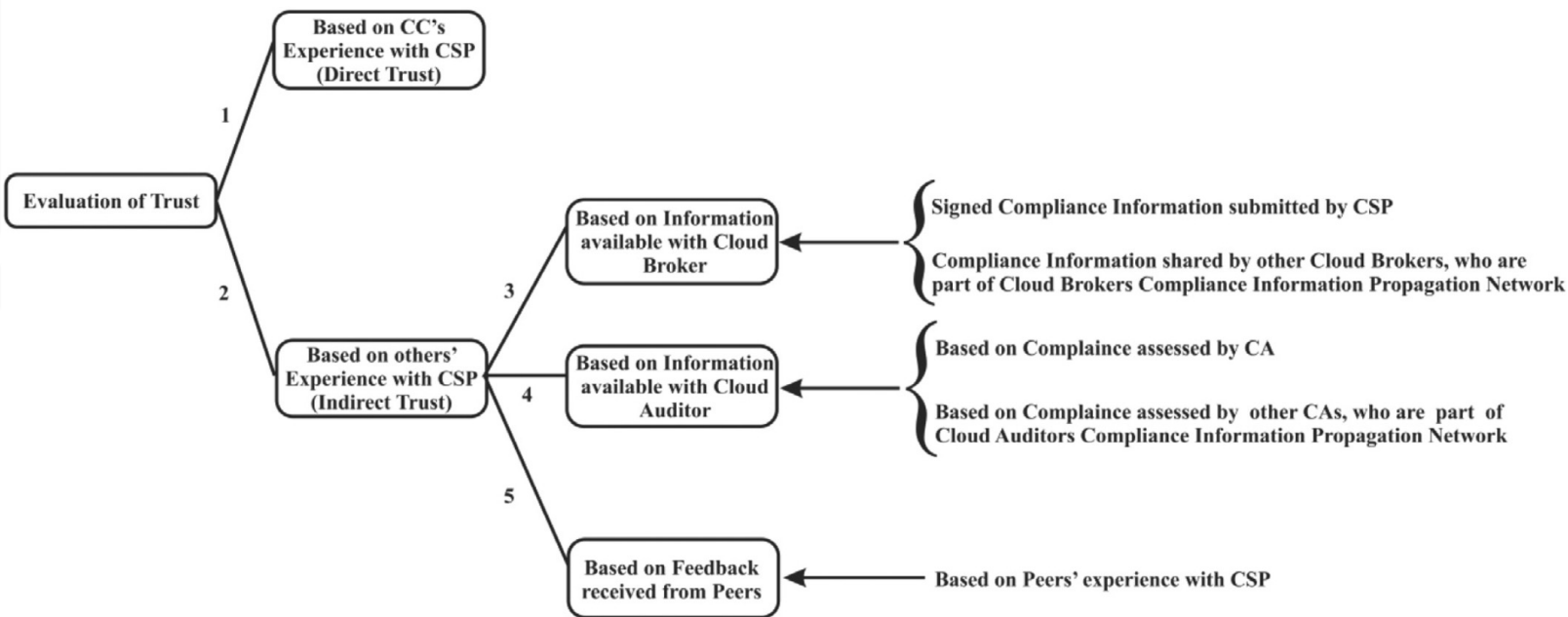


Fig. 7. Viewpoint hierarchy for trust evaluation.

【1】 Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers (Future Generation

# 信任的构建技术有哪些？

| 对比      | 可信计算基 (TCB)                        | 可信计算                               | 机密计算  | 隐私计算   |
|---------|------------------------------------|------------------------------------|---|--|
| 标准组织/联盟 | TCSEC/CC标准/等保                      | 可信计算工作组                            | 机密计算联盟  | Global Platform 联盟<br>隐私计算联盟                             |
| 技术支持    | 基于 <b>软件/硬件安全增强</b> （访问控制、沙箱隔离等）技术 | 基于 <b>密码学的硬件芯片</b> （TPM/TCM/TXT）设计 | 基于 <b>内存加密和内存保护机制的硬件指令</b> （SGX, TDX, SEV等）扩展 | 基于 <b>数据可用不可见</b> 的联邦学习、安全多方计算、可信执行环境等三大主流 <b>隐私计算技术</b> |
| 保护对象    | 计算机系统                              | 计算平台/网络连接                          | 应用程序代码及数据                                     | 大数据、AI模型   |
| 信任评估方   | 可信第三方机构                            | 用户/对等方                             | 用户  | 用户   |
| 信任评估依据  | 行为合规性                              | 行为合规性<br>行为透明性<br>行为可追责            | 行为合规性<br>行为透明性<br>行为可追责                       | 行为合规性<br>行为透明性<br>行为可追责                                  |
| 信任边界    | 安全硬件/软件                            | TPM/TCM/TXT硬件                      | CPU/GPU硬件                                     | 数据不出域-联邦学习<br>数据加密-安全多方计算<br>数据受硬件保护-可信执行环境              |
| 信任假设    | 安全模型                               | 密码学NP困难问题                          | 密码学NP困难问题                                     | 密码学NP困难问题  |



03

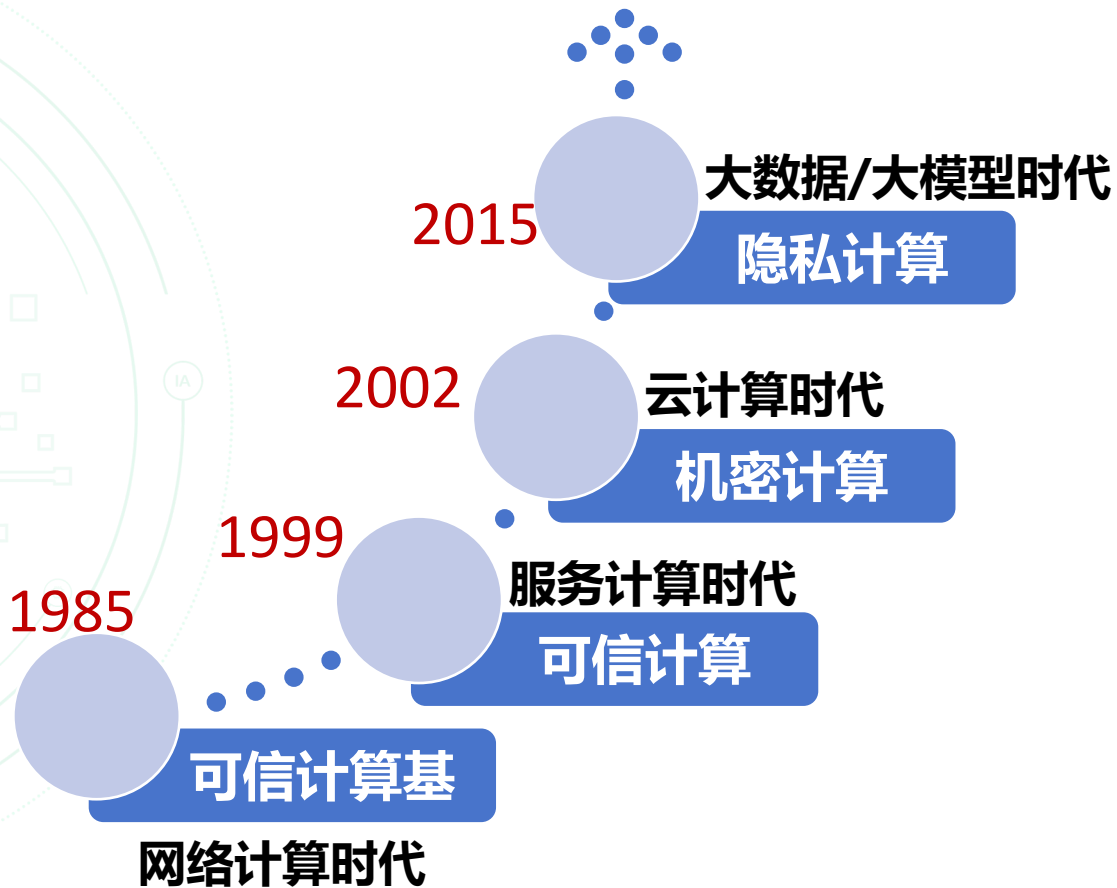
---

# 安全计算的演进历程

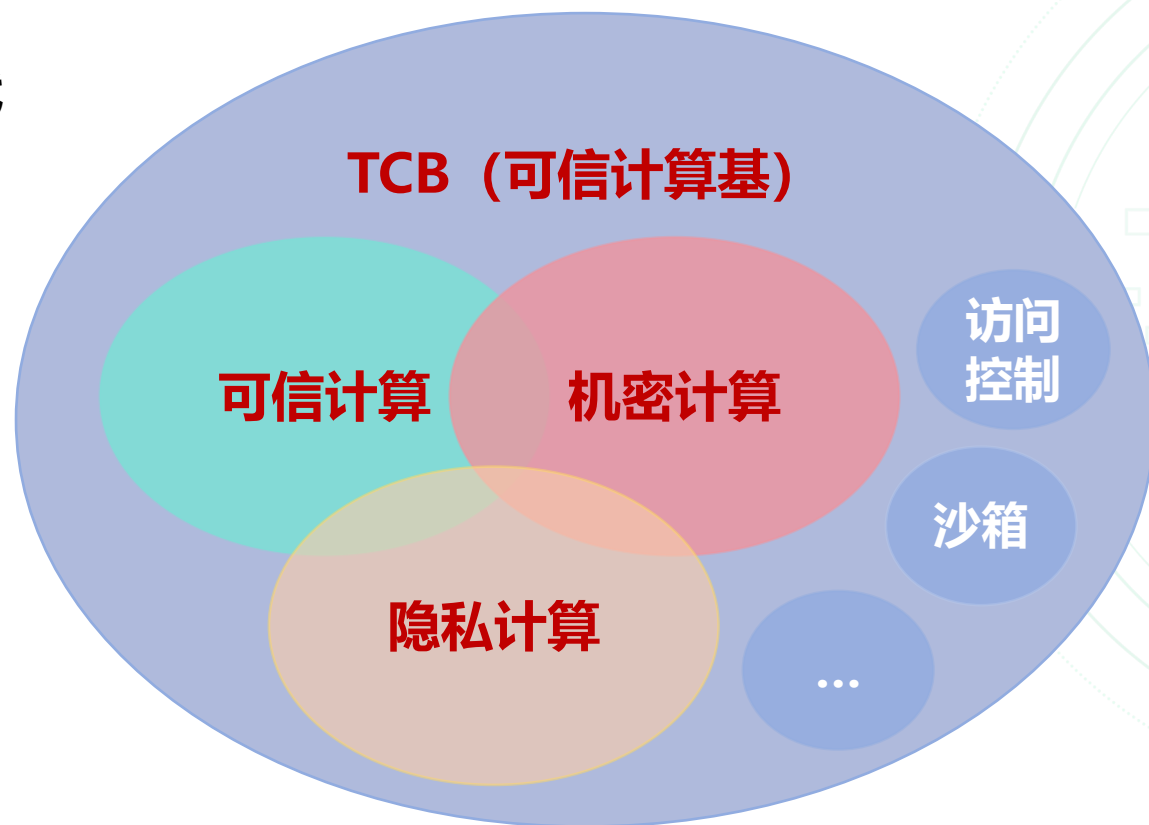


# 安全计算技术演进与关系如何？

## 安全计算技术的演进历史



## 安全计算技术间的关系



# 可信计算：核心功能有哪些？

基于密码学的安全芯片

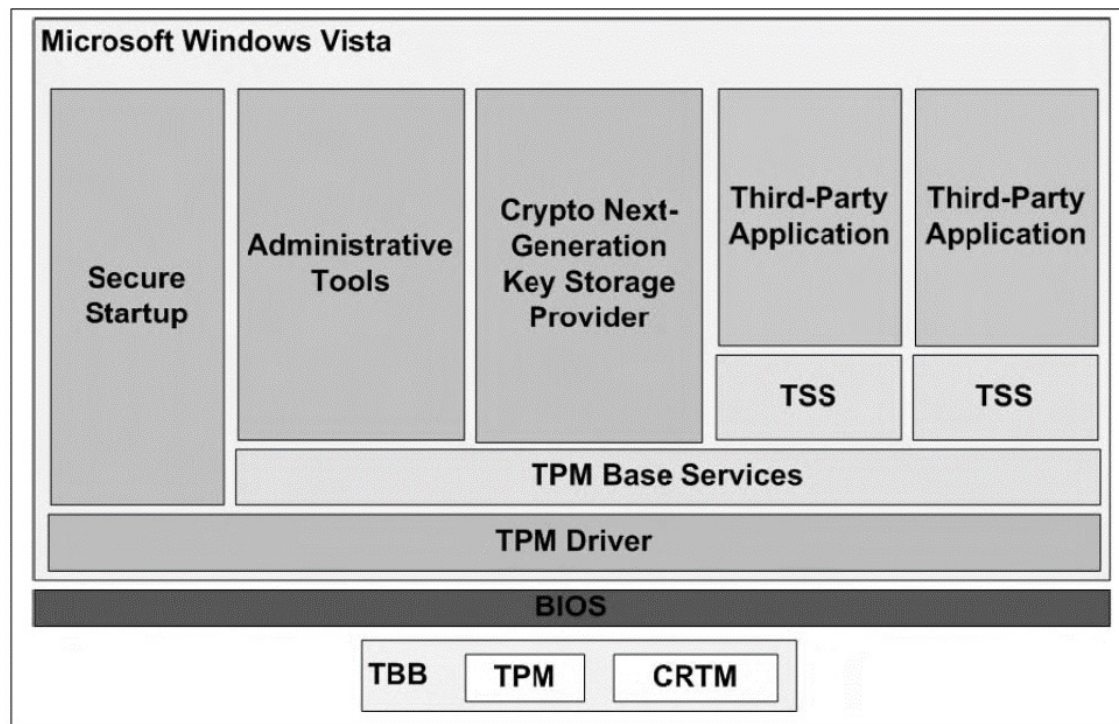
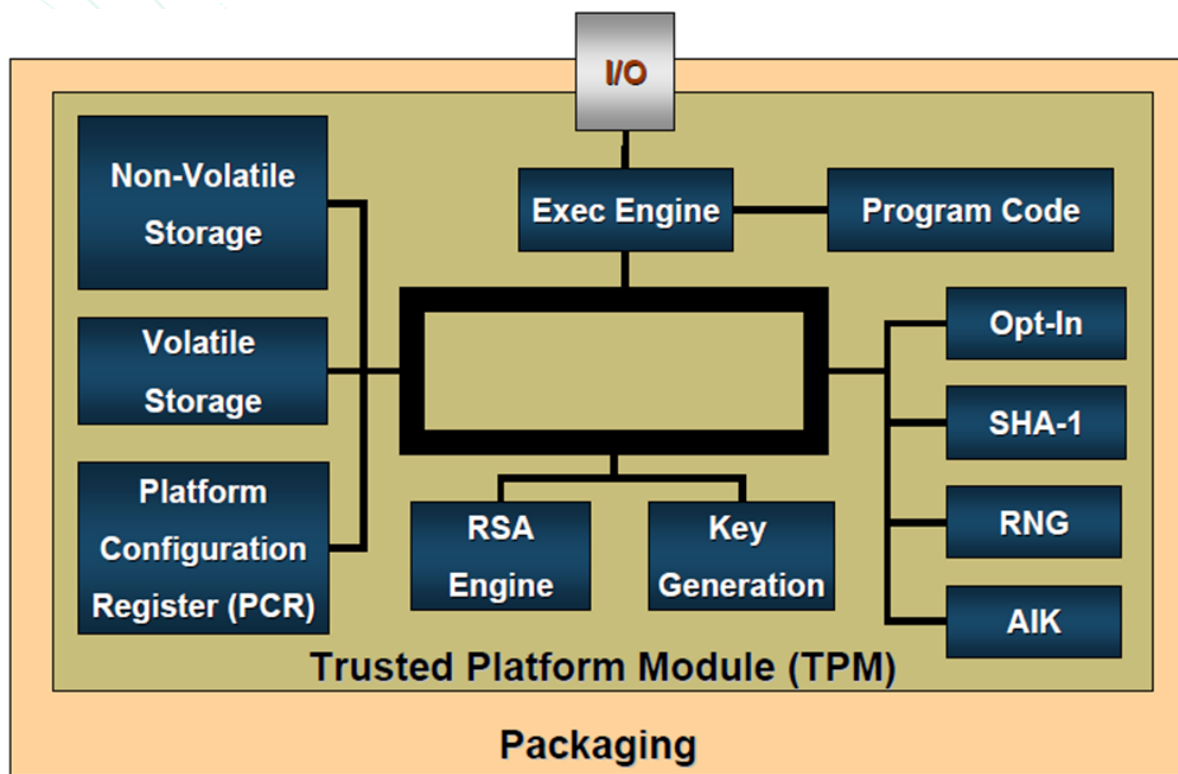
计算平台的信任链建立

平台完整性  
度量 and 报告

平台间的  
远程证明

数据保护/  
密钥管理

可信的  
网络连接



# 可信计算：芯片产品及应用如何？

**Infineon OPTIGA TPM:** 提供了硬件安全芯片，借助安全密钥存储和对多种加密算法的支持，用于嵌入式系统和工业设备中的可信计算和安全功能。 **保护嵌入式设备与系统的完整性和可靠性。**

**国民技术Z32H330TC可信计算芯片:** Z32H330TC是国际可信计算产业中**首个加载中国密码算法和国际密码算法的双算法可信计算核心产品**，已经**集成到微软Surface book中**，与Intel平台可信启动无缝配合。

**微芯Microchip ATECC系列:** Microchip的ATECC系列是一种**专为工业和嵌入式应用设计的安全芯片**，通过结合可信平台模块（TPM）和密码身份验证技术，为设备和系统提供安全的身份验证、数据保护和加密功能，广泛应用于工业自动化、物联网设备、智能家居、安全存储系统等领域。

**谷歌OpenTitan:** 是由**谷歌**发起的**可信根安全性项目**，旨在构建**基于开放标准的安全芯片设计**。它提供了一个完整的安全子系统设计，**可以在FPGA上实现**。OpenTitan使用FPGA提供的可编程逻辑和硬件资源来构建可信执行环境，保护关键数据和代码免受未经授权的访问和篡改。

# 可信计算：学术界进展如何？

| 方向       | 相关工作                                | 期刊/会议  | 简介   |
|----------|-------------------------------------|--|--|
| TPM的功能扩展 | SvTPM                               | TCC 2020   | 用SGX模拟实现TPM功能  |
|          | hTPM                                | CYSARM 2020  | 混合软件TPM和硬件TPM可实现TPM抗量子密码攻击                               |
|          | TPM-FAIL                            | USENIX Security 2022   | TPM可抵抗定时攻击、格攻击   |
| TPM的功能优化 | DAA                                 | TIFS 2021、AsiaCCS 2020   | 对TPM中DAA签名性能优化<br>对TPM 2.0 DAA机制的形式化分析                   |
|          | Remote Attestation                  | IET Inf. Secur. 2023、TDSC 2023和TDSC 2022、Comput. Secur. 2022、USENIX Security 2022、ACSAC 2022 | 基于硬件/软件实现的物联网设备远程证明、以及证据收集和扩展方案；<br>基于vTPM实现机密虚拟机远程证明方案等 |
| TPM的应用扩展 | simTPM                              | USENIX Security 2019   | TPM在移动设备上的应用   |
|          | iTPM                                | ISVLSI 2023  | TPM在智能电子设备上的应用   |
|          | TPM-Based Post-Quantum Cryptography | ARES 2021  | TPM在物联网设备上的应用  |

# 机密计算：为什么成立联盟？

Linux基金会于**2019年8月**成立机密计算联盟CCC，**致力于定义和加速机密计算的应用。**

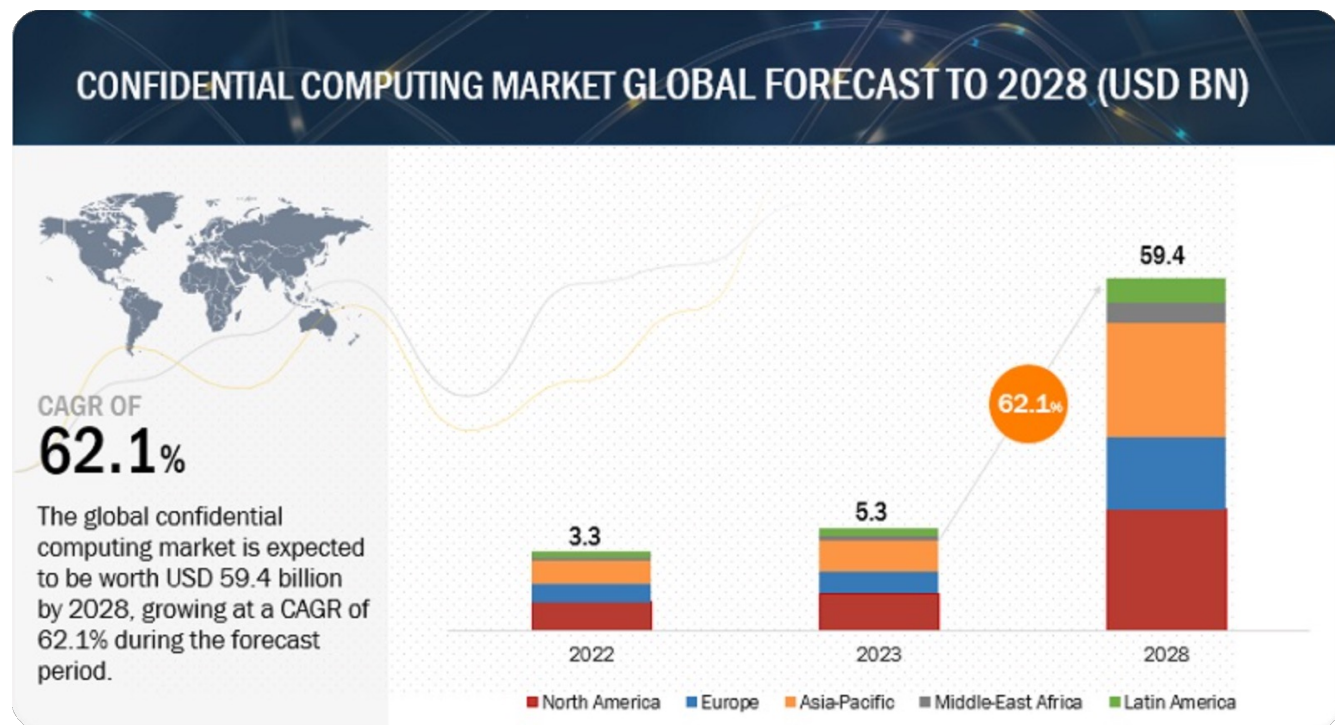
## Premier Members



## General Members



机密计算市场规模预计**将从 2023 年的 53 亿美元增长到 2028 年的 594 亿美元**，预测期内复合年增长率 (CAGR) 为 **62.1%**。



**目前许多科技巨头纷纷入局**，大力探索和开发机密计算。

- **微软Azure**：2017年增加了一项名为 Azure机密计算的安全功能，以确保数据在处理时能得到更多的控制。
- **阿里云**：亚太区首个推出基于SGX机密计算的云服务商。
- **谷歌云**：在Google Cloud Next 2020大会上，推出了一款机密虚拟机。

# 机密计算：关注重点？

在计算中，数据存在三种状态：静态存储、传输中和使用中，密码学普遍应用于提供数据机密性（方知未授权查看）和数据完整性（改制或检测未授权的更改）。**使用中的数据保护是机密计算联盟致力于解决的问题。** 工业界发生了几次备受瞩目的内存攻击，如Target breach和CPU侧信道攻击，**大幅度增加了对第三种状态的关注度。**

现有加密方案

机密计算



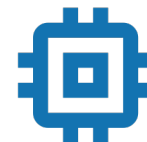
静态存储的数据

通过在存储之前对其进行加密或对设备本身进行加密来保护所存储的数据



传输中的数据

使用端到端加密或加密连接来保护网络之间传输的数据

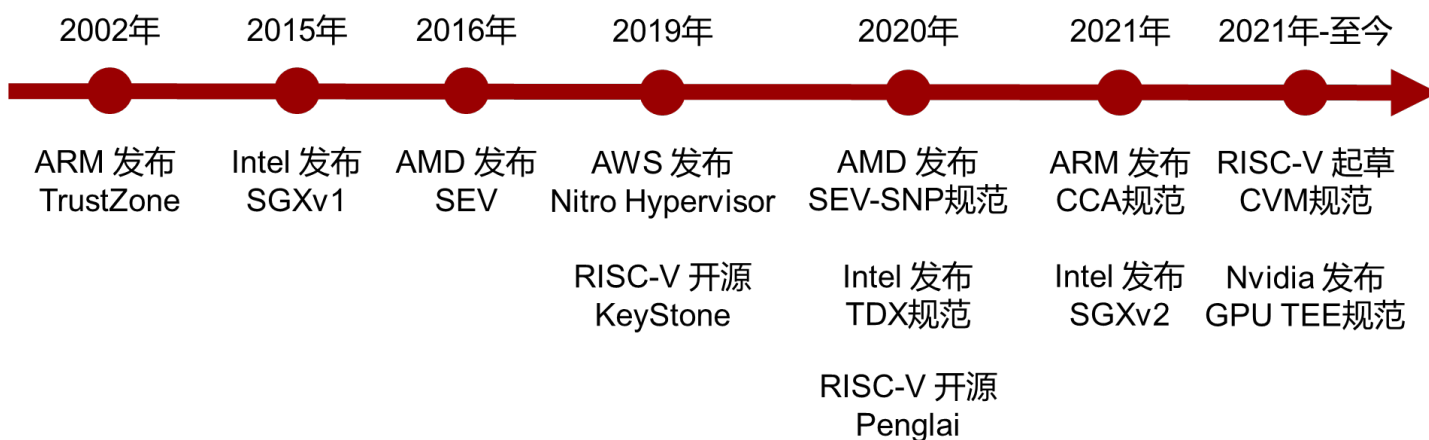
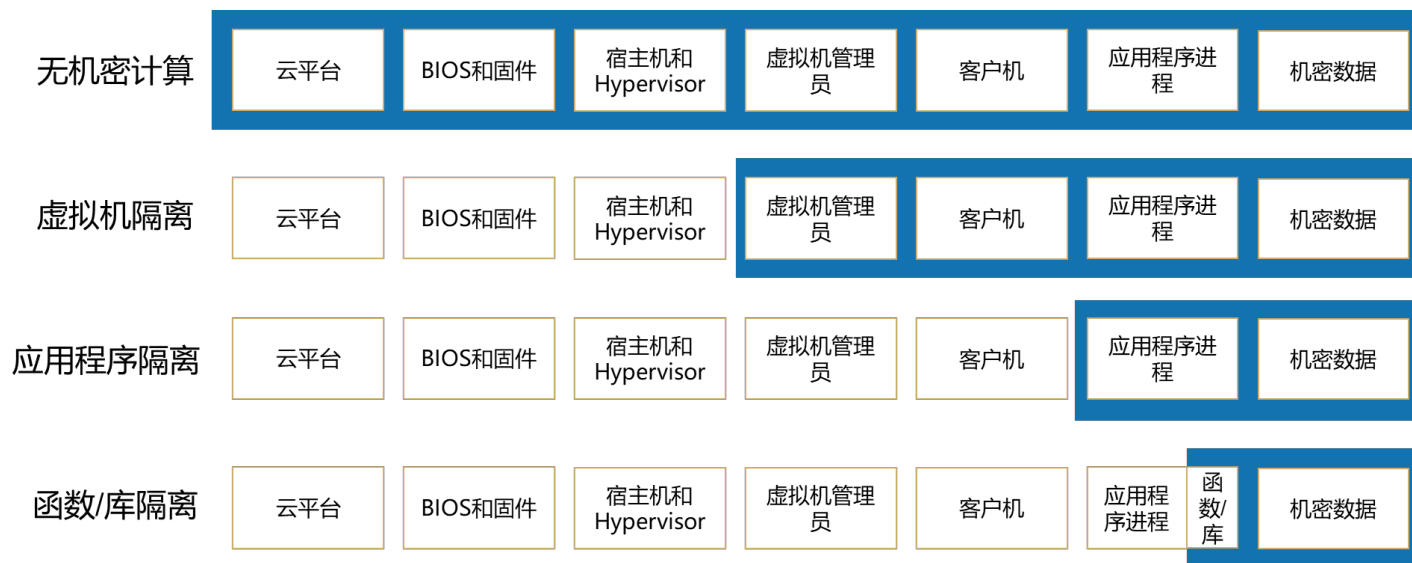


使用中的数据

当数据在 RAM 或处理器中用于计算时，通过加密来保护数据

# 机密计算：技术途径与产品演进？

机密计算是通过在**基于硬件的、经过验证的可信执行环境**中执行计算来保护正在使用的代码和数据，**实现虚拟机、应用程序或函数/库及数据的机密性和完整性保护。**



## 可信执行环境技术的发展历史

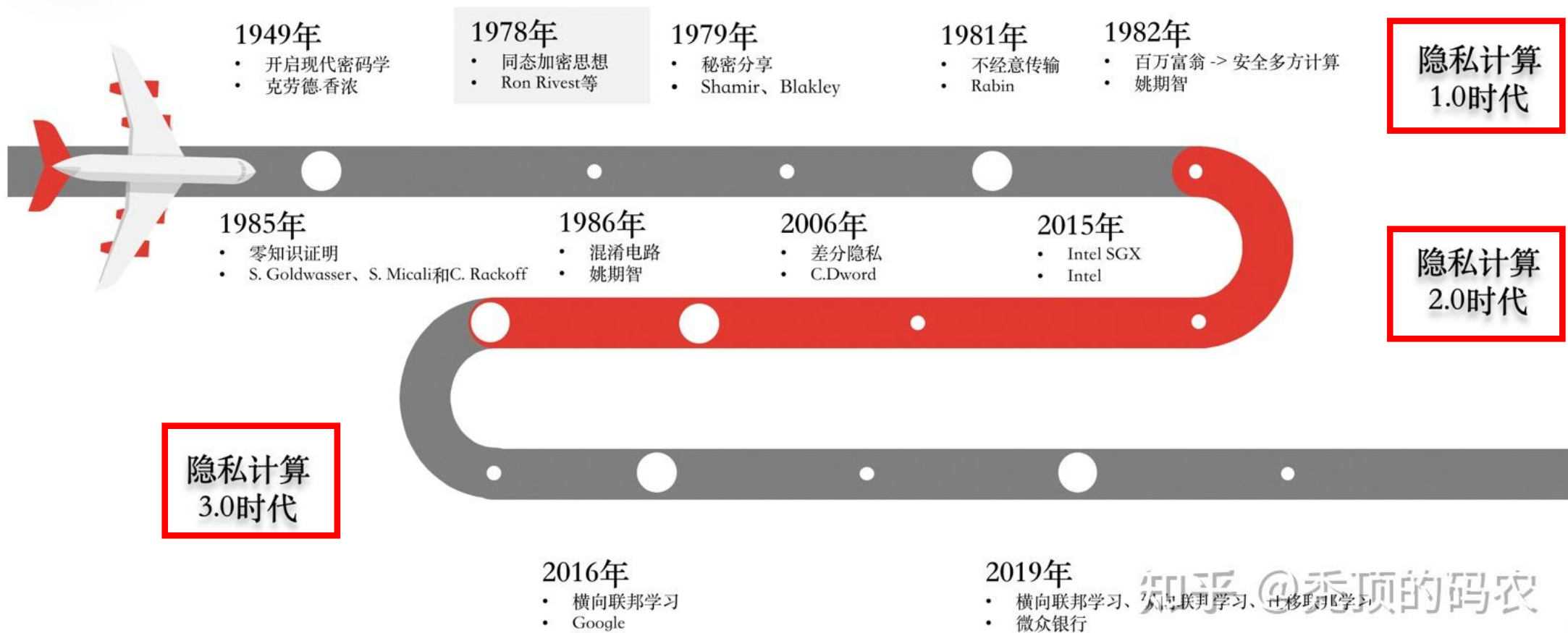
# 机密计算：开源项目及应用？

| 项目/产品   | 发布时间 | 开源 | 相关组织                        | 类型            | 优势                              | 应用                               |
|---|------|----|-----------------------------|---------------|---------------------------------|----------------------------------|
| Enarx <sup>1</sup><br><a href="https://enarx.dev/">https://enarx.dev/</a>   | 2019 | Y  | Red Hat                     | 运行时部署 (LibOS) | 基于WASM提供广泛的语言应用支持               | 应用于Azure和Equinix                 |
| Gramine <sup>2</sup> (曾命名: Graphene-SGX)<br><a href="https://gramineproject.io/">https://gramineproject.io/</a>                               | 2015 | Y  | Golem and ITL, Intel等成立的工作组 | 运行时部署 (LibOS) | 支持运行原生的、未经修改的 Linux 应用程序        | 应用于Eder Labs、京东云、腾讯云、德国国家数字健康机构  |
| Occlum <sup>3</sup><br><a href="https://occlum.io/">https://occlum.io/</a>  | 2020 | Y  | 蚂蚁集团                        | 运行时部署 (LibOS) | 飞地内隔离机制                         | 阿里云神龙云服务器                        |
| Open Enclave <sup>4</sup><br><a href="https://openenclave.io/sdk/">https://openenclave.io/sdk/</a>  | 2017 | Y  | 微软                          | 通用SDK         | 提供与特定供应商、服务提供商和操作系统选择无关的透明解决方案  | 与Agnostic Cloud Provider和Azure合作 |
| Nitro Enclave <sup>5</sup><br><a href="https://aws.amazon.com/ec2/nitro/nitro-enclaves/">https://aws.amazon.com/ec2/nitro/nitro-enclaves/</a> | 2020 | N  | AWS                         | 运行时部署 (VM)    | 提供无持久存储, 无交互式, 禁用外部网络的安全虚拟机     | Amazon EC2                       |
| Asylo <sup>6</sup><br><a href="https://asylo.dev/">https://asylo.dev/</a>   | 2018 | Y  | Google                      | 通用SDK         | 提供可移植的即用型容器、开源 API、库和工具         | google cloud                     |
| Veraison <sup>7</sup><br><a href="https://github.com/veraison">https://github.com/veraison</a>  | 2022 | Y  | ARM、EnactTrust、TPMdev       | 远程证明构建组件      | 提供具有一致性和便利性的证明验证服务构建方式          | 无                                |
| Veracruz <sup>8</sup><br><a href="https://github.com/veracruz-project/veracruz">https://github.com/veracruz-project/veracruz</a>              | 2022 | Y  | ARM                         | 运行时部署 (WASM)  | 用于在一组相互不信任个人之间定义和部署协作、隐私保护计算的框架 | 无                                |

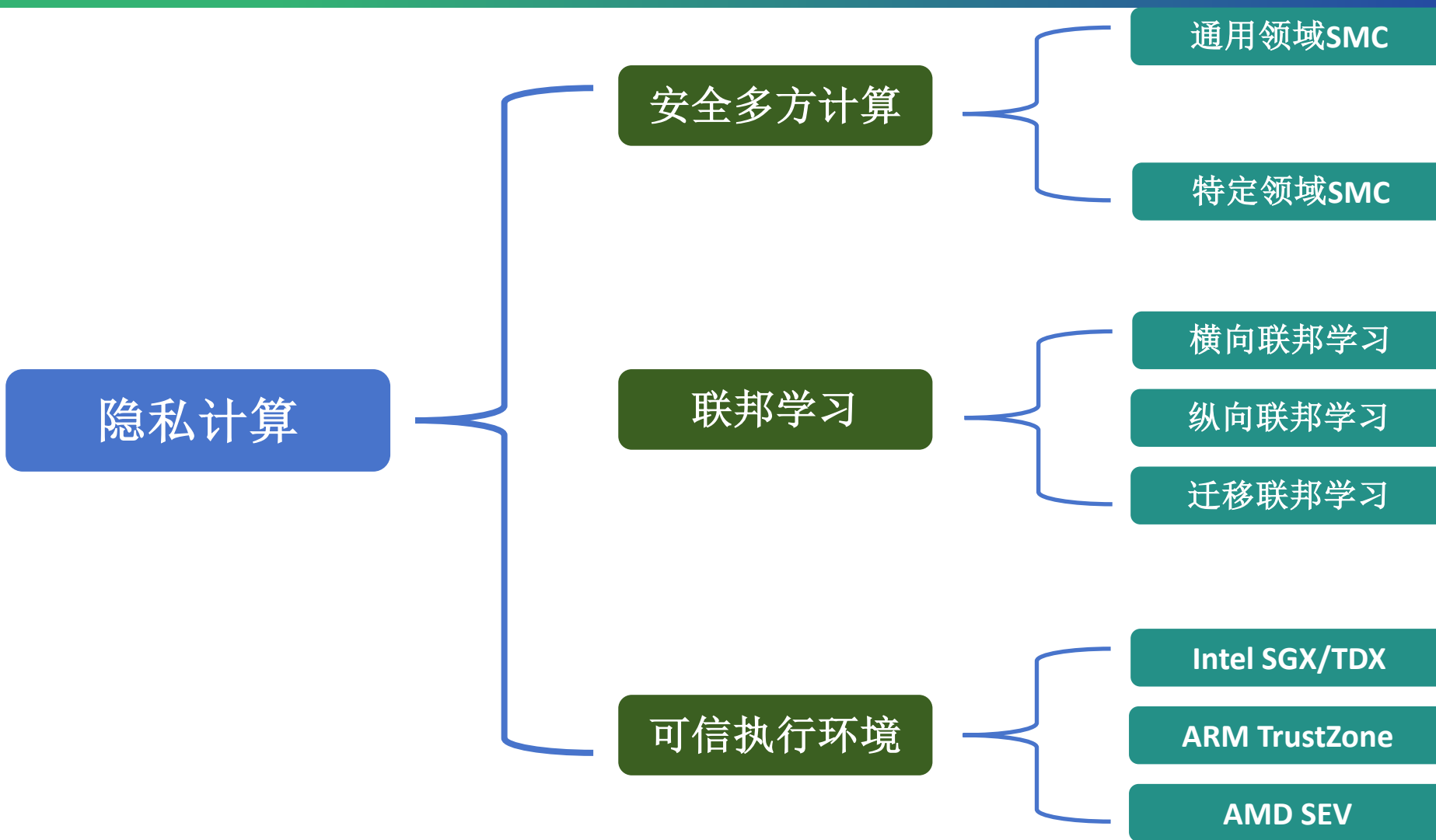
# 机密计算：学术界进展如何？

| 方向         | 相关工作                        | 期刊/会议        | 简介   |
|------------|-----------------------------|--------------|--|
| 安全漏洞与防护    | SGX-Step <sup>1</sup>       | ACSAC' 23    | 使用特权定时器中断来精确地单步执行飞地，一次只执行一个指令                    |
|            | AEX-Notify <sup>2</sup>     | Security' 23 | 基于硬件 ISA 扩展使 enclave 感知中断，从而构建基于中断的攻击对策          |
| Enclave内隔离 | Nested Enclave <sup>3</sup> | ISCA' 20     | 提出Enclave内隔离，以隔离当前整体模型中的第三方模块。                   |
|            | Light-Enclave <sup>4</sup>  | Security' 23 |  |
| 灵活性/兼容性    | vSGX <sup>5</sup>           | S&P' 22      | 基于AMD SEV提供虚拟化SGX Enclave机制                      |
|            | HyperEnclave <sup>6</sup>   | ATC' 22      | 提供跨平台、且灵活的TEE                                    |
| 资源使用量度量    | T-Counter <sup>7</sup>      | TDSC' 22     | T-Counter 允许应用程序构建一个可信的解决方案，在云计算中自行测量其 CPU 使用情况。 |
| 服务部署       | Graphene-SGX <sup>8</sup>   | ATC' 17      | 提供功能齐全的库操作系统在 SGX 上快速部署未修改的应用程序                  |
|            | Occlum <sup>9</sup>         | ASPLOS' 20   |  |

# 隐私计算：演进历史？



# 隐私计算：三大主流技术？



# 隐私计算：工业界落地？

| 产品名称                 | 技术路线          | 能力优势                         | 提出者  |
|----------------------|---------------|------------------------------|------|
| 隐私沙盒                 | 差分隐私          | 通过向数字广告运营数据添加噪声来保护用户隐私       | 谷歌   |
| iCloud Private Relay | VPN、TLS、IPsec | 保护所有离开设备的数据                  | 苹果   |
| 摩斯多方安全计算平台           | 多方安全计算、隐私保护   | 解决企业数据协同计算过程中的数据安全和隐私保护问题    | 蚂蚁金服 |
| PaddleFL             | 联邦学习          | 提供多种联邦学习方法在不同领域的轻松部署         | 百度   |
| Fedlearner           | 联邦学习          | 可对机构之间分布的数据进行联合建模            | 字节跳动 |
| PrivPy               | 多方安全计算        | 实现了支持通用计算类型、高性能、集群化和可扩展的解决方案 | 华控清交 |

隐私计算技术开源的整体现状 <https://baijiahao.baidu.com/s?id=1754058031793779409&wfr=spider&for=pc>

多方安全计算（MPC）发展脉络及应用实践 <https://baijiahao.baidu.com/s?id=1731346395339645713&wfr=spider&for=pc>

安全多方学习开源框架调研 <http://www.shouxieziti.cn/77089.html>

联邦学习开源框架综述 <https://d.wanfangdata.com.cn/periodical/jsjyjfz202307011>

近年来隐私计算领域有大量工作，**聚焦于更高的性能**（降低隐私计算带来的高开销）、**更自由的多方联邦学习**（无第三方、不依赖诚信假设）、**更强的可扩展性**（可以扩展到大型数据集和模型）、**更透明的验证机制**（零知识验证）等技术点。

| 工作名称                                    | 技术路线         | 能力优势           | 发表时间 |
|---|--------------|----------------|------|
| POSEIDON <sup>1</sup>                   | 联邦学习+多方同态加密  | 无第三方的联邦学习      | 2021 |
| DIFFERENTIALLY PRIVATE LMs <sup>2</sup> | 联邦学习+本地化差分隐私 | 具有用户级隐私保证的语言模型 | 2018 |
| SecureML <sup>3</sup>                   | 秘密分享+联邦学习    | 安全、可扩展的两方安全计算  | 2017 |
| TAP <sup>4</sup>                        | 零知识证明        | 不泄露用户隐私的透明验证   | 2023 |
| Squirrel <sup>5</sup>                   | 同态加密         | 性能极高的两方安全计算    | 2023 |
| mq-RPMT <sup>6</sup>                    | 隐私集合计算       | 高性能的两方隐私集合计算   | 2023 |



04

---

# 未来发展趋势与挑战



# 安全计算：趋势与挑战？

- 1、可验证计算技术？通过零知识证明？
- 2、可追溯计算技术？通过结合区块链？
- 3、计算性能最优化？通过CPU+GPU结合加速？
- 4、应用兼容与扩展？通过优化编程或编译器？
- 5、多种架构的兼容？建立通用的安全计算框架？

.....



边缘计算  
Edge Computing  
CONSORTIUM

CIEC2023

谢谢观看