# 隐语架构概览

## 架构介绍

(底层)

硬件层，支持常规设备（FPGA/GPU）、可信环境设备（intel SGX2）

资源层，Kuscia，可以管理数据、网络、计算资源、应用

计算层，MPC、HE、TEEU、TECCU

算法层，PSI/PIR，data analysis, FL

产品层，白屏产品+黑屏API、SDK

(顶层)

通用能力：

互联互通：白盒、黑盒、异构TEE

跨域管控：三权分置、密态存储、全栈审计

## 设计原因

1、完备性，有多种计算方式

2、希望分层之间低耦合，层内部高内聚。方便用户从任意一层开始集成

3、专业人员可以在自己擅长的一层发挥

# 隐语架构拆解

## 产品层

包含白屏和黑屏两大块。

产品定位：

1、通过可视化产品降低终端用户的体验、演示成本

2、模块化API允许中间商集成

1、SecretPad

轻量化安装

POC验证

可定制集成

2、多部署形态

中心模式

P2P（计划中）

3、全栈产品

MPC

TEE

SCQL

4、SecretNote

Notebook形式

交互建模

一站式管理：一个页面管理多个设备

运行状态跟踪

## 算法层

### PSI/PIR

PSI: 交集以外的信息无法获取

支持多种协议：半诚实模型(ecdh/kkrt16/bc22 || ec-oprf->ub PSI)、恶意模型

性能和协议优化

多层入口：

白屏用户可以用产品

开发人员可以通过python调用secretflow接入或者以库的形式集成

PIR: 用户查询数据库，但是服务端不知道用户查询了什么

支持多种协议：sealed/label pir

性能和协议优化

多层入口：

白屏用户可以用产品

开发人员可以通过python调用secretflow接入或者以库的形式集成

### Data Analysis

主要是SCQL: secure collaborative query language

多方安全数据分析系统，用SQL语言实现多方数据密态分析能力

支持：

常用SQL的语法和算子

多种数据源接入：MySQL, Postgres, CSV

多种协议：SEMI2K, CHEETAH, ABY3

### FL

以原始数据不出域为前提，通过交换中间数据完成建模

包括水平联邦、垂直联邦（拆分学习）

安全攻防：风险度量、攻防框架和算法

性能优化：稀疏化、量化、流水线

算法：营销算法（DeepFM/BST/MMoE）、SOTA安全聚合、（计划中）大模型

## 计算层

1、混合编译调度：RayFed

机构内计算：Ray + 跨机构协作能力：fed

2、密态引擎

(1) SPU

frontend: JAX (/tensorflow/pytorch在规划中) ->

compiler: -> XLA -> MLIR机器学习中间语言(PPHLO/PPLLO) ->

runtime: executor -> MPC protocol

(2) HEU

支持：

多种phe算法

高性能

多种接口：numpy API / CPP / python

硬件加速

(3) TEEU

提供数据分析、机器学习、MPC/FL加速

特色：

跨域管控：数据确权、使用授权、使用鉴权、结果授权

可信应用：预处理、机器学习（计划支持深度学习和大模型）

多硬件：SGX, HyperEnclave, 海光csv, intel TDX

(4) TECCU

…

3、密码原语：YACL

提供密码理论和上层应用的接口

特色：高性能、安全、易用

（下层）

## 资源层：kuscia

屏蔽机构间基础设施的差异，提供通用任务调度能力

核心：基于k8s的任务编排框架

两块内容：master / lite

### master

控制平面，内容：

k3s(轻量化k8s)

KusciaController: 跨域任务调度、服务发现、数据授权

InterConnController:互联互通控制器

### lite

ServiceMesh: 通信用的网络层基础

DataMesh: 方便数据管理，可以用于数据发现、多源适配、数据授权

Agent: 负责节点注册、容器管理

## 互联互通

黑盒模式：管理调度互联

管理面、控制面互联互通，算法容器相同

案例：两个机构任务调度不一样，但都是secretflow

白盒模式：基于开放算法协议的互联

算法容器可以不一样，可以直接互联算法引擎

## 跨域管控

核心是三权分置，资源持有权、加工使用权、产品经营权

管控的是：数据加工使用权

法规约束 + 技术保障

## 总结

根据使用者的条件分类：

产品使用者：关注产品层 （提供低门槛演示能力）

平台集成者：API/SDK, Kuscia （集成功能，提供解决方案）

算法使用者：FL/SPU/HEU/TEEU/TECCU

协议使用者：YACL （研究底层密码协议）