软硬件协同的计算系统安全

从理论到实践

01部 路 航

计算系统和网络空间安全的关系——以Intel处理器系统为例

A 网络安全

攻击发起

侦查

收集目标系统和网络的信息，包括网络拓扑、开放的端口等

钓鱼

攻击者通过诱饵邮件、恶意链接等方式诱导目标用户点击恶意链接或下载恶意附件，以获取用户凭证或植入恶意软件

最终：入侵计算系统

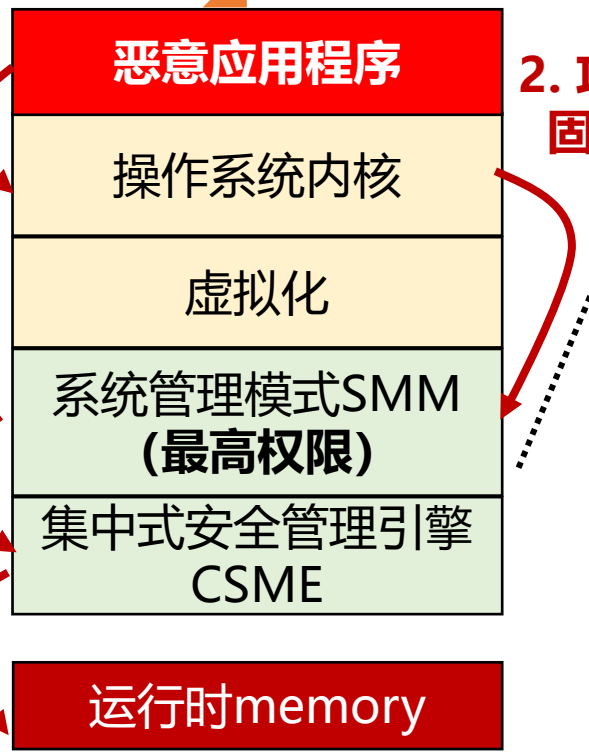
B 计算系统安全

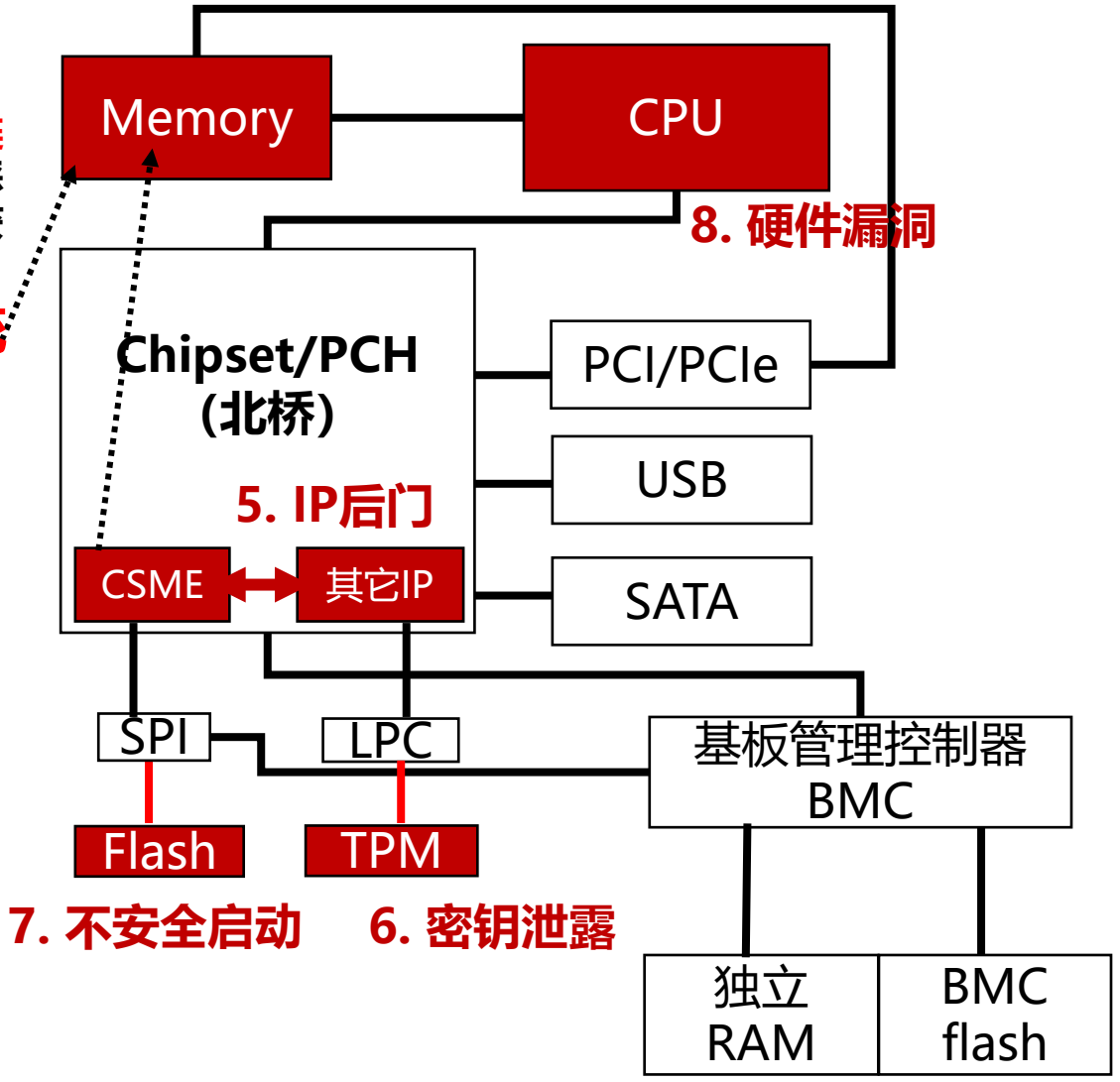
1.提权

2. 攻陷固件

3. 写允许

4. 篡改内存





计算系统是网络空间安全的最后一道防线！

危机四伏的计算系统

利用安全漏洞

“要不从烟囱进去？！”

利用内存越权访问

我怎么能进这个房子？

“伪造一下主人身份呗！”

利用未经认证的软件

“等他自己出来不就完了么！”

利用未加密的敏感数据

我怎么能不让它们进来？

我自己怎么才能安全的进来？

我要出去怎么能不被吃掉？

OUTLINE

一、安全可信的核心技术——机密计算

- “我怎么能不让它们进来？以及“我自己怎么才能安全的进来？”——**给应用提供安全屋**

二、未来敏感数据保护的主流技术——密态计算

- “我要出去怎么能不被吃掉？”——**给敏感数据穿“铠甲”**

三、重塑计算系统安全

- 基于RISC-V的计算系统安全增强

四、总结和未来展望

危机四伏的计算系统

“伪造一下主人身份呗！”

利用未经认证的软件

我自己怎么才能安全的进来?

OUTLINE

安全可信的核心技术——机密计算

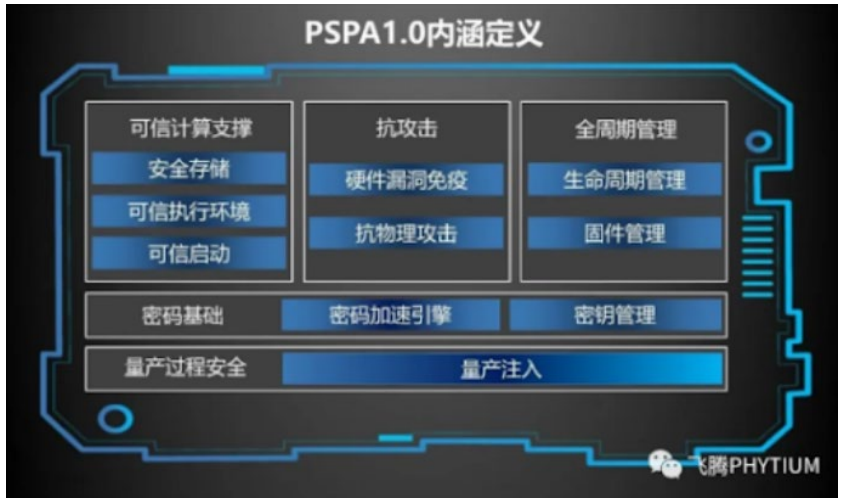
——给应用提供“安全屋”

安全可信的定义

何谓安全可信？《可信网络白皮书》的定义如下：

可信网络是将安全可信技术融入网络基础设施解决方案中，构筑网络的**内生安全能力**，实现**数据实体信任关系的传递和验证、**网络行为的持续监测和管控、业务异常的溯源和处理，从而实现结果可预期的网络。

设备可信：**设备可信是保证网络基础设施安全可信的基础，**通过**软硬件等关键能力的构建**，实现构建**内生安全全生命周期保护，软件“零”篡改、数据“零”泄密、安全态势自感知。**



沈昌祥院士给出定义：

安全可信指的是网络设备所具备的安全性能，即在设备工作的同时，**内含的安全部件**进行动态并行实时全方位安全检验，确保**计算过程及资源不被破坏和篡改，正确完成计算任务。**这就是主动免疫可信计算产品所具有的安全性能，符合国家法律战略制度推广应用的要求。

冯登国：机密计算发展现状与趋势，给出定义：

主要安全目标都是对关键计算进行**隔离**，对敏感数据进行安全保护，提供**机密性、完整性等安全属性**，并兼顾高效性与通用性。

机密计算技术——服务“安全可信”

- **从1990年代开始的前30年：“信息高速公路”的构建**
  - 全世界范围的互联构建了**最大的、最复杂**的互联网络
- **从2020开始：“数据归属权意识”的形成**
  - **政府**：数据要成为参与分配的要素
  - **企业**：数据已成为企业最重要的资产之一
  - **个人**：隐私数据的保护受到空前关注
- **机密计算技术契合了新时代发展的新需求**
  - **依靠底层的系统软硬件特性支撑了一系列的数据安全与保护能力**
  - **如：数据 "可用不可见"、"用后无沉淀"、"可控可回收"，等等**

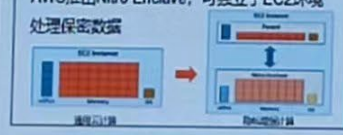
机密计算技术——服务“安全可信”

云计算安全的未来是机密计算

- 云计算发展迅猛，包括金融、电信等强监管的业务都已经开始上云
  - 纳斯达克会分阶段把全部业务迁移到亚马逊云
  - 日本最大的电信运营商会把数据仓库上云
  - 美国富国银行的目标是10年后让其所有工作量都在公共云上运行
- 微软AZure云，谷歌云，亚马逊云，阿里云等持续布局机密计算
- 安全和隐私问题已经成为云计算发展的最大障碍
- 云计算进入密态计算才有可能最终解决客户的安全顾虑
- 国际主流CPU厂商都已推出机密计算方案

AWS、Google、微软、IBM等巨头持续布局机密计算

AWS推出Nitro Enclave，可独立于EC2环境处理保密数据

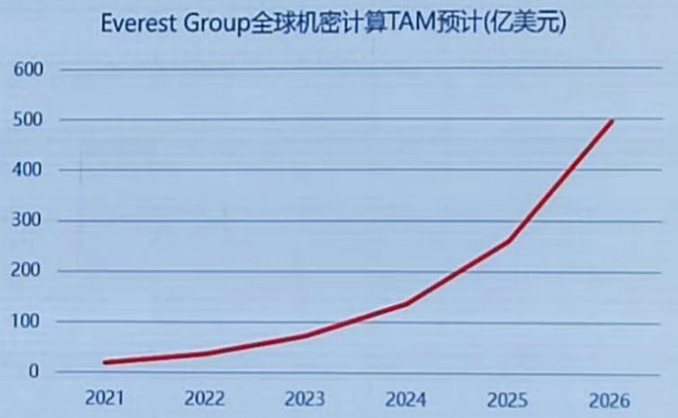


Google Cloud基于AMD二代霄龙处理器，推出Confidential VMs和Shielded VMs服务

微软云推出Confidential Compution

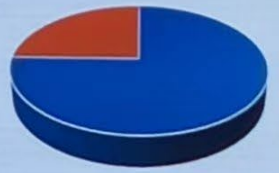
支持Intel SGX、AMD SEV、可信虚拟机等多种产品模式

IBM推出基于Intel SGX的数据隐私增强产品：Data Shield，支持裸金属和容器云多种模式



中国将占~15%的市场份额

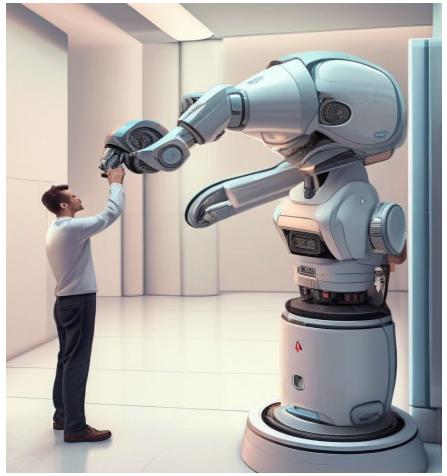
监管行业推动了75%的需求



举个例子，下面这件事如何实现？

- **数据：来自多方的隐私数据**
  - 例如：14亿人的人脸数据
- **目标：基于多方数据训练出一个模型**
  - 例如：得到一个人脸识别模型
- **要求：隐私不能泄露**
  - 例如：训练完后立刻销毁原始的人脸数据

安全屋：一种“简单”的机密计算抽象



- **找一间只有一个入口和一个出口的屋子——安全屋**
  - 确保没有窗、没有通风口，没有任何可以离开的通道（**无侧信道，实际很难做到**）
  - 屋子里只有一台仅安装了训练算法的电脑
- **在出入口的地方各安装一个机械臂**
  - 十四亿人排队将照片通过U盘交给输入机械臂，输入后U盘留在房间
- **训练完成后**
  - 得到的模型存入U盘，并通过输出机械臂送到出口处
  - 输出U盘被取走后触发清理流程，屋内所有电子设备全部销毁

“安全屋”的实现与流程

1. **输入**
   - U盘从仅有的入口输入
2. **运算**
   - 训练输入数据生成模型
3. **输出**
   - 模型通过仅有的出口输出
4. **清理**
   - 一旦输出完成立即清理
   - 没有任何数据沉淀

安全屋面临的安全挑战

1. 如何向用户证明安全屋是真的? ☑
2. 如何保证安全屋中的算法没有被篡改? ☑
3. 如何保证输出后的清理过程一定会执行? ☑
4. 如何保证安全屋的数据不被窃取或篡改? ☑

计算系统层面：机密计算 ↓ **可信执行环境**

5. 如何保证算法的输出数据不包含隐私?
6. 如何保证算法的实现没有可被利用的漏洞?

算法层面

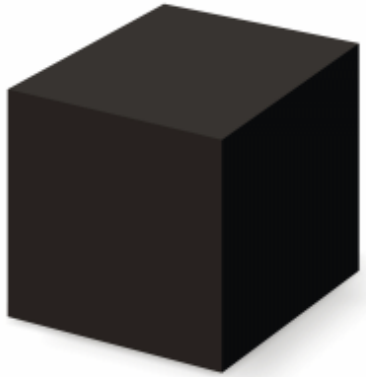
7. 如何保证用户输入的数据不是假的或错的? → **数据层面**

什么是可信执行环境（TEE）？

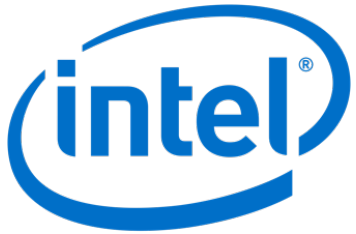
- **可信执行环境的定义**
  - “可信执行环境” （**TEE**，Trusted Execution Environment），又称**Enclave**，**是计算机系统中一块通过底层软硬件构造的安全区域**，通过保证加载到该区域的代码和数据的**完整性**和**隐私性**，实现对代码执行与数据资产的保护。

—— *Wikipedia*

- **机密计算有时特指可信执行环境**



主流云平台均推出了TEE相关云服务

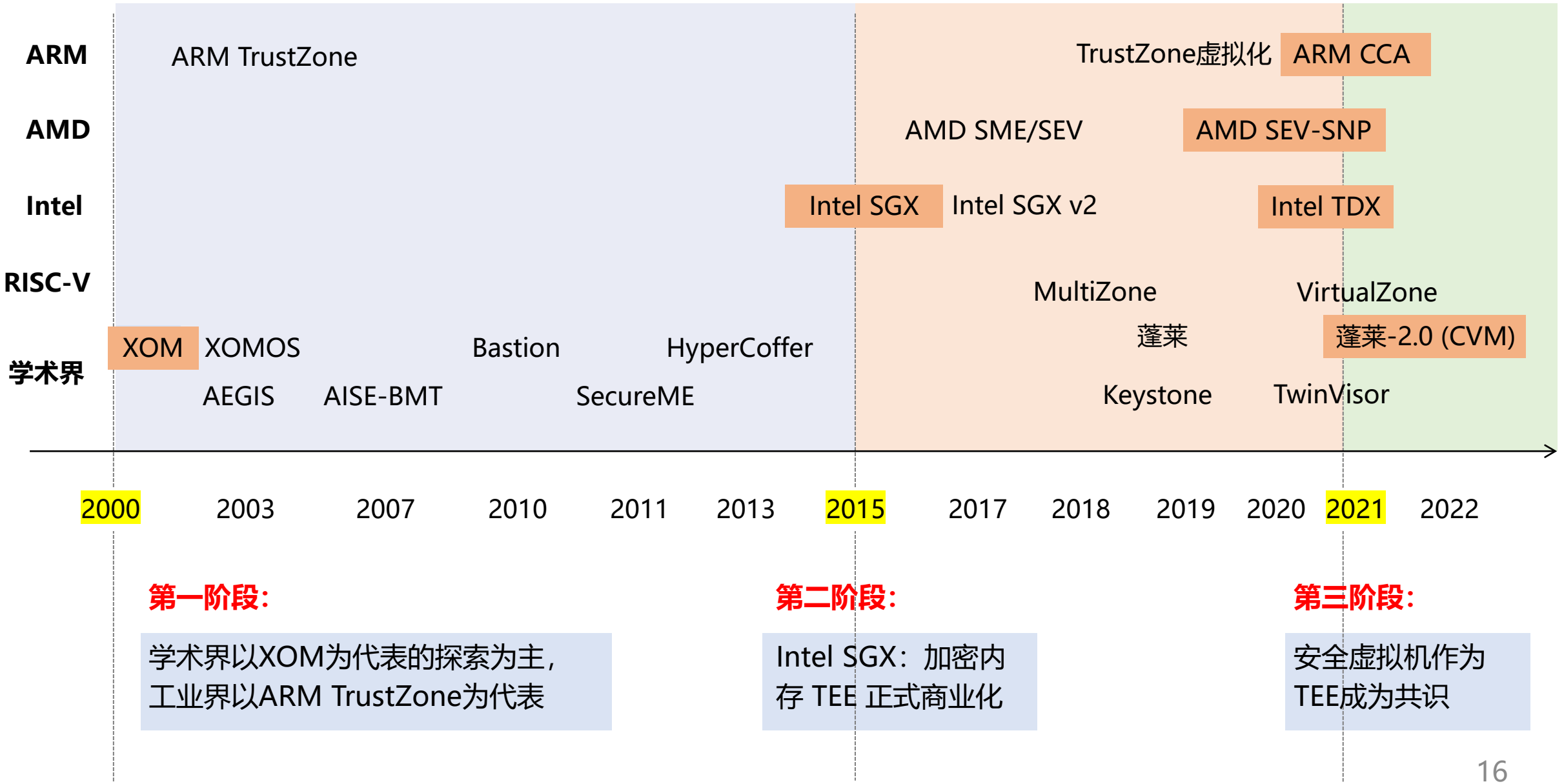


- Intel SGX/TDX
- AMD SEV
- ARM TrustZone/CCA
- Keystone、蓬莱

- **多家云厂商利用硬件安全特性保护虚拟机中的数据**
  - 2018年，Microsoft Azure 基于Intel SGX推出**Confidential Computing**
  - 2019年，Amazon 推出了**Nitro Enclave**保护用户的关键数据
  - 2020年，Google Cloud 基于AMD SEV推出加密虚拟机**Secure VM**

- **2019年8月，多家公司成立机密计算联盟**
  - 国内公司包括：华为、阿里云、腾讯、百度、字节跳动等
  - 国外公司包括：Arm、AMD、Intel、Redhat、Facebook、Google等

TEE 技术发展的三个阶段



第一阶段：

学术界以XOM为代表的探索为主，
工业界以ARM TrustZone为代表

第二阶段：

Intel SGX：加密内存 TEE 正式商业化

第三阶段：

安全虚拟机作为TEE成为共识

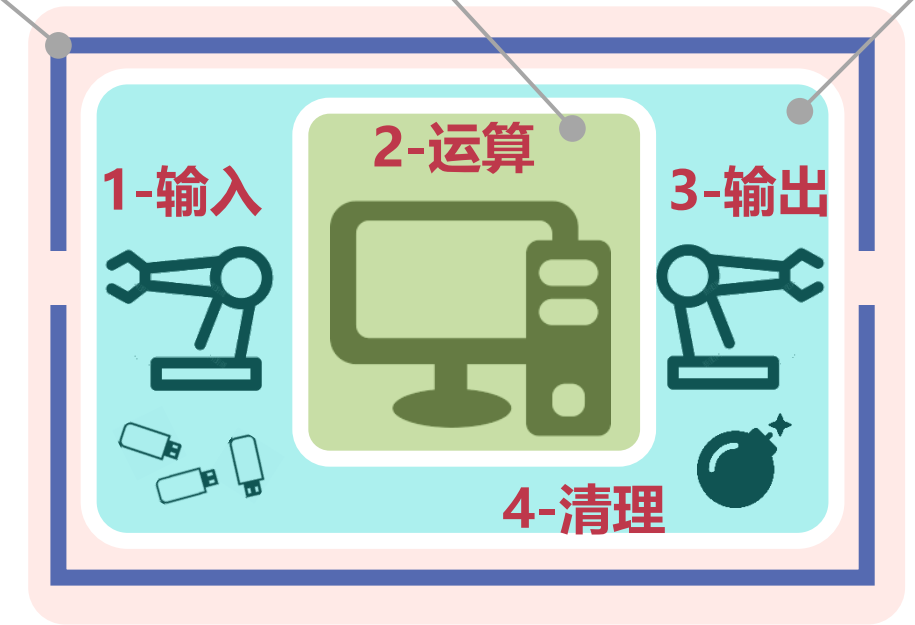
可信执行环境（TEE）的组成

TEE 硬件部分

- 通常由**芯片厂商**提供
- 提供两个主要能力
  - **远程认证**
  - **隔离执行**
- 芯片**厂商预埋私钥**
  - **用于远程认证**

算法（不属于TEE）

- 通常由用户自己或第三方提供
- 其安全性由提供方保证



安全屋

TEE 软件部分

- 通常由云服务商提供
  - 用户也可自己提供
- 提供算法的无关通用功能
  - 输入、输出
  - 初始化
  - 清理（可选）
- 通常开源，以接收审计

四个问题对应的两个技术点

1. 如何证明TEE是真的以及用户是真的?
2. 如何保证TEE中的算法没有被篡改?

远程认证 (初始时)

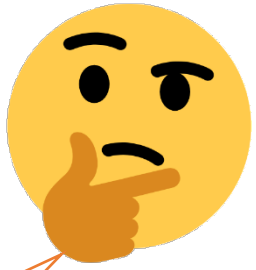
3. 如何保证输出后的清理过程一定会执行?
4. 如何保证安全屋的数据不被窃取或篡改?

隔离执行 (运行时)

TEE的重要应用：远程认证

TEE环境已经准备好：
硬件来自国产芯片X，
软件来自开源算法Y，
你可以把数据给我了

云服务器

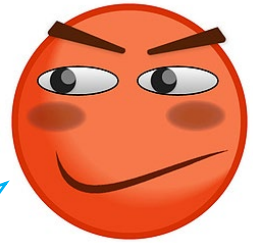


我怎么知道
你不在骗我？

用户

我怎么知道
你不在骗我？

云服务器



TEE软件已经准备好
我是来自xxx的xxx
你可以让我的数据进去了

用户

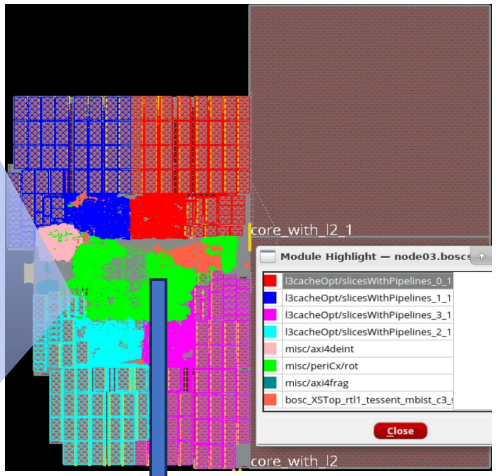
如何向用户证明TEE软硬件是真的?

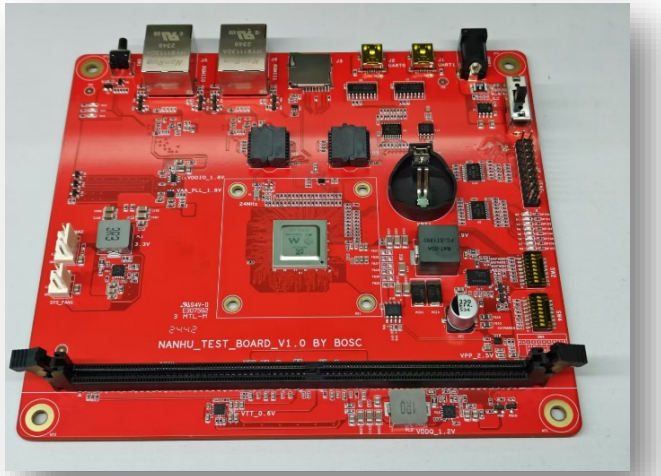
- **认证：TEE的硬件是真的**
  - TEE来自某个芯片制造商（如Intel）
  - 方法：通过硬件中内置的**私钥**来判断（对应公钥由**认证服务器**维护）
  - 前提：该私钥不出硬件，且对应的公钥不可伪造，可通过**硬件可信根**来解决

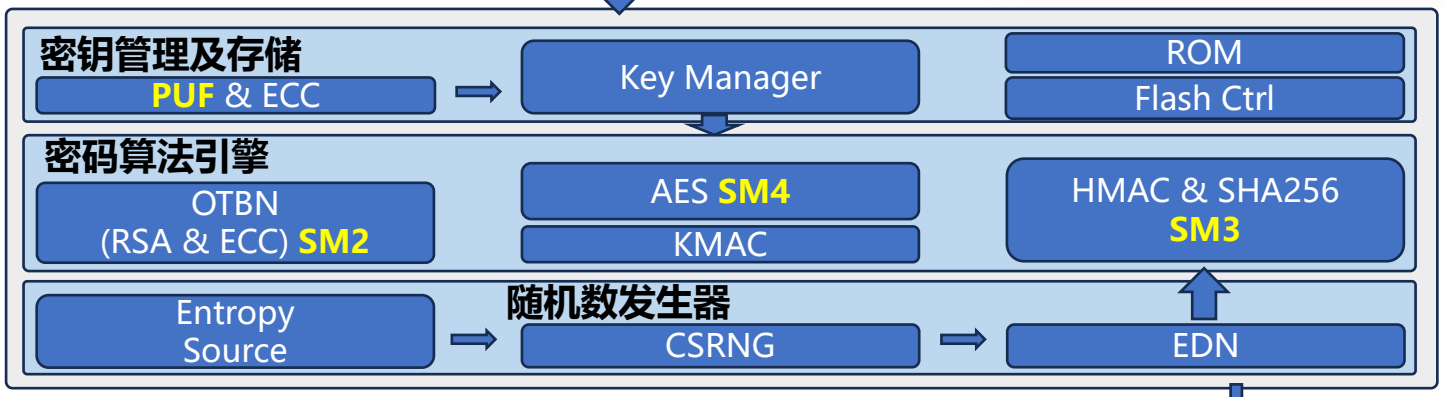
- **认证：TEE的软件是真的，严格意义上TEE的固件（管理受保护应用）也要验证**
  - TEE中加载的软件：包含系统软件和用户的软件
  - 方法：通过对TEE内存**计算hash**来判断（TEE内嵌私钥签名）
  - 时间节点：在代码加载入TEE内存后、执行第一行代码前（例如，固件和受保护应用的安全启动和加载）

从理论到实践——“翠湖”芯片中的可信根

双核、TSMC-28nm工艺，主频：1.0 – 1.5 GHz，SPEC2006 9.236/GHz







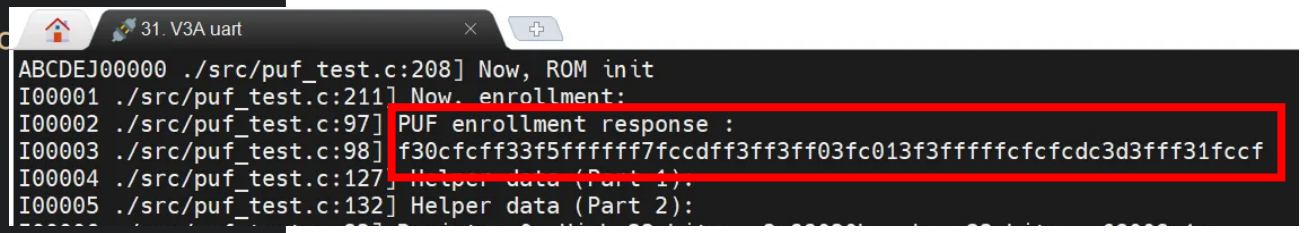

```
================== Score ==================
         astar:  6.978,  6.978
        bwaves:  9.869,  9.869
         bzip2:  5.768,  5.768
     cactusADM:  9.300,  9.300
      calculix:  4.393,  4.393
        dealII: 15.213, 15.213
        gamess:  9.770,  9.770
           gcc:  8.555,  8.555
     GemsFDTD:  9.861,  9.861
         gobmk:  7.579,  7.579
       gromacs:  7.612,  7.612
      h264ref: 12.133, 12.133
         hmmer:  8.903,  8.903
           lbm: 14.838, 14.838
      leslie3d:  8.289,  8.289
    libquantum: 17.096, 17.096
           mcf:  7.828,  7.828
          milc:  8.074,  8.074
          namd:  8.478,  8.478
       omnetpp:  7.891,  7.891
     perlbench:  8.408,  8.408
         povray: 13.401, 13.401
          sjeng:  8.067,  8.067
         soplex:  9.686,  9.686
        sphinx3:  9.888,  9.888
          tonto:  8.374,  8.374
            wrf:  9.163,  9.163
      xalancbmk: 12.278, 12.278
         zeusmp: 10.795, 10.795
SPEC2006@1.0GHz:   9.236
SPEC2006/GHz:   9.236

********* SPECINT 2006 *********
  400.perlbench:  8.408,  8.408
      401.bzip2:  5.768,  5.768
        403.gcc:  8.555,  8.555
        429.mcf:  7.828,  7.828
      445.gobmk:  7.579,  7.579
      456.hmmer:  8.903,  8.903
      458.sjeng:  8.067,  8.067
 462.libquantum: 17.096, 17.096
    464.h264ref: 12.133, 12.133
     471.omnetpp:  7.891,  7.891
       473.astar:  6.978,  6.978
  483.xalancbmk: 12.278, 12.278
SPECint2006@1.0GHz:  8.903
SPECint2006/GHz:   8.903
```

从理论到实践——“翠湖”芯片中的可信根

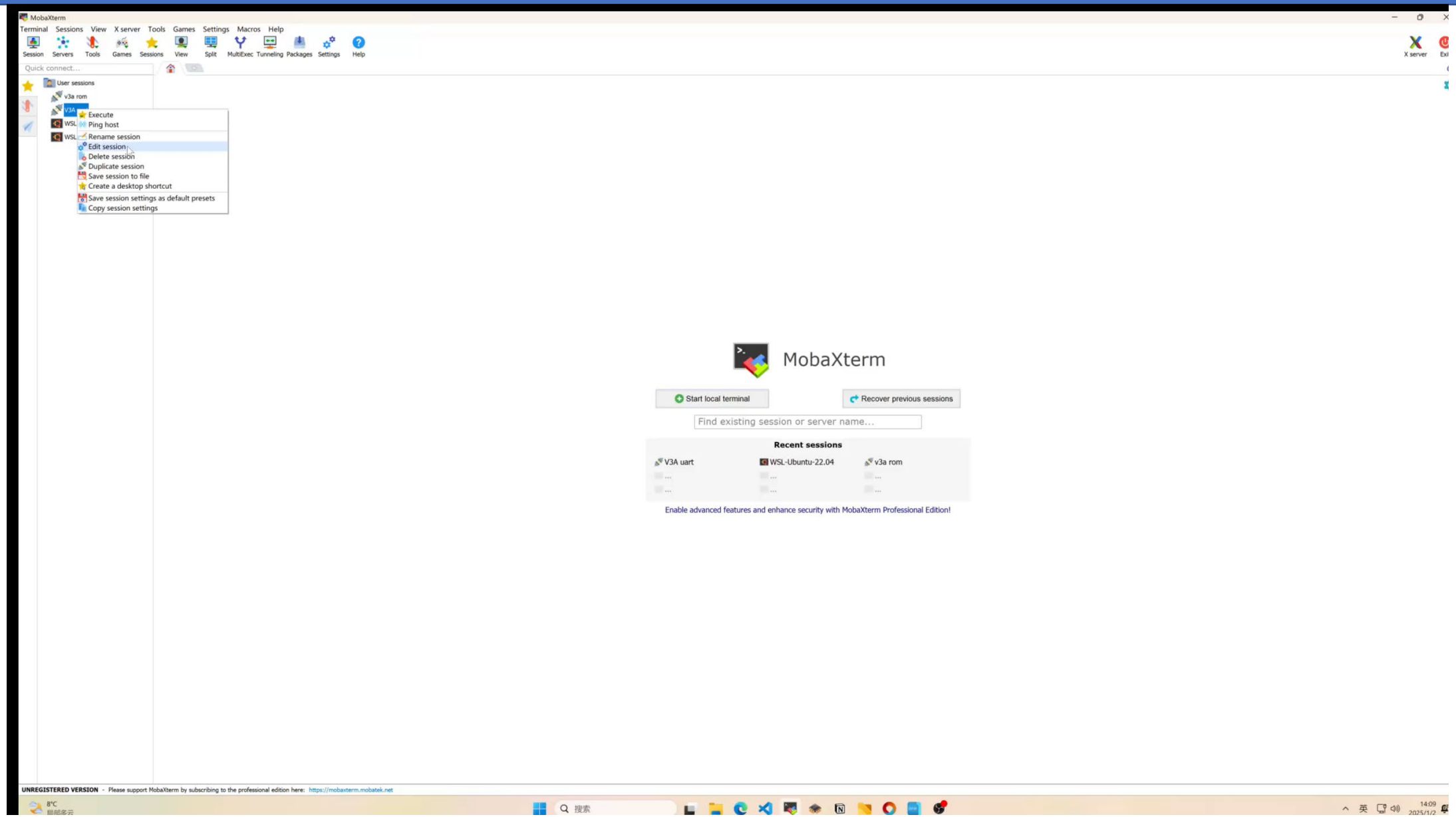
```
Multi-threaded TLS Server listening on port 8443...
Maximum concurrent clients: 10
Starting data generation thread...
Waiting for client connections... (Press Ctrl+C to stop)
New connection accepted. Active clients: 1/10
[Client 1] Connected from 127.0.0.1:35734
[TEE] ROT 256 bits seed: 500cfd3c0fc3ddfff0f307f333cdfff033373033ddfff03377f333cdfff0330f
[TEE] decrypts the premaster secret
[Client 1] === TLS Session Keys ===
[Client 1] Master Secret (48 bytes): 12b9708d4b7e324792e10350b1ed3cc1...
[Client 1] Server Random (32 bytes): bc136661559aa7c169fc6ebf56fe4b0b31748e3d4567b0a510909aff6c2298b3
[Client 1] Client Random (32 bytes): e88f3bfb107af7d86c1de18c163e937d713effa1a2aa65962e
[Client 1] Session established with symmetric encryption
[Client 1] Key exchange completed successfully
[Client 1] TLS handshake completed successfully!
[Client 1] ===== TLS Handshake Key Information =====
[Client 1] Client Public Key Type: RSA
[Client 1] Client Public Key Modulus (first 64 chars): A67C51D79FBF0D252817F6EA4817AC632364783B97BE3CD78FB39DB976C6D023...
[Client 1] Client Public Key Exponent: 010001
[Client 1] Cipher Suite: ECDHE-RSA-AES256-GCM-SHA384
[Client 1] ==========================================
New connection accepted. Active clients: 2/10
[Client 2] Connected from 127.0.0.1:44736
[Client 2] TLS handshake failed: received alert fatal error
[Client 2] Connection closed. Active clients: 1
```

PUF密钥



不同设备密钥均不同，具备唯一性、随机性、无需外部注入。

从理论到实践——“翠湖”的安全启动



TEE的初始化与远程认证过程

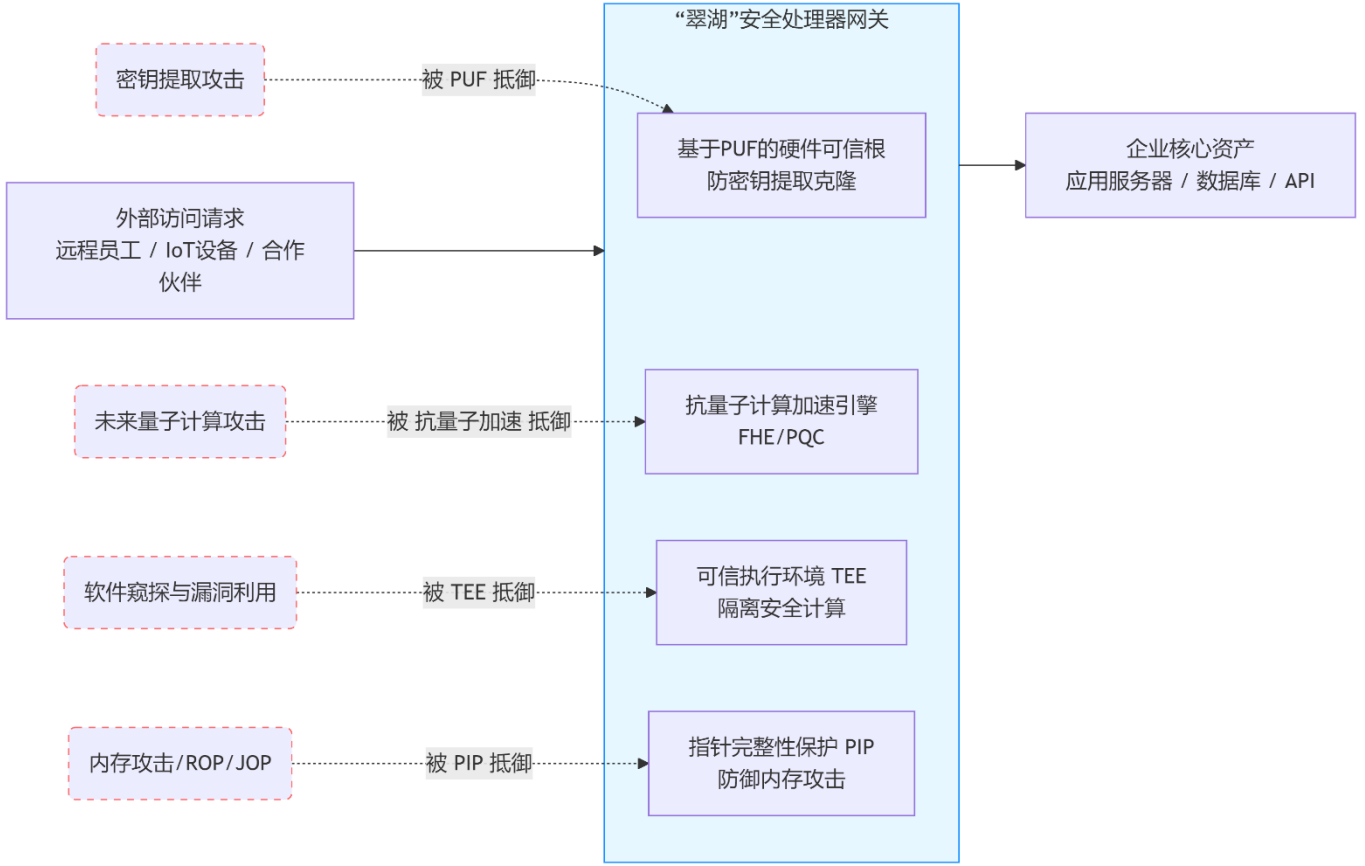
1. **TEE初始化（TEE服务商，安全启动）**
   - 初始化硬件环境，并加载软件进入**TEE**
2. **远程认证（三方交互）**
   - **用户/TEE**向**TEE/用户**发起一个**认证请求**
   - **TEE/用户生成认证**，签名后返回给用户/TEE
   - 用户/TEE向验证服务器确认**认证有效性**
3. **建立安全信道（用户与TEE）**
   - 用户与TEE交换加密方式和密钥后建立**加密通道**
4. **通过信道输入数据，并调用算法执行（用户与算法）**

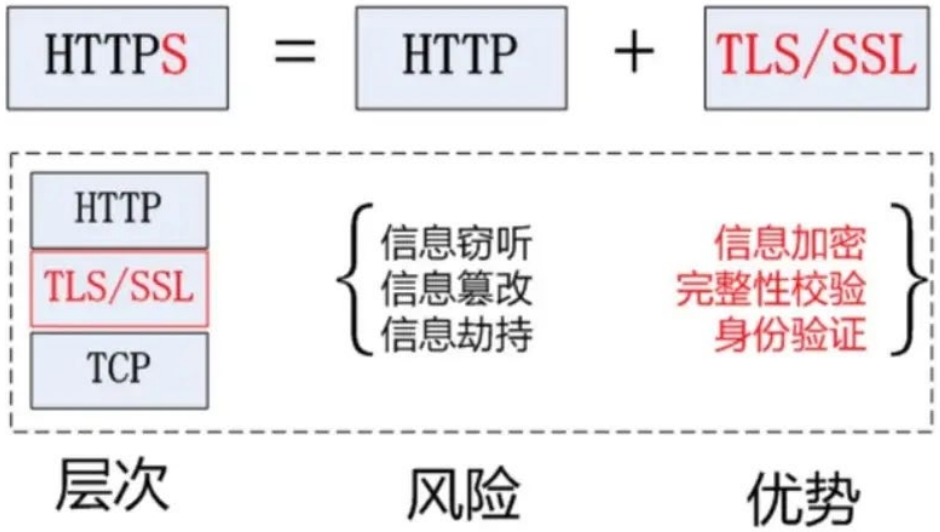
TEE

从理论到实践——“翠湖”远程认证支持

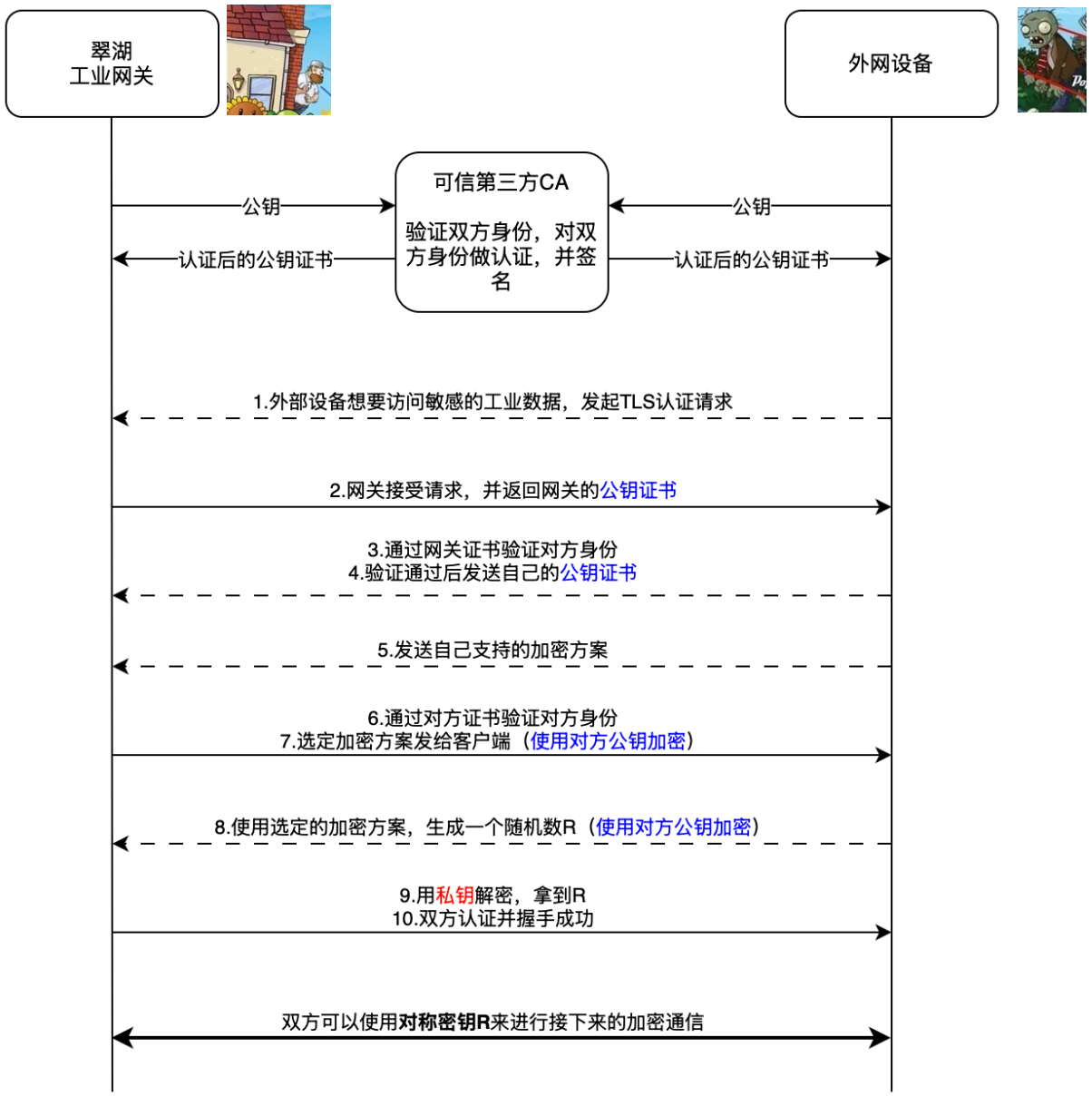
比如，**一个企业有自己的内部网站，该网站主要是用于员工查询信息和官方事务交流的。他们不希望任何人都可以这样自由访问内部网站。**这种情况下，就可以选择使用双向认证的SSL证书验证客户端身份，然后再让他们访问网站。如此一来，**企业可避免网络犯罪分子和僵尸程序进入该内部网站，降低不安全性风险。**

总的来说，一般Web应用都是采用SSL单向认证的，用户数自由无限制，且无需在通讯层对用户身份进行验证，一般都在应用逻辑层来保证用户的合法登入。但如果是企业应用对接，数据信息相对较多且复杂，可能会要求对客户端做身份验证，**这时就需要做SSL双向认证，这也是保护公司内部数据信息的最好的方法。**





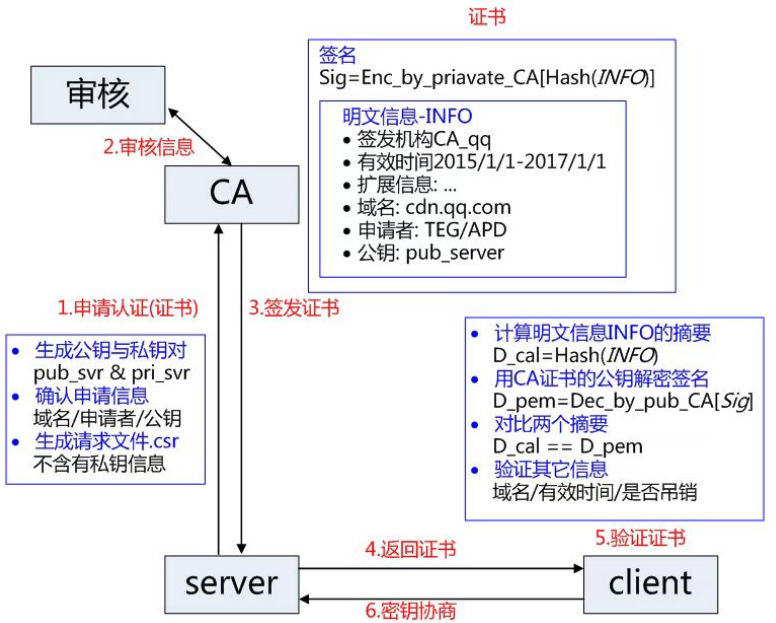
从理论到实践——“翠湖”远程认证支持



翠湖作为工业网关，保护工业内网数据。如果有外网设备想要访问内部数据，需要网关进行身份认证

认证过程如左图：

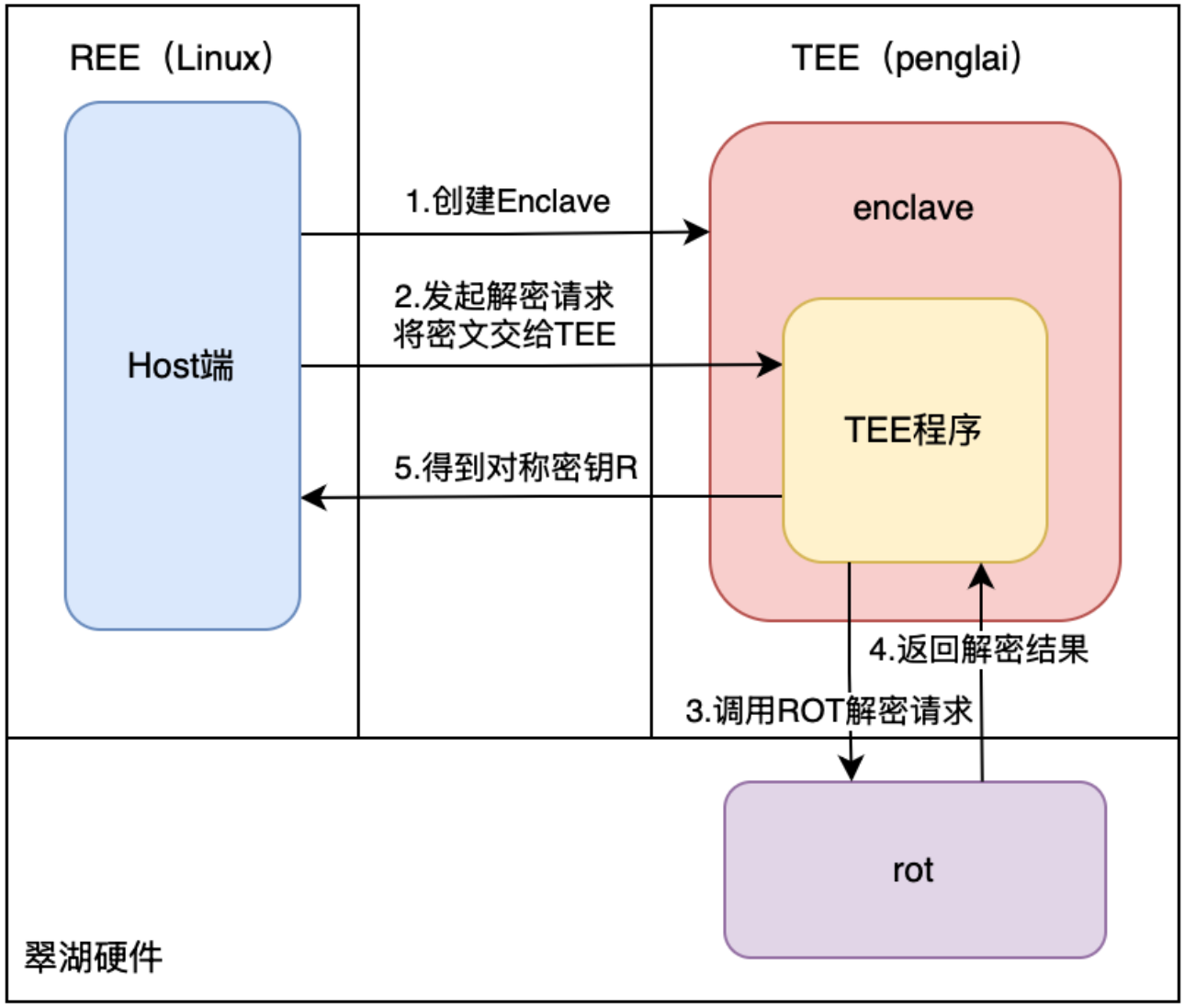
1. 最开始是需要一个可信第三方验证双方身份并签发证书
2. 当收到外部设备接入请求后，双方进行握手验证，只要双方身份都验证成功才能接入
3. 接入后拿到一个**对称密钥R**，相当于一个访问令牌，才能进行数据传输



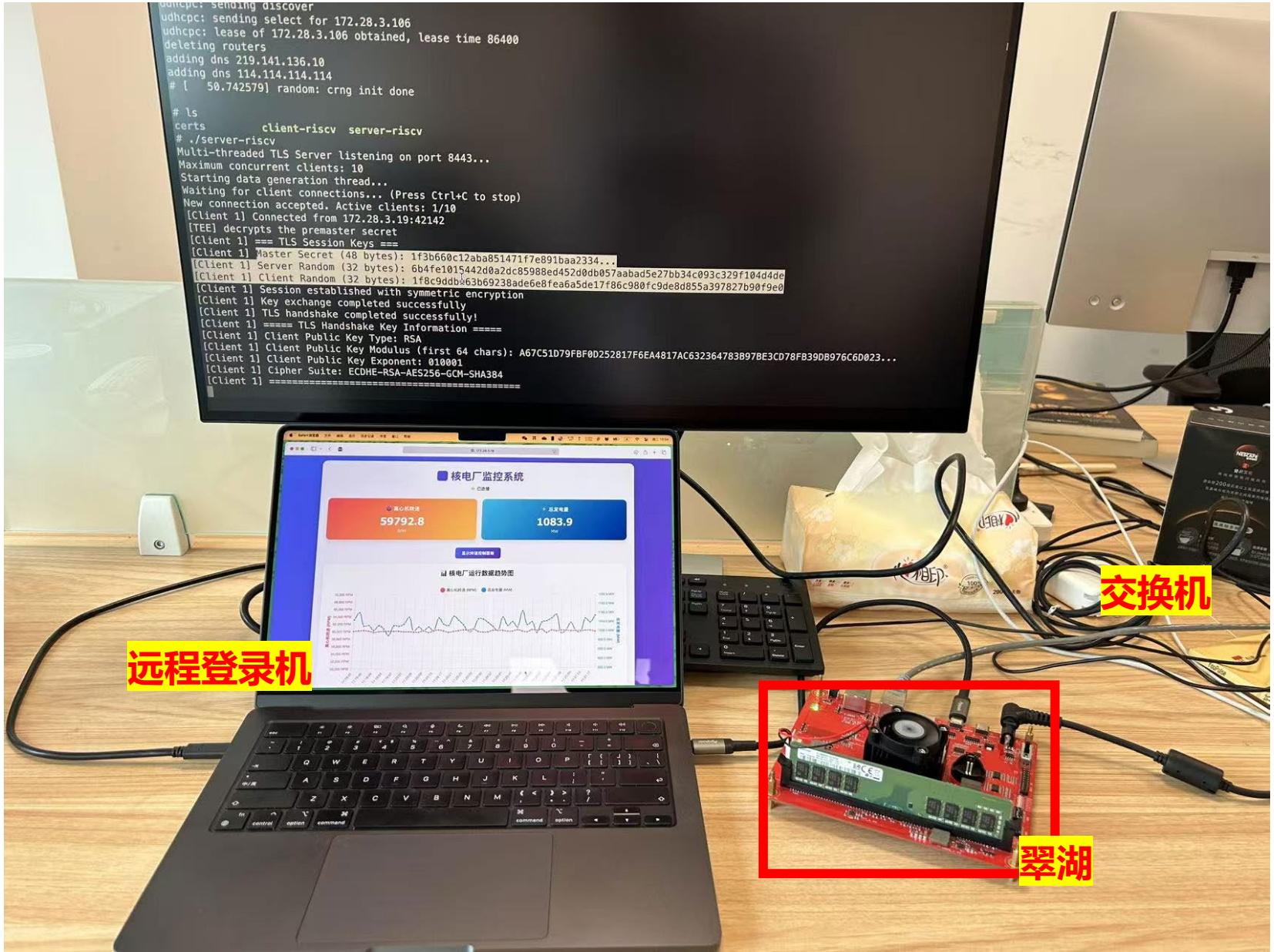
从理论到实践——“翠湖”远程认证支持

右图为工业网关在握手第9步，也就是用私钥解密的过程。

私钥作为整个握手中最重要的一环，是不可以被泄露的，所以需要将涉及到的私钥的解密过程放在可信根中处理，由TEE程序调用。



从理论到实践——“翠湖”远程认证支持



危机四伏的计算系统

你水平不行，要不我来吧！

利用内存越权访问

我怎么能进这个房子?

我怎么能不让它们进来?

TEE的安全保障——隔离执行

- **利用“硬件隔离机制”限制特权软件的权限**
  - 方法-1：直接**新增硬件隔离能力**保护TEE范围的硬件
  - 方法-2：引入更底层的**特权软件**（属于**可信计算基，TCB**）

- **典型实现**
  - **页表**机制，主流CPU均支持
  - PMP（Physical Memory Protection），如：RISC-V
  - PRM（Processor Reserved Memory），如：Intel SGX

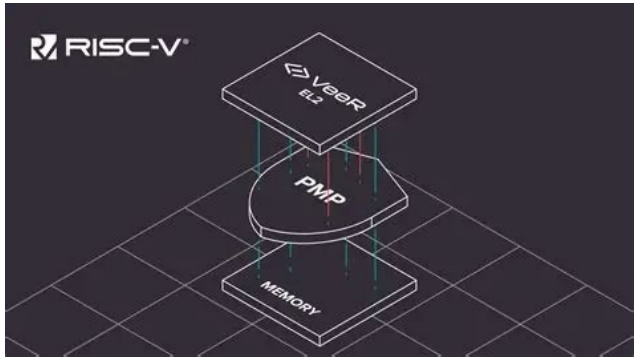
页表项的数据结构抽象与类型定义

第一小节中我们提到，在页表中以虚拟页号作为索引不仅能够查到物理页号，还能查到一组保护位，它控制了应用对地址空间每个虚拟页面的访问权限。但实际上还有更多的标志位，物理页号和全部的标志位以某种固定的格式保存在一个结构体中，它被称为 **页表项** (PTE, Page Table Entry)，是利用虚拟页号在页表中查到的结果。

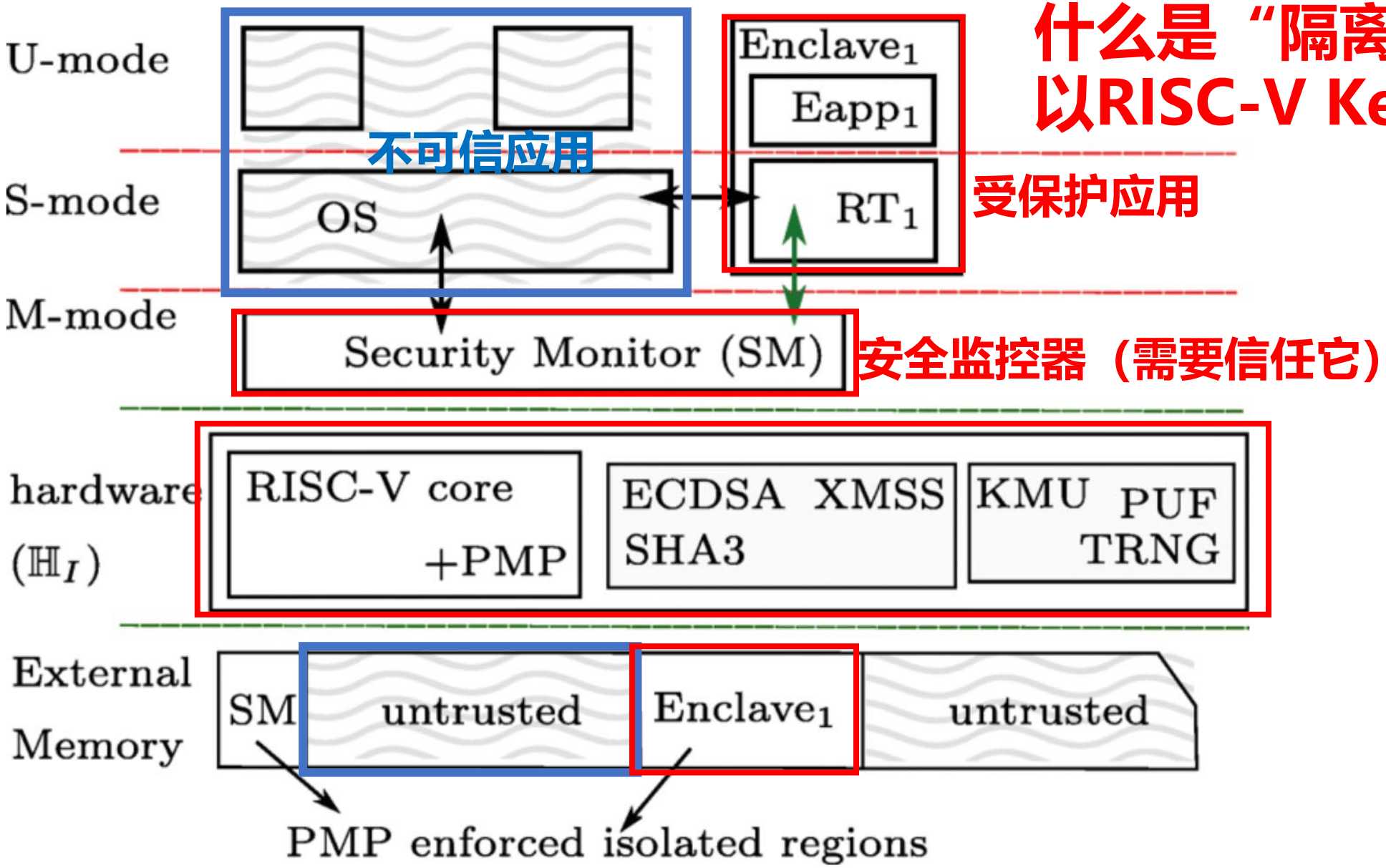
63 54	53 28	27 19	18 10	9 8	7	6	5	4	3	2	1	0
Reserved	PPN[2]	PPN[1]	PPN[0]	RSW	D	A	G	U	X	W	R	V
10	26	9	9	2	1	1	1	1	1	1	1	1

上图为 SV39 分页模式下的页表项，其中 $[53:10]$ 这 44 位是物理页号，最低的 8 位 $[7:0]$ 则是标志位，它们的含义如下（请注意，为方便说明，下文我们用 *页表项的对应虚拟页面* 来表示索引到一个页表项的虚拟页号对应的虚拟页面）：

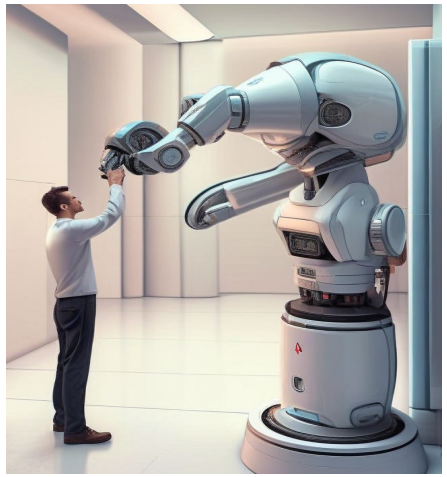
- V(Valid)：仅当位 V 为 1 时，页表项才是合法的；
- R(Read)/W(Write)/X(eXecute)：分别控制索引到这个页表项的对应虚拟页面是否允许读/写/执行；
- U(User)：控制索引到这个页表项的对应虚拟页面是否在 CPU 处于 U 特权级的情况下是否被允许访问；
- G：暂且不理会；
- A(Accessed)：处理器记录自从页表项上的这一位被清零之后，页表项的对应虚拟页面是否被访问过；
- D(Dirty)：处理器记录自从页表项上的这一位被清零之后，页表项的对应虚拟页面是否被修改过。



TEE的安全保障——隔离执行

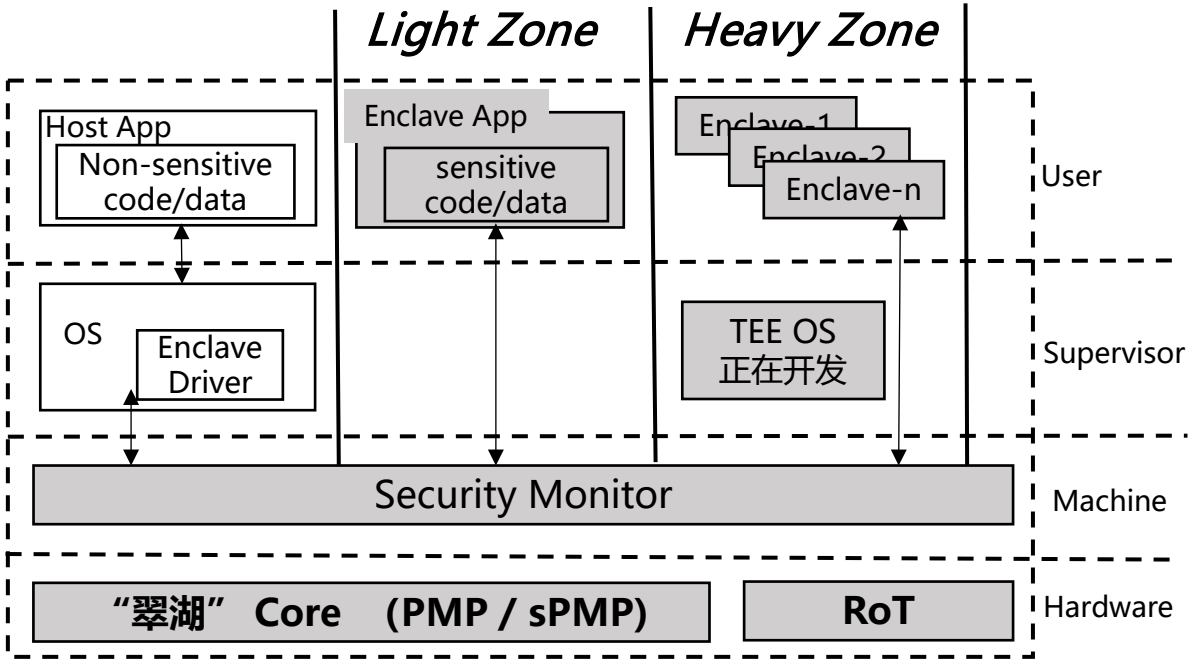


什么是“隔离”？
以RISC-V KeyStone为例



从理论到实践——“翠湖”的隔离执行

ZGC-TEE Heavy.Light 方案：在RISC-V架构PMP物理内存保护机制的基础上引入了sPMP硬件扩展和相关访存权限检查逻辑，保证安全性的同时进一步提高了Enclave的**可扩展性。**

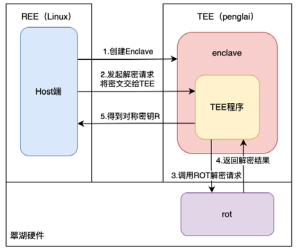


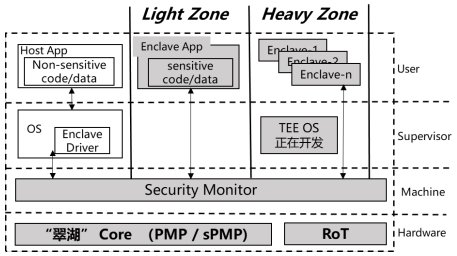
sha	1834115730	1888146900	2.95%
rijndael enc	467300800	477417270	2.16%
rijndael dec	431700190	438917570	1.67%
bitcnts	1329739030	1393779280	4.82%

小结

一、安全可信的核心技术——机密计算

- “我怎么能不让它们进来？以及“我自己怎么才能安全的进来？” ——给**应用提供安全屋**





- **机密计算的简单抽象：安全屋**

  输入、运算、输出、清理

- **可信执行环境的两个主要技术点：远程认证、隔离执行**

  可信根、安全启动、双向认证；专用硬件和软件隔离；

所有的安全认证和机密信息处理均依赖于TEE展开！各大处理器巨头纷纷构建自己的TEE技术和生态，如Intel SGX，AMD SEV等

CONFIDENTIAL COMPUTING CONSORTIUM **2019年8月，机密计算联盟成立**

美国及其盟友企业

- **Intel、Arm、AMD、Google、Facebook...**

中国企业 **无芯片企业**

- **阿里云、腾讯、百度、字节跳动...**

危机四伏的计算系统

利用安全漏洞

“要不从烟囱进去？！”

我要出去怎么能不被吃掉？

“等他自己出来不就完了么！”

利用未加密的敏感数据

TEE的安全边界：何时无效?

TEE存在的问题——明文处理!

- **可能被攻击成功的场景**
  - 利用“**隐蔽信道**”等安全漏洞
  - TEE内部的**私钥**被泄露或被伪造
  - 认证服务器**签名私钥**被泄露或被伪造
  - 加密算法被攻破（如量子计算等）
  - 依然基于传统的PKI体系（如CA等）

“僵尸”打洞进来or守株待兔怎么办?

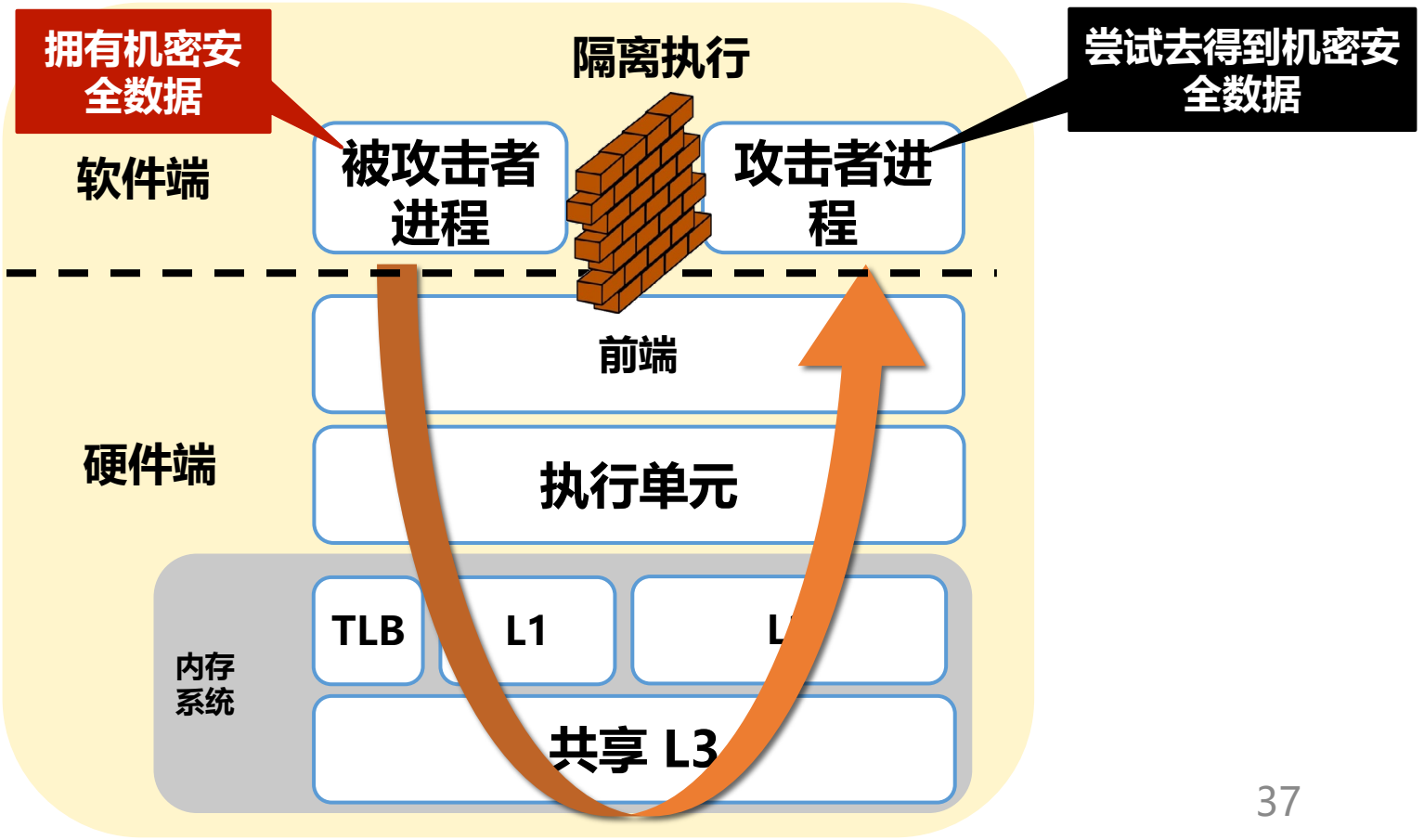
- **信任方**
  - TEE硬件制造商、远程认证服务提供方

是否有办法确保数据“绝对安全”？可用不可见、可算不可得!

TEE的安全边界：何时无效?

- **侧信道（隐秘信道）**
  - 原本无法直接通信的两方，通过原本不被用于通信的机制进行数据传输
  - 常见的隐秘信道：时间、功耗、电磁泄露、声音等

CPU



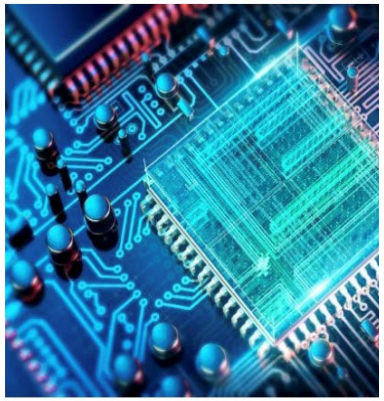
TEE的安全边界：何时无效?

暂态执行（Speculative Execution）+ 侧信道攻击

Newest Intel Side-Channel Atta Sensitive Data

Author:
Lindsey O'Donnell
March 8, 2021 / 4:20 pm
3:30 minute read

Share this article:



A new side-channel attack takes aim at Intel's order to glean sensitive data.

Intel processors are vulnerable to a new side-channel att allow attackers to steal sensitive information such as enc

Unlike previous side-channel attacks, this attack does no sets and other former tactics. Instead it leverages a comp interconnect contention. This component facilitates com units – including cores, the last-level cache, system ager Intel processors, such as the Skylake and Coffee Lake CP

Riccardo Paccagnella, one of the researchers with the Ur Champaign who discovered the attack, told Threatpost tl give attackers the means to infer "key bits" from both vuln implementations and from the precise timing of keystrok

AMD Discloses a Spectre-Like Vulnerability in Zen 3 CPUs

By Joel Hruska on April 5, 2021 at 9:31 am | Comments

AMD has published details of a Spectre-like vulnerability that affects Zen 3 CPU related to a new feature AMD introduced with its latest architecture called Predi Store Forwarding (PSF). AMD is not aware of any code exploiting this issue in th is releasing this information preemptively.

PSF is used to guess what the result of a load will be and to execute instructions on that assumption. PSF builds on an earlier performance improvement known a Load Forwarding (STLF). STLF refers to the practice of transferring data from a s directly to a load without writing it to main memory first. Before the STLF comple CPU checks to make sure the load address and the store address match.

New Spectre Flaws in Intel and AMD CPUs Affect Billions of Computers

May 06, 2021 Ravie Lakshmanan

When Spectre, a class of critical vulnerabilities impacting modern processors, was publicly revea in January 2018, the researchers behind the discovery said, "As it is not easy to fix, it will haunt u for quite some time," explaining the inspiration behind naming the speculative execution attacks.

Indeed, it's been more than three years, and there is no end to Spectre in sight.

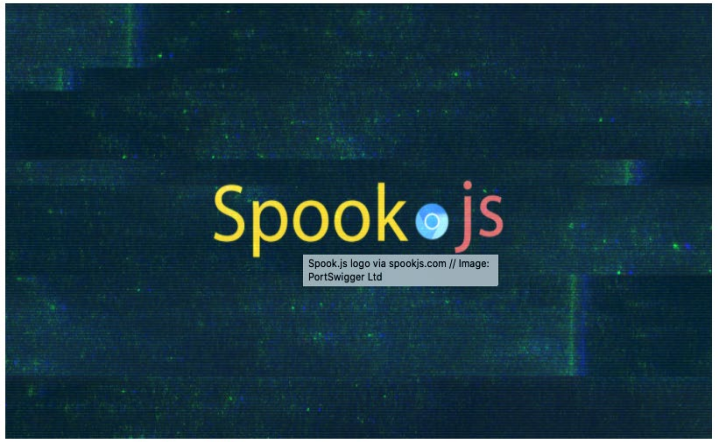
A team of academics from the University of Virginia and University of California, San Diego, have discovered a new line of attack that bypasses all current Spectre protections built into the chips, potentially putting almost every system – desktops, laptops, cloud servers, and smartphones – once again at risk just as they were three years ago.

Spook.js – New side-channel attack can bypass Google Chrome's protections against Spectre-style exploits

Jessica Haworth 10 September 2021 at 11:06 UTC
Updated: 10 September 2021 at 11:24 UTC

Side-channel Google Browsers

CPU-level data leak technique still kicking, three years on



A newly discovered side-channel attack targeting Google Chrome can allow an attacker to overcome the web browser's security defenses to retrieve sensitive information using a Spectre-style attack.

Dubbed Spook.js, the 'transient execution side-channel attack' can bypass Chrome's protections against speculative execution (Spectre) exploits to steal credentials, personal data, and more.

This is according to the authors of a paper titled 'Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution' (PDF).

Spectre attacks

Spectre, which hit global headlines back in 2018, exploits flaws in the optimization features of modern CPUs to bypass the security mechanisms that prevent different processes from accessing each other's memory space.

This allowed a wide range of attacks against different types of applications, including web apps, enabling attackers to steal sensitive information across different websites by exploiting how different applications and processes interact with processors and on-chip memory.

TEE的安全边界：何时无效?

- 攻击隐蔽、变种繁多，造成安全**漏洞难以防范，修复困难**

利用指令集、硬件漏洞发起攻击

2014

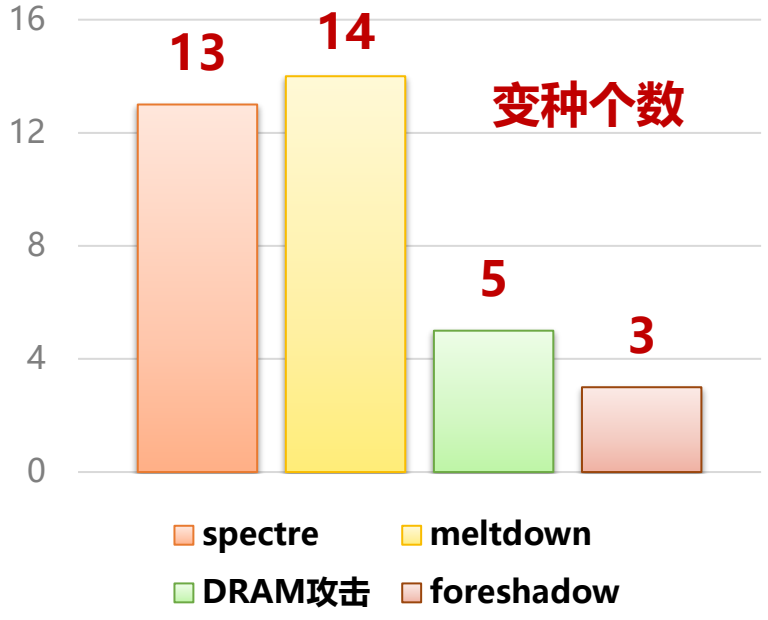
2018

2018

2019

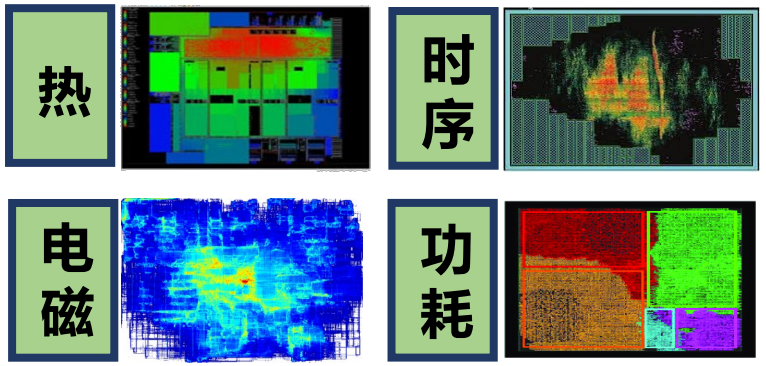
2021

2022

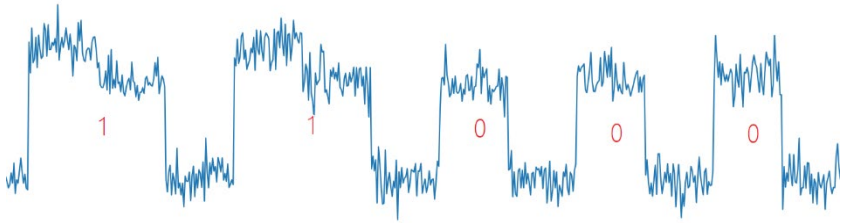


攻击变种 \ 攻击信道	BTB	BHB	PHT	RSB	STL
Spectre-PHT	○	◑	●	○	○
Spectre-PHT	○	◑	●	○	○
Spectre-BTB	●	◑	○	○	○
Spectre-RSB	◑	○	○	●	○
Spectre-STL	○	○	○	○	●

利用电磁侧信道发起攻击



根据微处理器的功耗曲线推断出密钥信息



TEE的安全边界：何时无效?

攻击对象

for(i=0; i<=100 ; i++)
{}

循环指令的特点是指令的内容在一段时间内保持不变

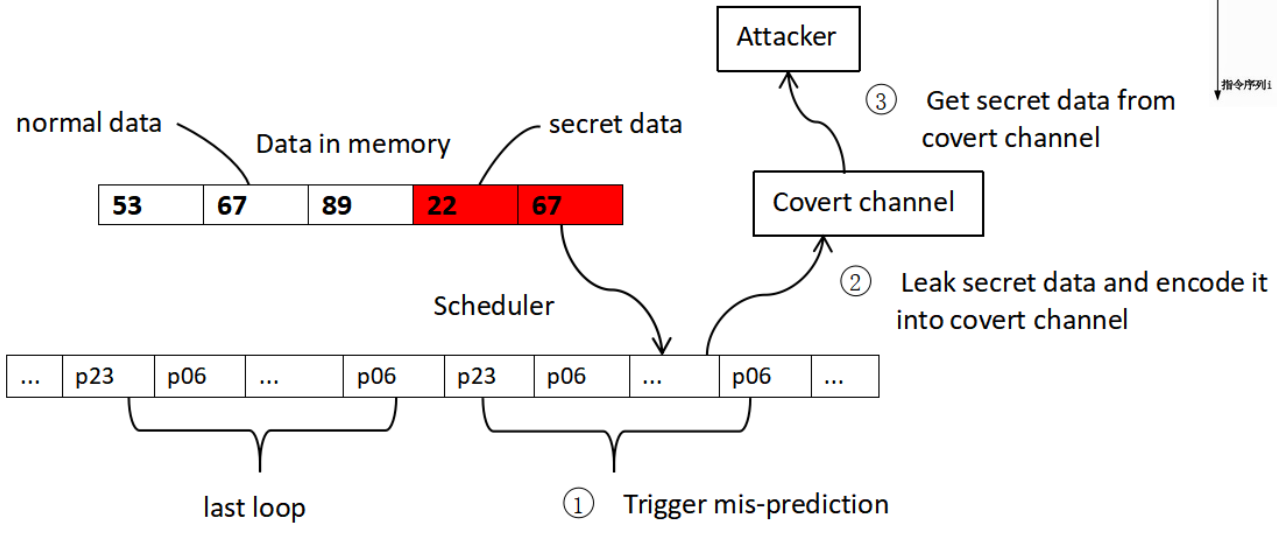
LSD in X86

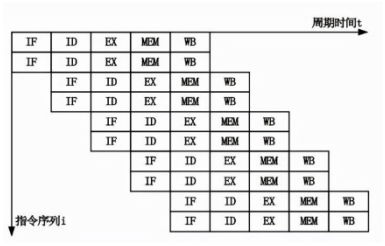
攻击原理

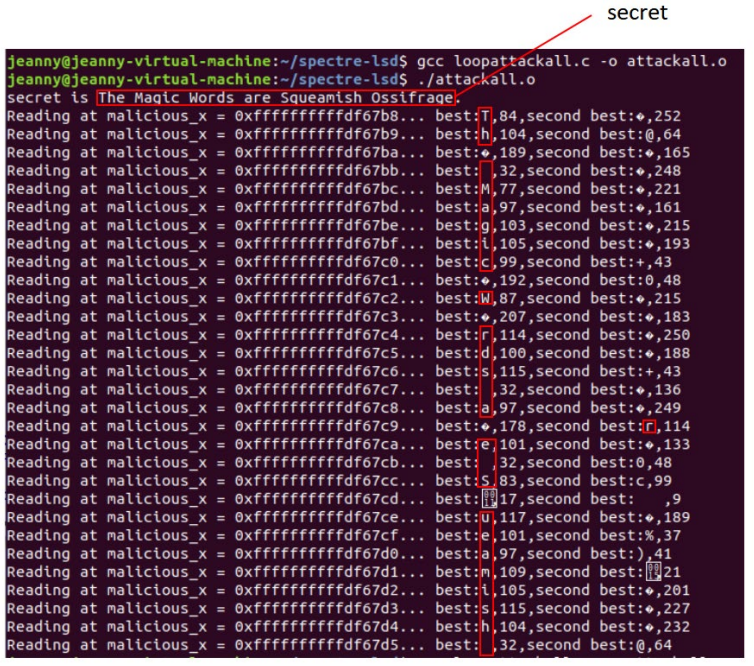
发现循环后会休眠前端资源，**导致跳出循环时产生暂态执行**，利用LSD产生的暂态执行越权读取数据

攻击效果

运行迭代次数为20的循环进行攻击，**成功率为89.3%**







OUTLINE

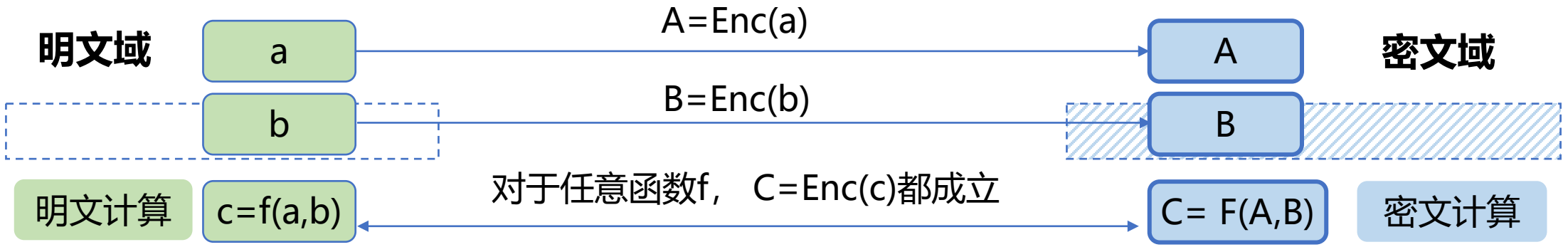
未来敏感数据保护的主流技术——密态计算

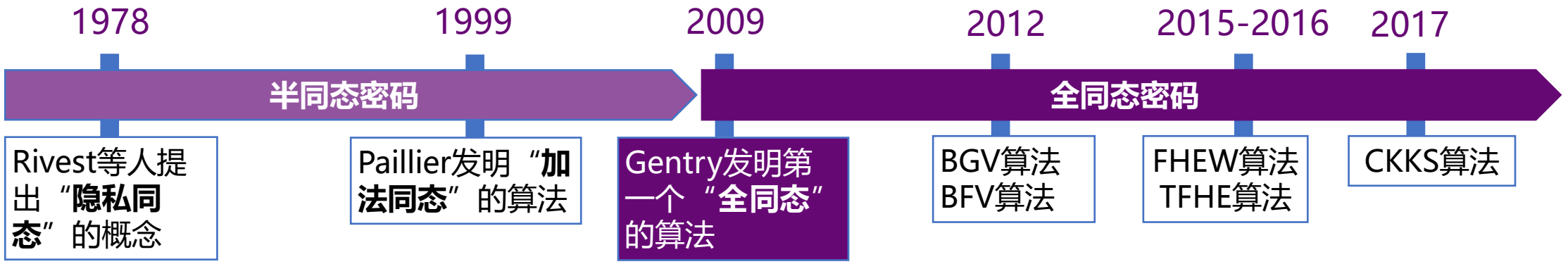
“我要出去怎么能不被吃掉？” ——**给敏感数据穿“铠甲”**

漏洞怎么也堵不住。。。

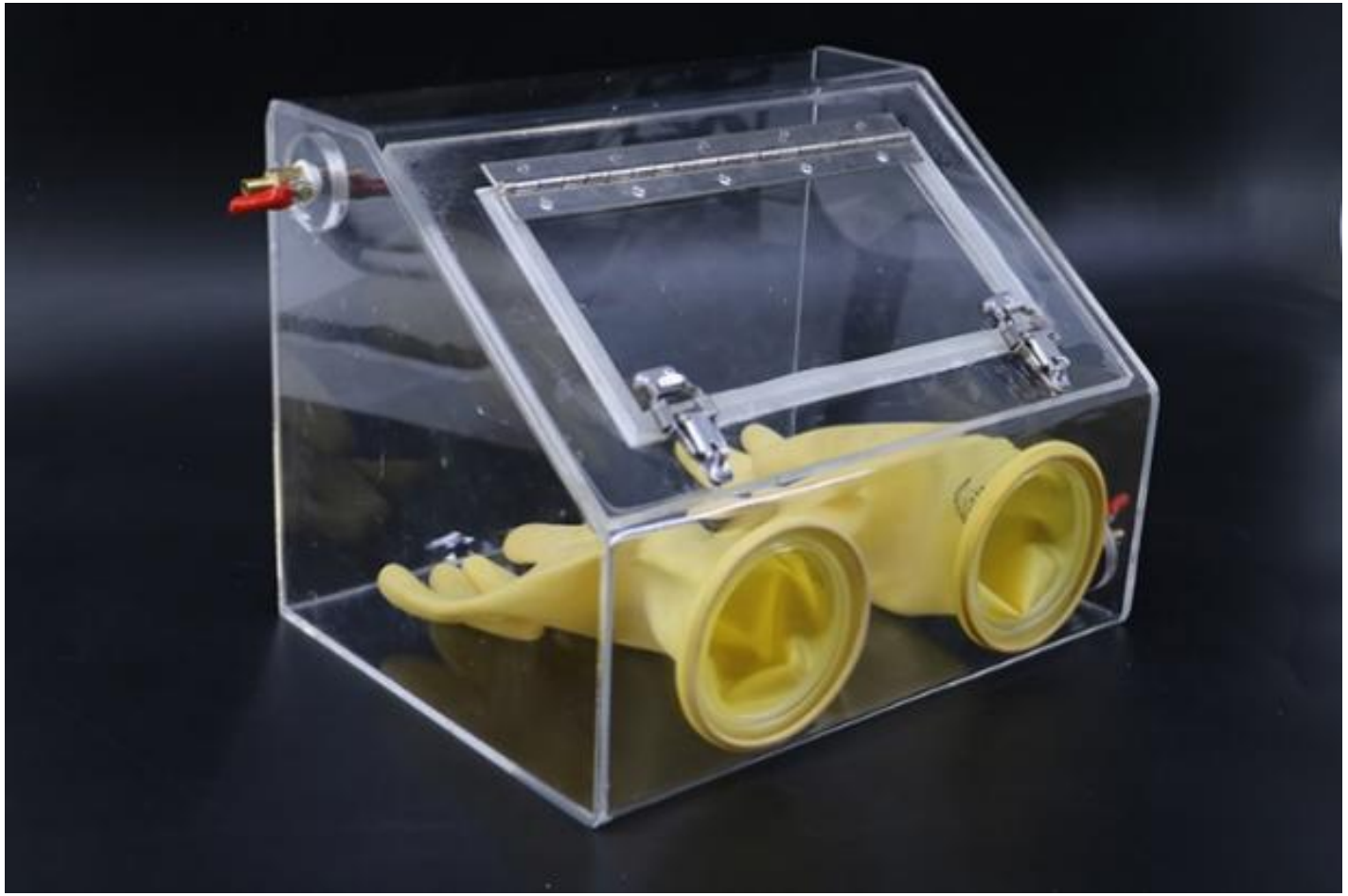
基于现代密码学的数据安全保护——FHE

- 全同态加密（FHE）是支持“**在密文域上进行任意计算**”的加密算法。





基于现代密码学的数据安全保护——FHE



是否有办法确保数据“绝对安全”？可用不可见、可算不可得！

全同态加密的重要作用

全同态加密是隐私保护计算的重要手段

Fully Homomorphic Encryption

Idea: Outsource computation w/o revealing inputs.

Enc(x)

Enc(f(x))

User: Has input x,
Wants f(x)

Cloud: has f(·)

通信成本

降低计算供应商数据安全方面的成本

信任成本

吸引更多用户将数据和计算迁移至云端

丰富应用

打破数据孤岛，用于联邦学习

数据安全

实现数据存储加密,保障数据安全

安全成本

减少通信代价，平衡各方的计算代价

Homomorphic Encryption

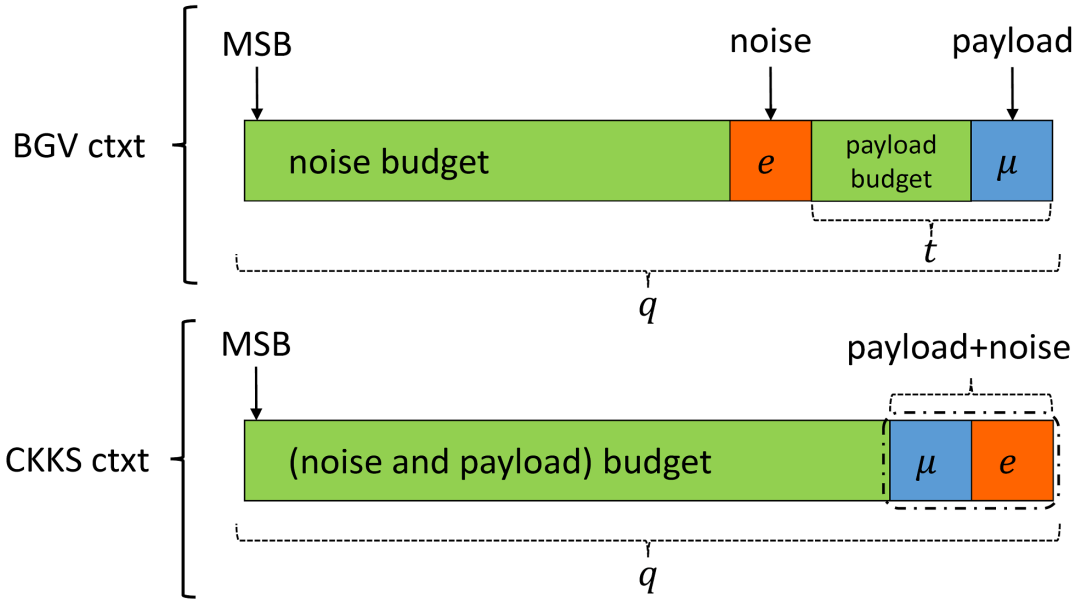
全同态加密可以在不交换明文数据的情况下依然进行业务计算

全同态加密落地的最大挑战——性能开销

保证密文计算结果正确性的前提下，提高计算性能是当前世界公认的难题！

- 计算非常复杂，运算速度慢，密文显著扩张
- 需要大量计算资源支持，现有CPU无法运行

应用	同态加密方式	明文数据长度	密文数据长度	明文计算时间	密文计算时间
联邦学习模型训练	CKKS	30.5 KB	**1.33 GB (5.2万倍)**	0.145 秒	**390.6 秒 (2694倍)**
神经网络推理	CKKS	29.9 MB	**546.8 GB (1.9万倍)**	212.16 秒	**112,026.16 秒 (528倍)**
保密数据库查询	BGV	0.71 KB	**1.58 GB (40万倍)**	0.053 毫秒	**7401.49秒 (1.4 亿倍)**



全同态加密落地的最大挑战——性能开销

应用	总存储器访问（未加密 / 加密）	理论带宽需求	Runtime（未加密，无内存访问限制）	Runtime（加密，无内存访问限制）
线性回归（训练）	48.63MB / 538.5GB	**3.37 TB/s**	0.145 s	**390.6 s (2,693.8x)**
线性回归（测试）	26.19MB / 28.6GB	**1.99 TB/s**	13.48 ms	**2.44 s (181.4x)**
MNIST 推理	19.25GB / 62,408.5GB	**273.28 GB/s**	212.16 s	**112,026.16 s (528.0x)**
矩阵相乘	0.565 GB / 1,683.52 GB	**1.49 TB/s**	1.1 s	**1,838.5 s (1,111.76x)**

实验参数配置：10-core / 20-thread, 2.2GHz Xeon Silver E4114 CPU×2; DDR4, 2666 MHz DRAM; 4TB SATA III hard drive
DDR4 2666MHz峰值带宽：21.3 GB/s

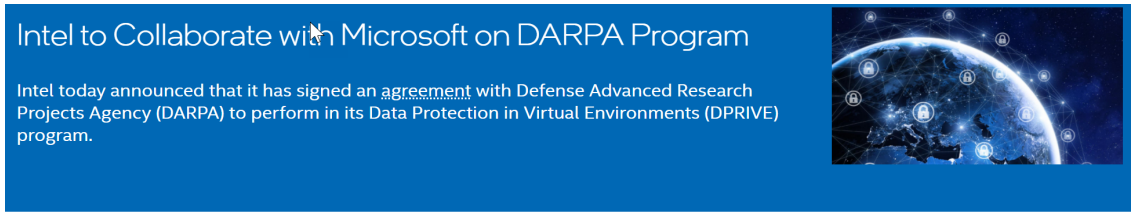
全同态加密落地的最大挑战——性能开销

- **美国**

军方研究单位DARPA于2019年陆续启动项目，**研究新一代软硬件隔离的安全数据流通计算架构、数据隐私处理芯片和硬件加速器**，特别针对同态加密的硬件加速，**总预算额约1亿美元，微软、IBM、英特尔、通用电气等参与芯片设计和软件库开发。**

- **欧盟**

批准HEAT项目，旨在研究**加密的方式处理敏感数据**，保护个人隐私信息的新型软硬件系统架构。



News
- March 8, 2021
- Contact Intel PR

More Security News →

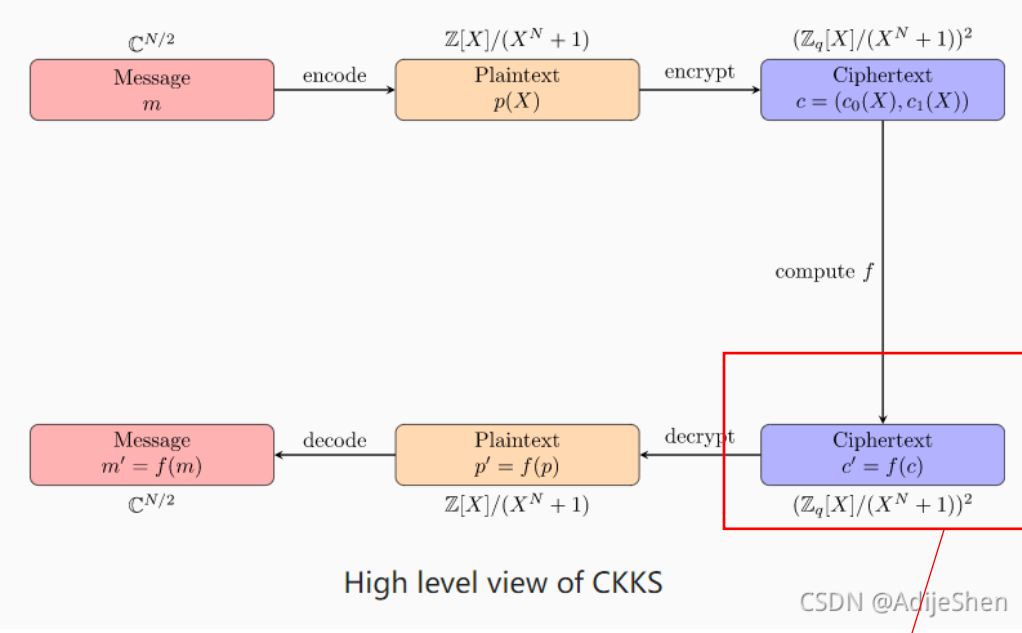
Tags
Security

What's New: Intel today announced that it has signed an agreement with Defense Advanced Research Projects Agency (DARPA) to perform in its Data Protection in Virtual Environments (DPRIVE) program. The program aims to develop an accelerator for fully homomorphic encryption (FHE). Microsoft is the key cloud ecosystem and homomorphic encryption partner leading the commercial adoption of the technology once developed by testing it in its cloud offerings, including Microsoft Azure and the Microsoft JEDI cloud, with the U.S. government. The multiyear program represents a cross-team effort across multiple Intel groups, including Intel Labs, the Design Engineering Group and the Data Platforms Group, to tackle "the final frontier" in data privacy, which is computing on fully encrypted data without access to decryption keys.

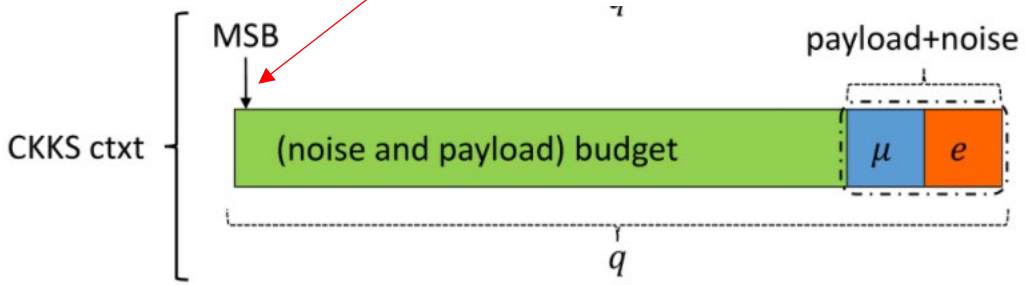
全同态加密落地的最大挑战——性能开销

- 密文乘法的基本步骤
  - （1）编码encode
  - （2）加密encryption
  - （3）多项式换成点值表示NTT
  - （4）重线性化relinearization（keyswitch）
  - （5）重缩放rescale

为何开销如此之大?



High level view of CKKS



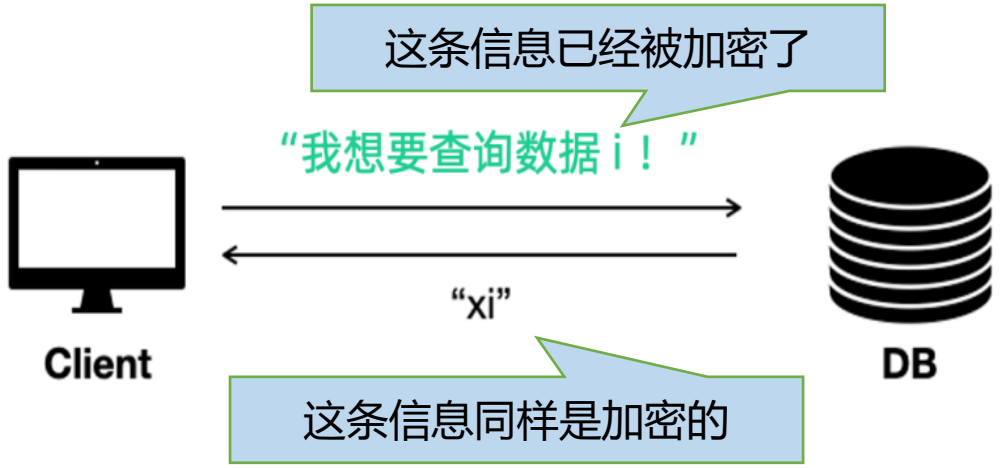
$$\begin{aligned}\mathrm{Dec}(c)\cdot\mathrm{Dec}(c') \mod q &= (c_0+c_1\cdot s)\cdot(c_0'+c_1'\cdot s) \mod q\\ &= c_0\cdot c_0' + (c_0\cdot c_1' + c_0'\cdot c_1)\cdot s + c_1\cdot c_1'\cdot s^2 \mod q\\ &= d_0 + d_1\cdot s + d_2\cdot s^2 \mod q\end{aligned}$$

这里$d_0 = c_0\cdot c_0' \mod q, d_1 = (c_0\cdot c_1' + c_0'\cdot c_1) \mod q, d_2 = c_1\cdot c_1' \mod q$

为何开销如此之大?

PIR应用简介

隐私信息检索（Private Information Retrieval），也称匿踪查询，是安全多方计算中非常实用的一门技术与应用，可以用来保护用户的查询隐私，进而也可以保护用户的查询结果。其目标是保证用户向数据源方提交查询请求时，在查询信息不被感知与泄漏的前提下完成查询。即对于数据源方来说，只知道有查询到来，但是不知道真正的查询条件、也就不知道对方查了什么。



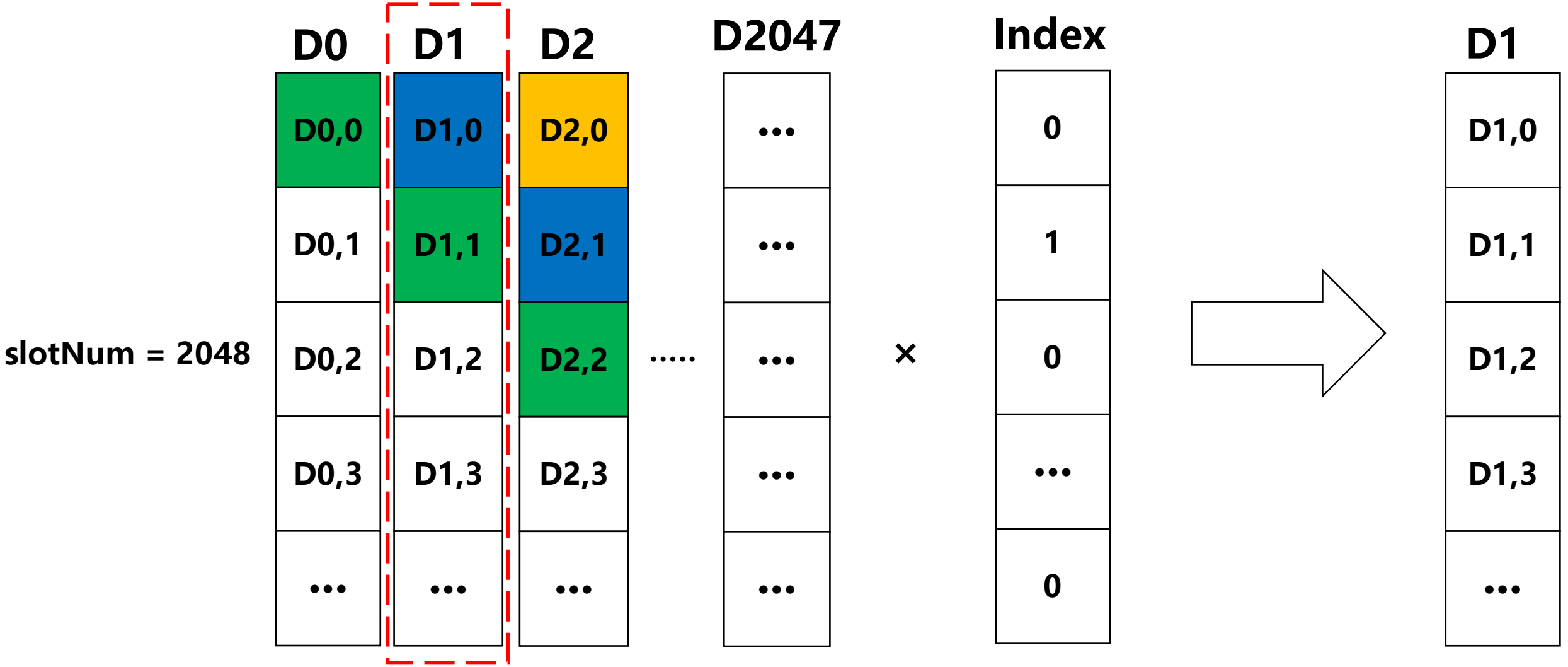
查询流程

1.数据方在数据库中存储的数据格式为<key, value>的格式;
2.查询方使用其要查询的key，进行加密后去数据方查询对应的value;
3.在查询过程中数据方无法获知查询方的key具体是多少，也并不清楚最终发送了哪条value给了查询方。

为何开销如此之大?

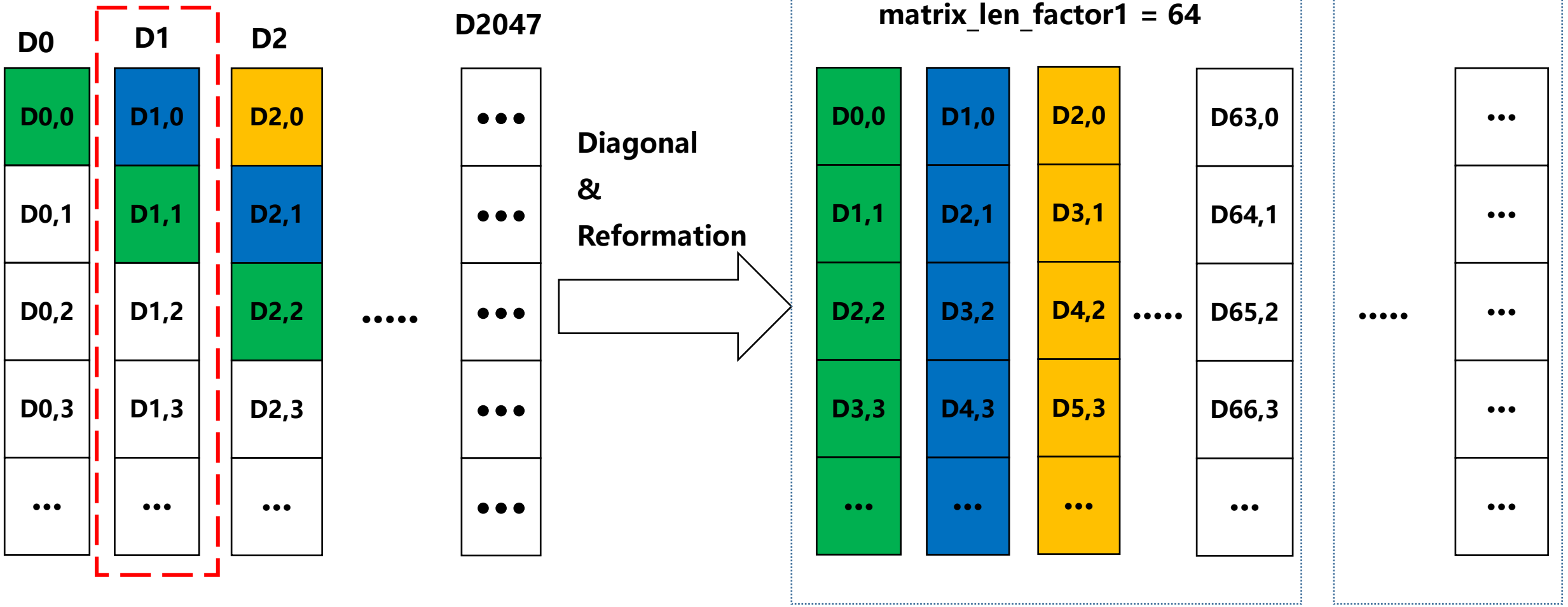
PIR矩阵构造方法

实际场景中
index是加密的



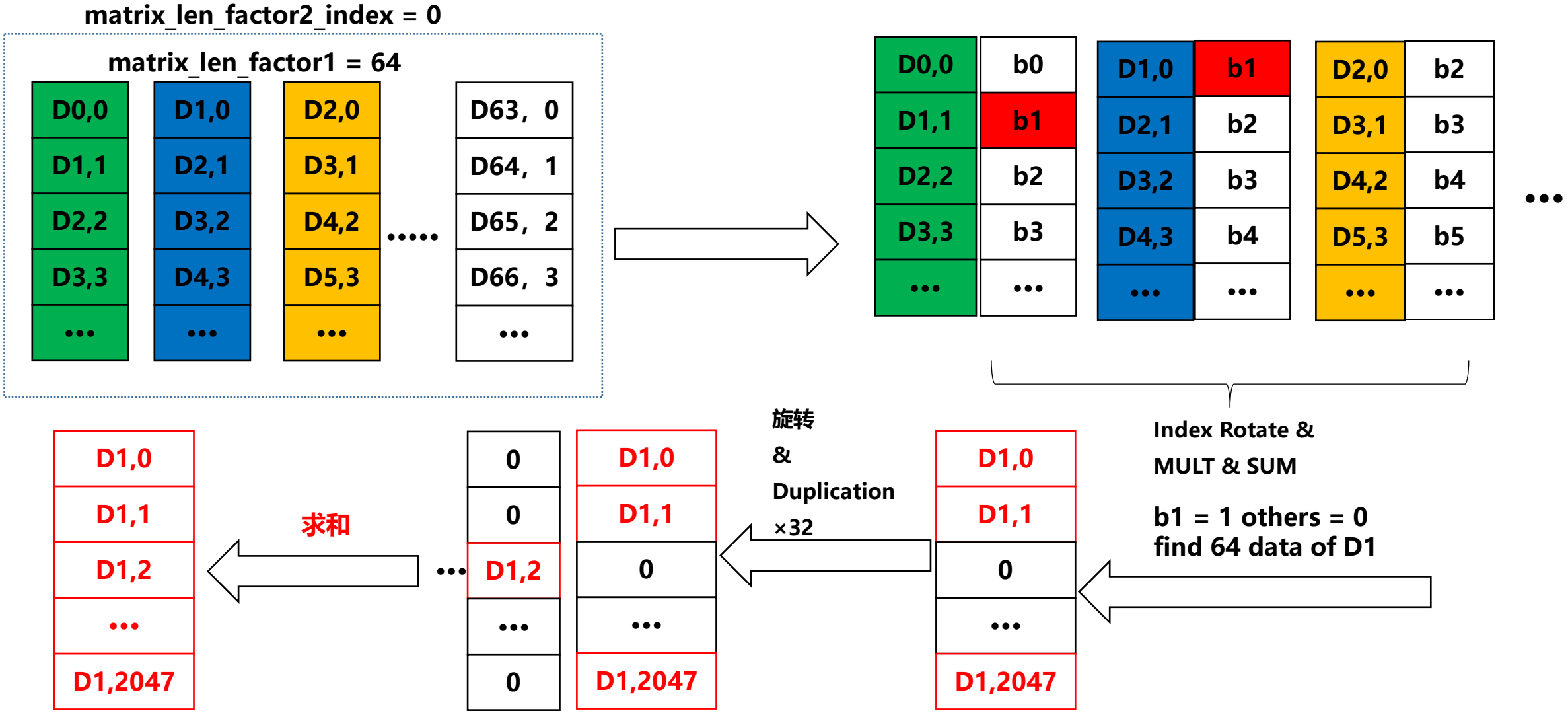
为何开销如此之大?

PIR矩阵构造方法



为何开销如此之大?

PIR矩阵构造方法



软硬件协同设计

通用FHE加速器

CKKS BFV TFHE

应用专用FHE加速器

CNN 01

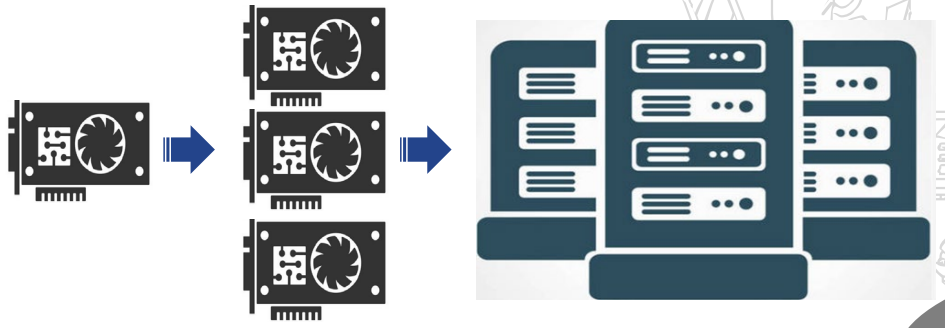
GNN 02

ML 03

LLM 04

PIR 05

PSI 06



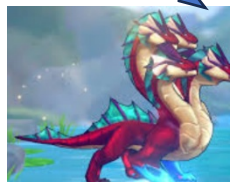
单卡 多卡 集群化

可扩展FHE加速器

软硬件协同设计

可扩展

Hydra (HPCA 2025)
可扩展的FHE深度学习
推理加速器设计

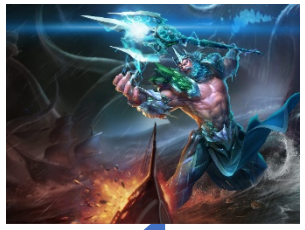


GNN

Uranus (ICCAD 2025)
基于FHE的高效密态图
神经网络推理加速器

CNN

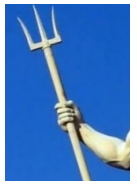
Athena (MICRO 2025)
量化卷积神经网络密态
推理框架和加速器



Poseidon (HPCA 2023)
Poseidon-NDP (TCAD 2023)
Hypnos (DAC 2025)
通用全同态加速器设计

通用

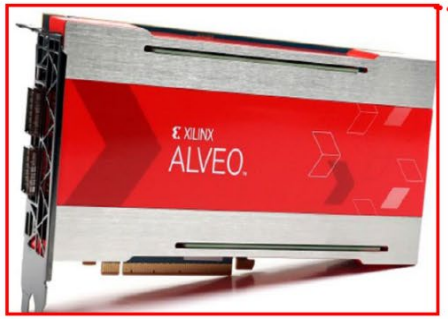
PSI



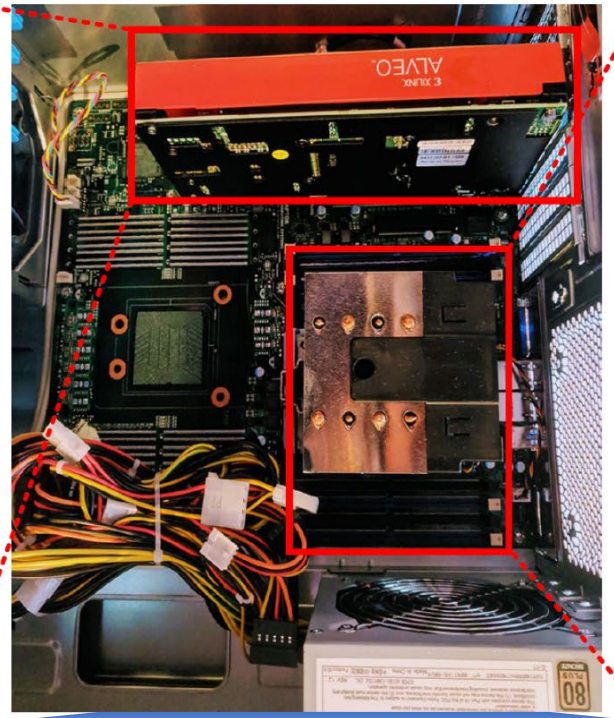
Trident (TC 2024)
Ares (DAC 2025)
基于FHE的隐私求
交软硬件协同加速

从理论到实践——国内首个FHE硬件加速器架构

技术对标：
1. 业界首次支持全同态加密的SoC，安全性更高
2. 首个全同态加速器算法库Poseidon



U280	
Storage	
HBM	8 GB
DRAM	32 GB
FPGA	
Device	xcvu37p
LUT	1304 k
FF	2607 k
DSP	9024
BRAM	70.9 Mb



CPU	
Core:	10-core Intel Xeon Silver 4114
Frequency:	2.2GHz
Threads:	20
TDP:	85W
DRAM	
Capacity:	64 GB x 4
Interface:	DDR4
Frequency:	2666 MHz
SSD	
Capacity:	256 GB
Interface :	SATA 3.0
HDD	
Capacity:	4 TB
Interface:	SATA 3.0

HPCA 2023 高分录用!
团队是国内首次在体系结构4大顶会上发表全同态处理器论文，技术得到了学术界认可。

	CPU (Xeon)	Over 100x (GPU) [21]	HEAX (FPGA) [32]	Poseidon (FPGA)	speedup
HAdd	35.56	4807	4,161	13,310	**374**×
PMult	38.14	7,407	4,161	13,310	**349**×
CMult	0.38	57	119	273	**718**×
NTT	9.25	/	237	12,474	**1,348**×
Keyswitch	0.4	/	104	312	**780**×
Rotation	0.39	61	/	302	**774**×
Rescale	6.9	1,574	/	3,948	**572**×

	LR [19]	LSTM [27]	ResNet-20 [28]	Packed Bootstrapping [30]
F1+ (ASIC)	639	2,573	2,693	58.3
CraterLake (ASIC)	119.52	138.0	249.45	3.91
BTS-1 (ASIC)	39.9	/	1,910	/
BTS-2 (ASIC)	28.4	/	2,020	/
BTS-3 (ASIC)	43.5	/	3,090	/
ARK (ASIC)	7.717	/	294	/
over100x (GPU)	775	/	/	/
Poseidon (FPGA)	**72.98**	**1,848.89**	**2,661.23**	**127.45**

软硬件协同——FHE算子库“Poseidon”

软硬件协同技术提升FHE的硬件性能

框架和上层业务逻辑

FATE　PrimiHub 原语　保护数据在应用过程中的隐私安全　隐语 SECRET FLOW 可信隐私计算框架

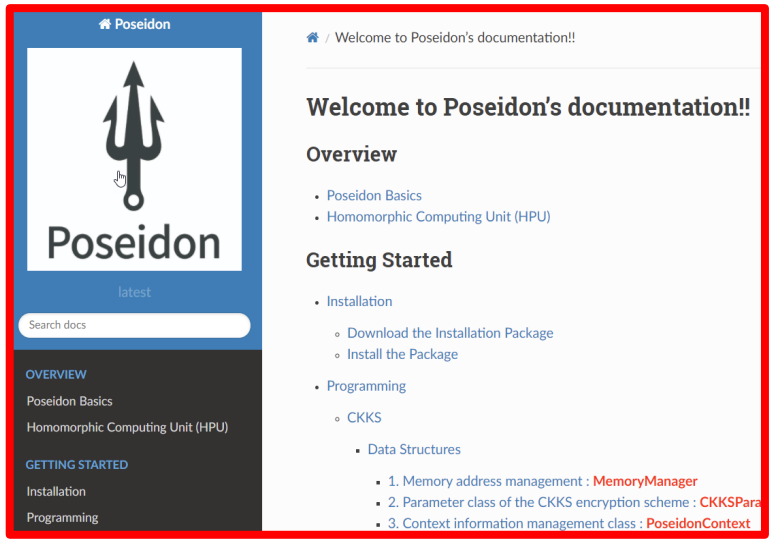
调用　支持

编译器

算法库：CKKS、BGV、BFV等

基本操作库（如自举）

驱动程序

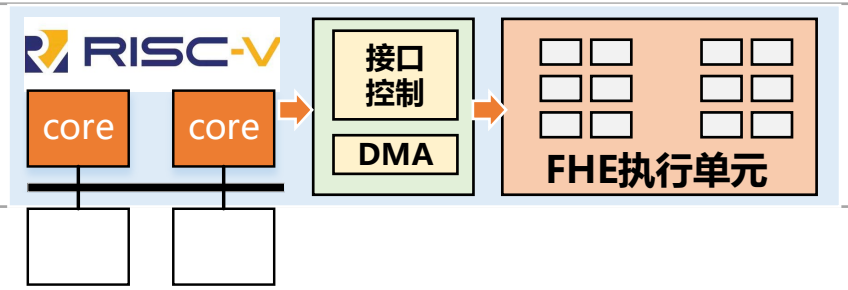


自主研发“翠湖”FHE软件栈，包含数十种复杂密态计算操作，支持快速密态数据库查询

https://poseidon-hpu.readthedocs.io/en/latest/

硬件基本算子

“翠湖”全同态硬件加速卡



在FPGA上提升200~300倍

指标类别	名称	Intel Platinum 8160（时间：s）	翠湖“全同态协处理器”（时间s）	加速比
函数级操作 (degree=32768, Q=640bit)	密文-密文加减（HAdd、HSub）	0.1132	0.0092	226.4
	密文-密文乘（HMult）	3.2173	0.2476	208.9
	密文-明文加减（PAdd、PSub）	0.0541	0.0075	135.3
	密文-明文乘（PMult）	0.1123	0.0067	224.6
	旋转（Rotate）	3.7496	0.2583	248.3
	共轭（Conjungate）	2.8623	0.2855	187.1
	系数转点值（Ftt）	0.3952	0.0066	304.0
	点值转系数（IFtt）	0.4083	0.0071	291.6
	重缩放（Rescale）	0.9315	0.0204	245.1
高层次复杂操作 (degree=32768, Q=640bit)	自举（Bootstrap）	610.7011	85.8794	161.5
	矩阵相乘（MatrixMult）	2267.6586	272.6833	153.9
	系数到槽(Coeff to slot)	139.3284	16.1165	169.7
	槽到系数(Slot to coeff)	235.9373	27.0728	155.3

胜利了！

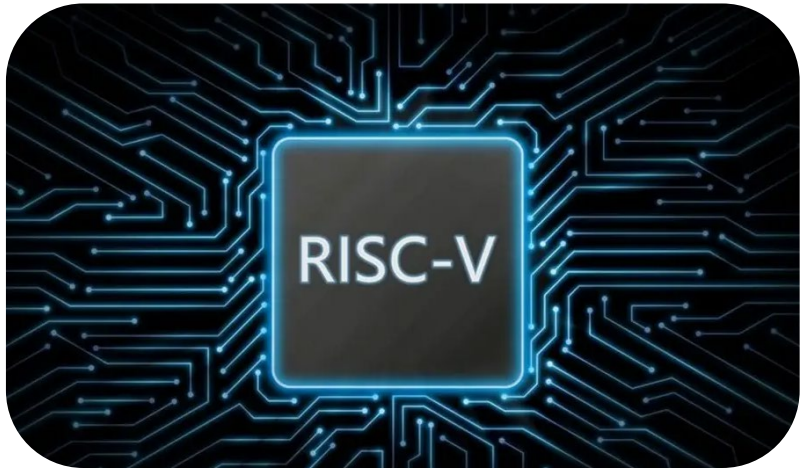

计算系统
PLANTS
VS.
ZOMBIES
PopCap


第二届『隐语杯』数据挑战赛
2026
赛道：密态大模型推理的隐私保护
二等奖
赛队：迫击炮隐私推理小队
第二届『隐语杯』数据挑战赛
2026
赛道：基于全同态加密的最近邻选取
二等奖
赛队：ICTPoseidon

OUTLINE

重塑计算系统安全

基于RISC-V的计算系统安全增强

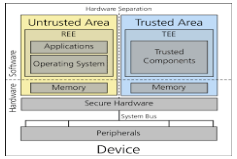


现有国产处理器的安全策略概览

CPU厂商	型号	指令集架构	性能参数(核数，主频)	工艺制程	主要安全策略
海光	7285	X86	32核，2.0 GHz	14nm	安全启动 虚拟化加密 SM3/4国密算法加速 熔断幽灵漏洞防范 控制流完整性保护 可信执行环境
兆芯	KH-30000	X86	8核，2.7 GHz	16nm	SM3/4国密算法加速
龙芯	3A/5000	龙arch	4核，2.3-2.5 GHz	12nm	SM2/3/4国密算法加速 熔断幽灵漏洞防范 可信执行环境
飞腾	FT-2000/4	ARM	4核，2.2/2.6 GHz	16nm	安全启动 可信执行环境 密钥管理、安全存储
申威	SW3231	Alpha	32核，2.4 GHz	16nm	可信执行环境 基于 AI 的恶意软件检测

国产处理器安全整体态势：性能在追赶、安全补短板



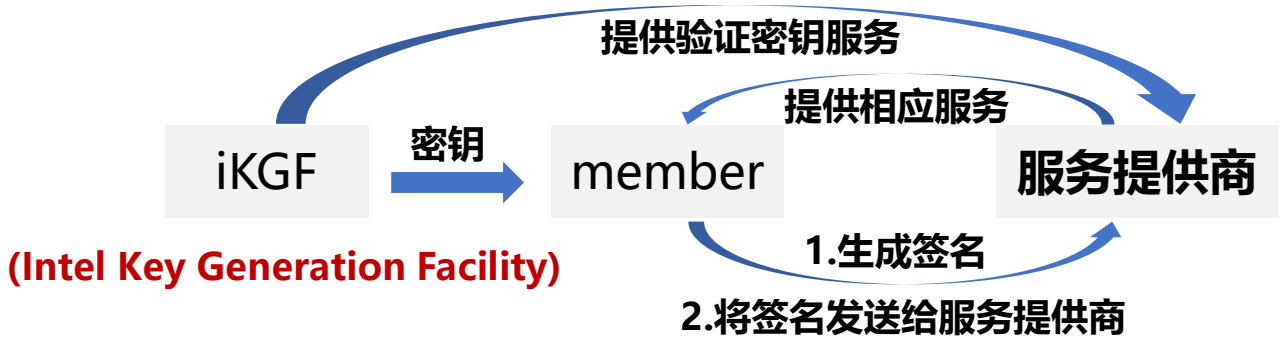


国产处理器	SPEC性能	加解密性能	硬件漏洞防护	可信执行环境	对标国外处理器
海光 7285 (2019年)	略差	超越	持平		AMD EPYC 7542 (2019年)
龙芯 3A5000 (2021年)					Intel i5-7200u (2016年)
飞腾 FT-2000/4 (2019年)					Intel i5-6400 (2015年)
兆芯 KH-30000 (2019年)					Intel i5-7400 (2017年)



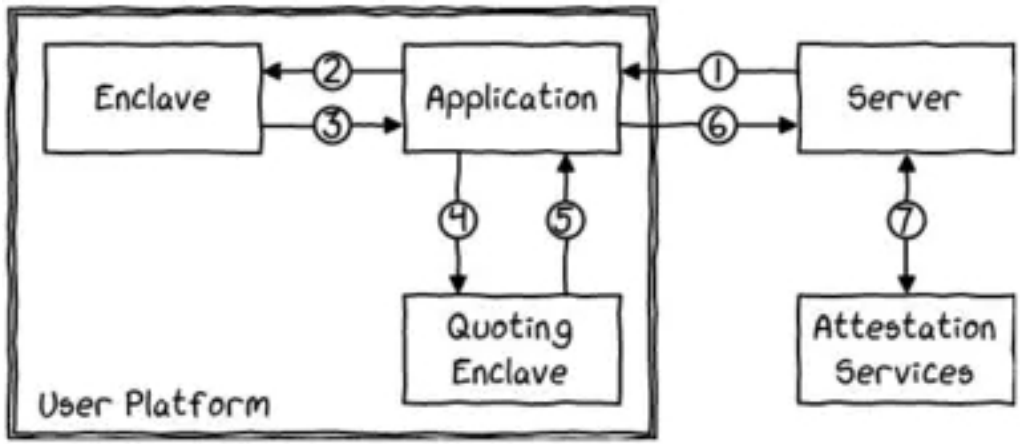

现有国产处理器的安全策略概览

Intel密钥注入流程



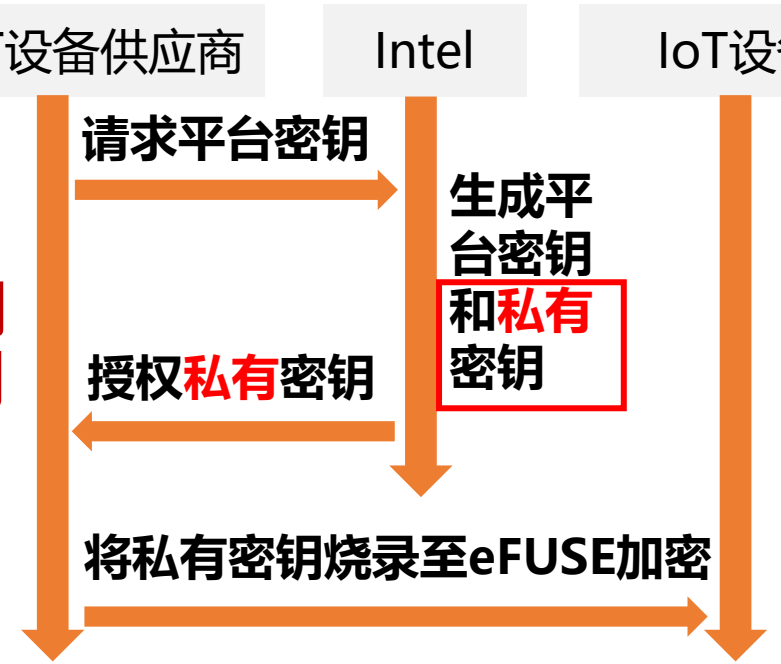
Intel知晓任何一台机器的密钥信息

SGX的远程认证过程



认证服务器位于美国

Intel SGX密钥授权机制



资料来源：https://www.jianshu.com/p/3b11e1b995fd

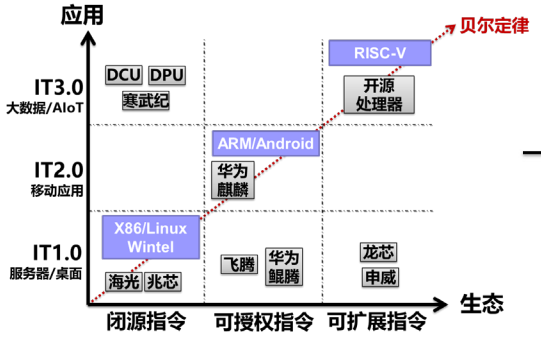
“重塑计算系统安全”如何破局？——RISC-V

CPU架构	基于x86架构CPU	基于ARM 架构授权国产CPU	申威、龙芯等国产CPU	基于RISC-V国产CPU
自主可控测评	难以满足要求	现阶段能满足要求，未来发展存在变数	能满足要求	**可望满足要求**
既有生态状况	成熟	成熟	发展中	**起步中**
新兴市场预测	不详	不详	不详	**前景看好**
开放创新	**不开放，难创新**	**不开放，难创新**	**不开放，难创新**	**开放，易创新**
授权费用	缺乏成熟的授权模式	架构授权费用高	无	**无**

RISC-V将成为主流计算系统生态

- **历史上，成为主流计算系统的标志**
  - X86在数据中心场景的标志——用X86芯片研制的超算进入Top500前十
  - ARM在终端场景的标志——Android手机市场崛起
  - GPU在数据中心场景的标志——大规模AI模型训练的广泛应用
- **目前：RISC-V 12年出货量累计超100亿颗，中国公司占据半壁江山[1]**
- **预测：2020-2025年增长率达115%， RISC-V应用数量将增至850亿颗[2]**
- **预测：2024年进军手机市场，2027年杀入服务器市场[3]**

代表实体	模式	营业额	利润	赋能产业
Intel	IDM + 芯片销售	>500亿美元	>100亿美元	PC产业
Nvidia	Fabless + 芯片销售	~150亿美元	~30亿美元	AI产业
ARM	Fabless + IP销售	~20亿美元	~3亿美元	智能手机产业
开源芯片?	**Fabless + 开源IP + 开放流程**	**~2亿美元 （众筹）**	**0 非盈利机构**	**AIoT 产业**



标准规范

RISC-V国际基金会

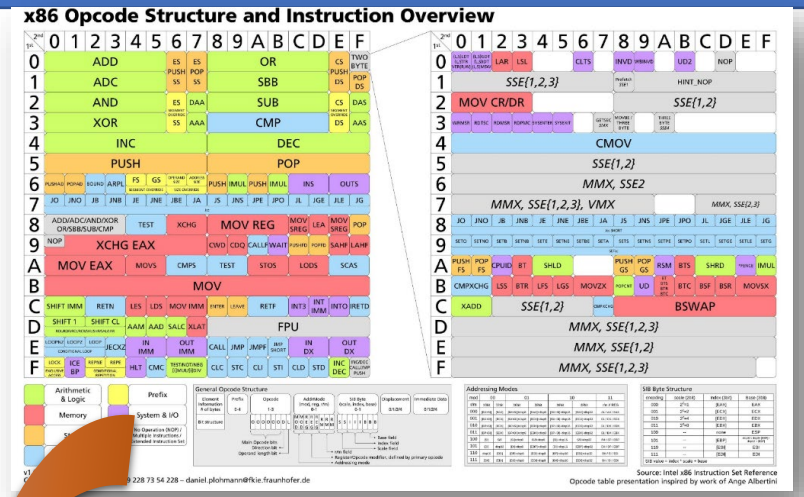
产品实现

HiFive芯片
美国SiFive公司

D1-H芯片
平头哥/全志

香山芯片
中科院/鹏城实验室

指令集➔微架构➔芯片➔系统软件全栈安全性可定制

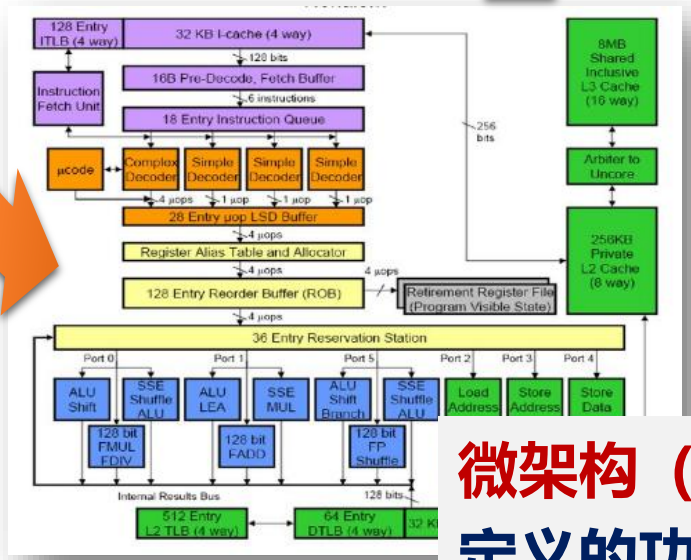


指令集是规范，定义
指令的格式、功能

芯片产品

安全性可自由定制！

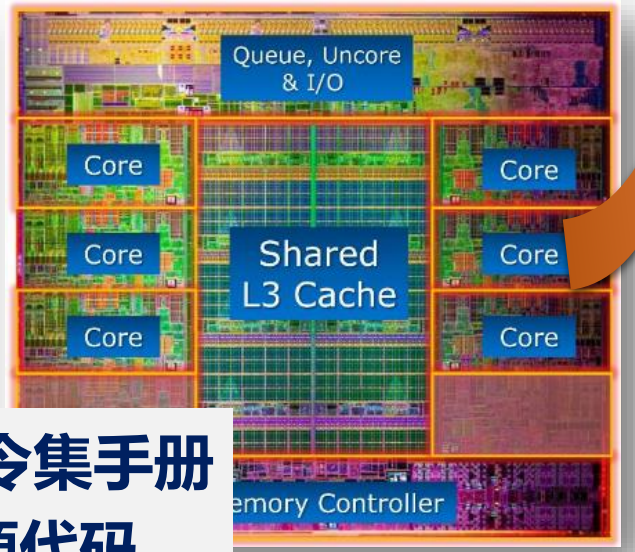
微架构设计 → 工程开发 → RTL代码 → EDA工具 → 芯片版图




```
component DebugCoreTop is
    port (
        -- Trigger and Data
        cu_Clk      : in    std_logic_vector(2 downto 0) := (others => '0');
        cu0_Trig    : in    t_trig_0 := (others => (others => '0'));
        cu1_Trig    : in    t_trig_1 := (others => (others => '0'));
        cu2_Trig    : in    t_trig_2 := (others => (others => '0'));
        cu0_Data    : in    t_data_0 := (others => (others => '0'));
        cu1_Data    : in    t_data_1 := (others => (others => '0'));
        cu2_Data    : in    t_data_2 := (others => (others => '0'));

        -- Downstream I2C
        SCL         : in    std_logic := '0';
        SDA         : inout std_logic := '0';

        -- Upstream
        gt_RefClk_p : in    std_logic := '0';
        gt_RefClk_n : in    std_logic := '0';
```



微架构（microarchitecture）设计，就是将指令集手册定义的功能实例化，然后通过工程开发，变成源代码

实现我国计算系统安全核心技术自主可控

RISC-V基金会不受制于美国政府

- 威斯康星州共和党代表迈克•加拉格尔（Mike Gallagher）、阿肯色州共和党参议员汤姆•科顿（Tom Cotton）均表示反对将RISC-V总部转移出美国
- 但RISC-V不是一般的商品，它是**处理器指令集规范**，并采用”Creative Commons Attribution 4.0 International License“开放共享协议，在**法律上不受美国出口管制**
- 从制裁华为角度来看，RISC-V确实可以**绕过美国的出口管制**。即使在总部留在美国，**中国企业做RISC-V芯片卖给华为也不受美国出口管制影响**

从理论到实践

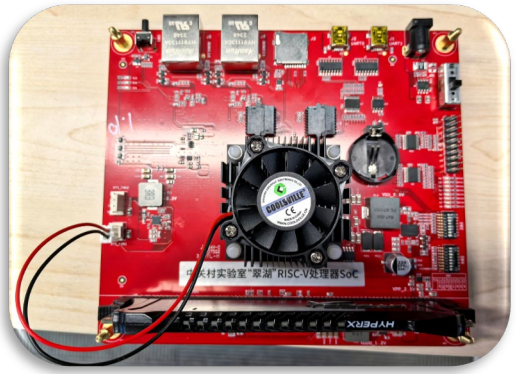
前端机 @上海

服务器 @北京

人脸提取和特征采集
显示比对结果

1、人脸特征向量（敏感信息）

5、解密



2、人脸特征加密

3、密态比对

4、密态比对结果返回

翠湖在**TEE中进行全同态加密密钥由可信根提供**，全同态加密的人脸特征通过网络发送给服务器

数据库中是密态的人脸信息，在密态下进行人脸比对（使用翠湖全同态协处理器）

从理论到实践

OUTLINE

一、安全可信的核心技术——机密计算

- “我怎么能不让它们进来？以及“我自己怎么才能安全的进来？”——**给应用提供安全屋**

二、未来敏感数据保护的主流技术——密态计算

- “我要出去怎么能不被吃掉？”——**给敏感数据穿“铠甲”**

三、重塑计算系统安全

- 基于RISC-V的计算系统安全增强

四、总结和未来展望

总结和未来展望

美国国防高级研究计划局6个技术办公室

国防科学办公室

- 新型材料与结构
- 传感与测量
- 计算与处理
- 支持操作
- 集体智能
- 新兴威胁

生物技术办

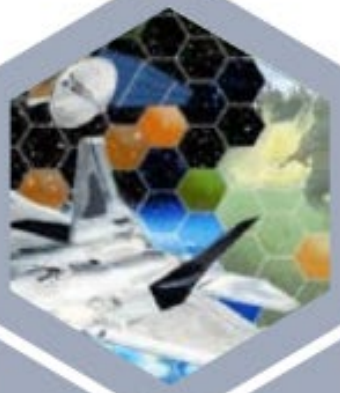
- 作战支援能力
- 战术作战人员护理与功能恢复
- 战略韧性与后勤安全
- 感知并应对新兴威胁

信息创新办

- 先进AI技术
- 网络作战优势
- 信息领域的信心
- 弹性、适应性和安全性的系统

微系统技术办

- 量子、光子和有机电路
- 新型微系统制造生态系统
- 军民两用设计



战略技术办

- 先进传感器与处理技术
- 战场效应
- 指挥、控制与通信
- 系统战
- 国家韧性

战术技术办

- 颠覆性平台与系统
- 硬件设计、开发、测试、制造及维护的重新构想
- 专注于快速、经济且可扩展的部署

总结和未来展望

2025年年中，通过对DARPA 265项在研项目进行了梳理，经初步分析，发现：

- DARPA的布局清晰地表明，美国已将与中国的长期战略竞争作为其国防科技发展的核心驱动力。
- 其战略核心是利用技术代差来抵消我地缘和规模优势，力图在未来的冲突中实现"零伤亡"和"外科手术式"打击。
- "脱钩"和"自主"成为底层逻辑，从后勤到核心技术，正在追求摆脱对外部（特别是中国）的依赖。

项目分类

5. 网络、信息战与通信 (Cyber, Information Warfare & Networking)

- **软件安全与保障:** 可信微补丁 (AMP), 软件自动快速认证 (ARCOS), 不透明处理器上的持续正确性 (COOP), 划分与权限管理 (CPM), 增强型软件物料清单优化软件维护 (E-BOSS), 网络物理系统虚实集成逆向工程与利用 (FIRE), 抵御突现执行引擎的开发工具链加固 (HARDEN), 意图定义自适应软件 (IDAS), 智能安全工具生成 (INGOTS), 支持鲁棒系统的验证器流水线推理 (PROVERS), 安全文档 (SafeDocs), 将所有C代码翻译为Rust (TRACTOR), 大型遗留软件的验证安全与性能增强 (V-SPELLS)
- **网络攻防与弹性:** 安全测试与学习环境的网络代理 (CASTLE), 大规模网络狩猎 (CHASE), 退化、中断、间歇和受限网络下的流体作战 (FLUID), 保证物理安全的架构 (GAPS), 生成可操作的通信渠道 (GeCCO), 任务集成网络控制 (MINC), 可证明的怪异网络部署和检测 (PWND2), 面向所有人的弹性匿名通信 (RACE), 攻陷期间总线系统回收 (Red-C), 利用操作知识和环境进行签名管理 (SMOKE)
- **数据安全与取证:** 业务流程逻辑 (BPL), 人机通信促进义务推理开发运维 (CODORD), 虚拟环境中的数据保护 (DPRIVE), 确保系统信息一致性 (ECoSystemic), 语义取证 (SemaFor), 加密验证与评估信息安全 (SIEVE)
- **通信节点:** 开放、可编程、安全的5G (OPS-5G), 天基自适应通信节点 (Space-BACN)

TEE

FHE

集群三：微电子与可信硬件

重大项目群

- **项目群:** 通用异构集成与IP复用策略 (CHIPS), 自动化安全芯片实现 (AISS), 下一代微电子制造 (NGMM), 通过硬件和固件的系统安全集成 (SSITH), 联合大学微电子计划 2.0 (JUMP 2.0), 新型计算所需的基础 (FRANC)。
- **战略意图:** 在半导体领域与中国"技术脱钩"，并建立一套完全自主可控、从设计、制造到封装都"美国化"的军事微电子生态。通过架构创新（如Chiplet）和硬件安全（如SSITH）构建下一代技术护城河。美国不仅要在存量上"卡脖子"，更要在增量上"立标准、造壁垒"。 下一代微电子制造 (NGMM)旨在本土建立3D异构集成（3DHI）中心。通用异构集成与IP复用策略 (CHIPS) 和特定领域片上系统 (DSSoC) 正在推广"芯粒"(Chiplet)模式。自动化安全芯片实现 (AISS) 和 通过硬件和固件的系统安全集成 (SSITH) 表明美国对其硬件供应链的极度不信任。

总结和未来展望


SSITH
远望防务映像
TECHXCOPE
SSITH汽车验证机将SSITH安全处理器技术整合到汽车电子控制系统的核心中
DARPA
DARPA

总结和未来展望

DESIGNLINES | AI & BIG DATA DESIGNLINE

Niobuim Raises $5.5 Million, Tapes Out FHE Chip

By Sally Ward-Foxton 06.05.2024 0

Share Post Share on Facebook Share on Twitter

Intel Completes DARPA DPRIVE Phase One Milestone for a Fully Homomorphic Encryption Platform

Subscribe

Fully homomorphic encryption (FHE) accelerator startup Niobium has taped out its first chip and raised $5.5 million in seed funding. Niobium's initial chip will accelerate FHE by a factor of 1,000-5,000 versus standard CPUs, Niobium CEO Kevin Yoder told EE Times.

总结和未来展望

Intel Completes DARPA DPRIVE Phase One Milestone for a Fully Homomorphic Encryption Platform

Creating a Five Order of Magnitude Faster FHE Accelerator

To achieve real-time FHE, Intel signed an agreement with Defense Advanced Research Projects Agency (DARPA) in 2021 to take part in its Data Protection in Virtual Environments (DPRIVE) program. As part of the selection announcement, DARPA program manager Tom Rondeau noted “We currently estimate we are about a million times slower to compute in the FHE world then we are in the plaintext world. The goal of DPRIVE is to bring FHE down to the computational speeds we see in plaintext. If we are able to achieve this goal while positioning the technology to scale, DPRIVE will have a significant impact on our ability to protect and preserve data and user privacy.” Intel’s role in the project is to develop a platform with the orders-of-magnitude faster performance capability that can perform real-time FHE in a form factor that can be plugged into a conventional computer system.[ii] Scalability obviously occurs according to the number of FHE accelerated nodes in a cloud or compute cluster.

🚀 DPRIVE计划的意义与未来展望

DPRIVE计划的成功，意味着我们有望在**不泄露任何原始数据内容**的前提下，对加密数据进行各种复杂的分析和计算（比如在云服务器上直接处理加密的医疗数据或金融交易记录）。这将极大地提升云计算和数据协作中的隐私安全水平，解决所谓的“**数据保密性的最后一英里差距**”[2]。

总结和未来展望

如何“重塑”这座房子，让它更安全？

- **现在：** 构建国产、安全的TEE，实现软硬件协同安全
- **未来：** 支持全同态加密等密态计算以及新型密码
- **同步：** 创新硬件微架构，防范硬件安全漏洞

HarmonyOS 麒麟 OS 蓬莱

不断完善： 硬件安全漏洞修复，侧信道攻击防范

已有基础： 可信固件，安全启动，密钥安全管理

高性能CPU → “安全”高性能CPU

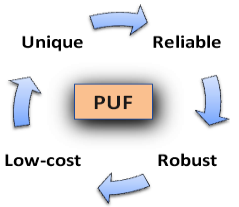
构建安全操作系统　　国产可信执行环境

还需加强： 软硬件协同的硬件攻击防范

弯道超车： 发展新型安全增强技术

密态计算、新型密码

新型可信根



计算系统对网络空间安全意义重大
是核心环节和基石！
重塑计算系统安全任重而道远！

软硬件协同的计算系统安全

从理论到实践

01部 路 航