1. **华控清交同态加速卡（TsingJ X1）**

华控清交同态加速卡（TsingJ X1）是业界首款专用于半同态计算加速的特定集成电路芯片（ASIC），在隐私安全计算领域具有里程碑意义。TsingJ X1以PCIe2.0作为接口，在应用层有专用的驱动，开发人员可以十分方便地调用驱动接口使用加速卡的计算资源，针对特定的运算（如大整数模乘、模幂等）具备十分显著的加速效果。

TsingJ X1已深度嵌入到华控清交的隐私保护计算产品中，对于某些应用场景的性能在业界遥遥领先。用户经过简单地配置便可指定是否使用硬件，应用软件也具备硬件自动探测功能，有助于应用在纯软件与软硬结合环境中无缝切换。

总的来说，TsingJ X1特点及优势在于：

**（1）安全自主可控的加密引擎：**加速卡支持多芯片、多核并行处理，核心电路的计算逻辑及控制逻辑的设计均自主可控，期间申请了多项专利。

**（2）极高的计算吞吐量：**能够实现上千个加密处理单元对同态加密协议和模运算的并发执行，从而达到极致的计算性能。单块加速卡计算大整数模幂的性能可媲美约1000个CPU核。

**（3）极高的能效比：**单块加速卡满负荷运载时的功率仅为约120W。相比传统的通用处理器CPU与GPU，具备更好的效能比，践行国家碳中和的理念。

**（4）支持一机多卡和多机并行**的部署方式，通过高效的驱动设计和软硬件协同优化，提供极佳的并行计算能力，在最小的空间中部署最多的算力。

TsingJ X1能够应用于隐匿查询、联合建模、联合预测、反欺诈及协同监管等诸多隐私计算场景。以下是我们测试过的两个常见场景：

**1）**使用Paillier半同态加密算法实现两方数据隐匿查询（涉及数据量百万级）。在采用TsingJ X1和旗舰型号的AMD处理器进行性能对比，发现在相同的带宽条件下（分别试验了100Mbps、10Mbps、1Mbps三种情况）TsingJ X1比传统AMD处理器性能高出10倍以上。

**2）**逻辑回归模型的联合预测算法**。**假定数据方有1000条数据，每条数据经过编码后有50000个特征。预测时数据方将数据加密发送给模型方，而模型方对每条数据使用自己的模型计算点积，并将结果发还给数据方。在采用TsingJ X1的情况下比旗舰型号的AMD处理器高出性能5倍左右。

1. **计算引擎升级**

**（1）新增预计算功能。**将密文计算协议所需要的三元组在计算前生成，降低在线计算时算力消耗和通讯量，提升计算性能达1个数量级。

**（2）新增SSn秘密分享计算引擎**

支持任意**多方**密文计算，支持两种部署模式：存算一体模式（对等计算）、存算分离模式（代理计算）。

图示

描述已自动生成

图示

描述已自动生成

**（3）安全升级支持“半诚实+恶意模型”**

以下计算引擎新增支持恶意安全模型：PSI两方求交、PIR关键字查询、SSN通用密文计算协议，安全性升级。

1. **产品架构升级**

新研发ME节点功能模块，逐步将PrivPy通用计算引擎、SSN通用计算引擎、PSI/PIR专用算法引擎进行整合，按应用场景适配。支持点对点对等模式部署、代理计算部署两种方式，示例如下：

ME-A

ME-B



**对等计算模式**

PrivPy

ME-A

ME-B



**代理计算模式**