报告编号:

检　验　报　告

产品型号：	V1.0
产品名称：	清交 **PrivPy** 多方安全计算平台
受检单位：	华控清交信息科技（北京）有限公司
检验类别：	委托检验

中　国　泰　尔　实　验　室

注　意　事　项

1. 本报告无“检测专用章”或检验单位公章无效。

2. 本报告需加盖骑缝章。

3. 复制本报告未重新加盖“检测专用章”无效。

4. 本报告无主检、审核、批准人签字无效。

5. 本报告涂改无效。

6. 为了客户的利益，若对本报告有异议，请于收到本报告之日起十五日内向本检验机构提出。

7. 本检验报告仅对被检样品及所检项目负责；本检验报告中样品来源信息（如送样人、产地、生产单位等）为客户提供，实验室不负责其真实性。

8. 未经实验室书面批准不得部分复制本报告。

9. 中国泰尔实验室质量管理体系共包括以下 9 个质检中心：
国家电话机质量监督检验中心
信息产业北京移动通信设备质量监督检验中心
信息产业图文通信设备质量监督检验中心
信息产业北京电话交换设备质量监督检验中心
信息产业通信电磁兼容质量监督检验中心
信息产业通信软件测评中心
信息产业邮电工业产品质量监督检验中心
信息产业通信设备抗震性能质量监督检验中心
国家物联网通信产品质量监督检验中心

地址：北京海淀区花园北路 52 号

邮政编码：100191

电话：010-62300293

传真：010-62300299

网址：www.caict.ac.cn

E-mail：data@caict.ac.cn

目　　录

中 国 泰 尔 实 验 室

检　　验　　报　　告

报告编号：　　共 8 页　　第 1 页

产品名称	清交 PrivPy 多方计算平台	产品数量	--
产品型号	V1.0	商标	--
委托单位	华控清交信息科技（北京）有限公司		
生产单位	华控清交信息科技（北京）有限公司		
检验类别	委托检验	抽样基数	--
送样人		抽样日期	--
检验项目	基于多方安全计算的隐私计算产品性能测试	到样日期	2021 年 6 月 4 日
检验依据	1. BDC 57-2021《隐私计算 多方安全计算产品性能要求和测试方法》		
检验结论	1. 测试项目包括必选项 35 项，可选项 0 项 2. 实际完成必选项 35 项，可选项 0 项 3. 不涉及项：共 0 项 4. 不合格项：共 0 项 5. 结论：合格 签发日期：2021 年 06 月 24 日		
备注	--		

批准：　　审核：　　主检：

检 验 样 品 描 述

一、测试环境

1 硬件环境

设备类型		配置描述
华为 2288H V5 6 台	处理器	2 * Intel 至强 5218(2.3GHz/16-Core/22MB/125W)
	内存	8 * 32GB DDR4
	硬盘	6*1.8T SAS 12Gb/s-10K rpm-128MB-2.5 英寸
		4*1.2T SAS 12Gb/s-10K rpm-128MB-2.5 英寸
		1*1.6T NVME SSD
交换机 1 台		千兆网络

2 数据集配置

配置描述	来源	数据量	特征维度	适用算法
数据集 α	生成	千万级	7	基础运算、联合统计
数据集 β	生成	亿级别	4	PIR
数据集 γ	生成	亿级别	1	PSI
epsilon	公开	400,000 / 100,000	2000 抽取 900	特征工程、建模、预测

2.1 数据集 α

通过 Python 脚本生成三份一千万行的随机浮点数(float32)样本集。每份样本集包含一列 ID（对 1 到 10000000 进行 32 位的 MD5 加密处理），两列特征(样本 1 为 X1、X2；样本 2 为 X3、X4；样本 3 为 X5、X6)，其中三份样本的 ID 列相同，X1、X2、X3、X4、X5、X6 为随机生成的浮点数（范围从 1.0-1000.0）。X1、X3、X5 用于基础运算，X2、X4、X6 用于联合统计。

2.2 数据集 β

数据集由脚本随机生成，每条样本包含 ID、注册日期、年龄、消费金额四个特征。其中 ID 为 18 位十进制的随机整数，注册日期为 2000-01-01 到 2020-12-31 范围的随机年月日数值，年龄为 15 到 80 之间的随机整数，消费金额为 0.00-1000000.00 范围内的随机浮点数(小数点后保留 2 位)。

从被查询数据集中随机抽取 10000 个 ID 值，作为高效率查询（百级不可区分度）的待查询 ID。从被查询数据集中随机抽取 1 个 ID 值，作为高隐匿性查询（百万级不可区分度）的待查询 ID。

2.3 数据集 γ

求交数据集由脚本随机生成，每个样本包含一个 ID 信息，ID 为 18 位十进制的随机整数。不同场景各数据方的数据集规模不同。

a）两方平衡场景：数据方 A、数据方 B 的数据总量均为一亿行，两方数据的相交率为 50%，即五千万条相同 ID。

b）两方非平衡场景：数据方 A 数据总量为一亿行、数据方 B 的数据总量为十万行，两方数据的相交率为 50%，即五万条相同 ID。

2.4 epsilon：

采用 epsilon 数据集，数据集已完成归一化、标准化。40 万行样本作为训练集，10 万行样本作为测试集。原始数据集包含 2000 个特征，随机抽取 900 个特征用于计算。数据方数量为两个，每个数据方都持有 450 个特征，只有一个数据方持有标签信息。

3 参与方及算法设置

配置 描述	基础 运算	联合 统计	隐匿 查询	安全 求交	特征 工程	联合 建模	联合 预测
数据方	两方 三方	两方	两方	两方	两方	两方	两方
算法类型	加法 乘法 比较	最大值 方差 中位数	高效率 高隐匿性	平衡 非平衡	WOE 和 IV 计算	LR	LR

二、产品部署情况（介绍在测试环境中搭建的产品架构、网络配置、节点配置等）

清交多方计算平台采用代理计算架构，4 台服务器做 ES 密文计算，1 台服务器做 DS 接入和加密数据，剩下 1 台服务器同时作为管理控制节点和 DS 数据接入和加密。6 台服务器划分不同的区域，通过千兆网络连接。

检验内容一览表

报告编号： 共 8 页 第 4 页

检验内容一览表					
产品名称：清交 PrivPy 多方计算平台					
测试项目：隐私计算 多方安全计算产品性能专项	应测项	实测项	合格项	不涉及项	不合格项数
第一部分：技术架构	1	1	1	0	0
第二部分：通用安全	5	5	5	0	0
第三部分：算法安全	7	7	7	0	0
第四部分：基础运算	4	4	4	0	0
第五部分：联合统计	4	4	4	0	0
第六部分：隐匿查询（PIR）	4	4	4	0	0
第七部分：安全求交（PSI）	4	4	4	0	0
第八部分：特征工程	2	2	2	0	0
第九部分：联合建模	2	2	2	0	0
第十部分：联合预测	2	2	2	0	0
总计	35	35	35	0	0
备注：不涉及项代表本被测产品不涉及的能力项，在本次测试中不做要求。					

审核人： 填表人：

检 验 结 果

报告编号： 共 8 页 第 5 页

序号	检验项目	标准要求	检验结果	结论
第一部分：技术构架（标准依据：BDC 57-2021 1.1）				
1	第三方安全性验证	检验产品中的第三方安全性	符合	通过
第二部分：通用安全（标准依据：BDC 57-2021 2.1）				
1	通信安全	隐私计算的通信信道安全性功能	符合	通过
2	身份认证	应对任务计算过程中的关键环节进行身份认证	符合	通过
3	结果安全	非结果方无法获取计算结果	符合	通过
4	安全参数	秘钥长度符合标准	符合	通过
5	密码安全	密码得到安全保护	符合	通过
第三部分：算法安全（标准依据：BDC 57-2021 3.1）				
1	基础运算	确保用户隐私数据及中间数据在基础运算任务全流程不会泄露	符合	通过
2	联合统计	确保用户隐私数据及中间数据在联合统计任务全流程不会泄露	符合	通过
3	隐匿查询（PIR）	确保用户隐私数据及中间数据在隐匿查询任务全流程不会泄露	符合	通过
4	安全求交（PSI）	确保用户隐私数据及中间数据在安全求交任务全流程不会泄露	符合	通过
5	特征工程	确保用户隐私数据及中间数据在特征工程任务全流程不会泄露	符合	通过
6	联合建模	确保用户隐私数据及中间数据在联合建模任务全流程不会泄露	符合	通过
7	联合预测	确保用户隐私数据及中间数据在联合预测任务全流程不会泄露	符合	通过
第四部分：基础运算（标准依据：BDC 57-2021 4.1）				
1	结果准确性：两方场景	检验数值基础运算的结果准确性	符合	通过
2	结果准确性：三方场景	检验数值基础运算的结果准确性	符合	通过
3	计算耗时：两方场景	检验数值基础运算的耗时情况	加法：20s 乘法：18s 比较：22s	
4	计算耗时：三方场景	检验数值基础运算的耗时情况	加法：18s 乘法：21s	
第五部分：联合统计（标准依据：BDC 57-2021 5.1）				
1	结果准确性：两方场景	检验联合统计结果准确性	符合	通过
2	结果准确性：三方场景	检验联合统计结果准确性	符合	通过
3	计算耗时：两方场景	检验联合统计的耗时情况	最大值：3s	

			方差： 4s 中位数：41s	
4	计算耗时：三方场景	检验联合统计的耗时情况	最大值：4s 方差： 3s 中位数：43s	
第六部分：隐匿查询（标准依据：BDC 57-2021 6.1）				
1	结果准确性：高效率	检验隐匿查询结果准确性	符合	通过
2	结果准确性：高隐匿性	检验隐匿查询结果准确性	符合	通过
3	计算耗时：高效率	检验隐匿查询的耗时情况	33s	
4	计算耗时：高隐匿性	检验隐匿查询的耗时情况	21s	
第七部分：安全求交（标准依据：BDC 57-2021 7.1）				
1	结果准确性：两方平衡	检验安全求交的结果准确性	符合	通过
2	结果准确性：两方非平衡	检验安全求交的结果准确性	符合	通过
3	计算耗时：两方平衡	检验安全求交的耗时情况	9m54s	
4	计算耗时：两方非平衡	检验安全求交的耗时情况	6m29s	
第八部分：特征工程（标准依据：BDC 57-2021 8.1）				
1	结果准确性：两方场景	检验 WOE 和 IV 计算的结果准确性	符合	通过
2	计算耗时：两方场景	检验 WOE 和 IV 计算的耗时情况	7m12s	
第九部分：联合建模（标准依据：BDC 57-2021 9.1）				
1	结果准确性：两方逻辑回归	检验联合建模的模型结果准确性	符合	通过
2	计算耗时：两方逻辑回归	检验联合建模的耗时情况	5m22s	
第十部分：联合预测（标准依据：BDC 57-2021 10.1）				
1	结果准确性：两方逻辑回归	检验联合预测的预测结果的准确性	符合	通过
2	计算耗时：两方逻辑回归	检验联合预测的耗时情况	14s	

检 验 用 仪 表 设 备

序号	仪表名称	型号	生产厂家	出厂编号
1.	/	/	/	/

检验地点日期及人员

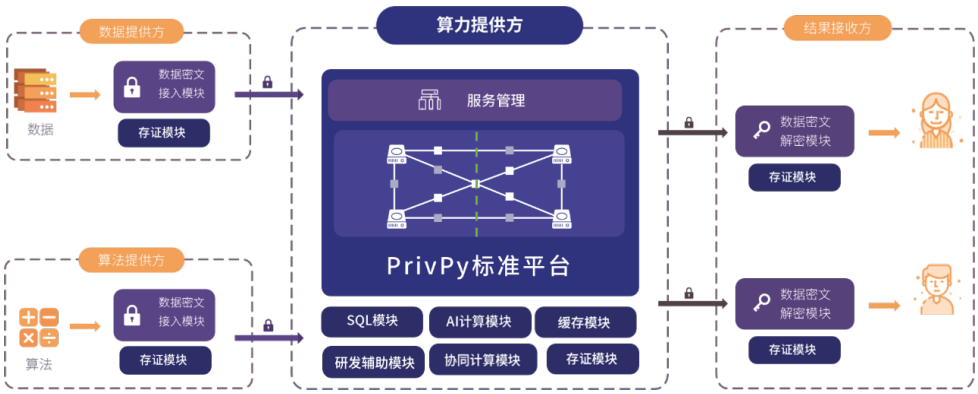
检验项目/模块	主 检 员	审 核 员
第一部分：技术构架	袁博	闫树
第二部分：通用安全	袁博	闫树
第三部分：算法安全	袁博	闫树
第四部分：基础运算	袁博	闫树
第五部分：联合统计	袁博	闫树
第六部分：隐匿查询（PIR）	袁博	闫树
第七部分：安全求交（PSI）	袁博	闫树
第八部分：特征工程	袁博	闫树
第九部分：联合建模	袁博	闫树
第十部分：联合预测	袁博	闫树

检验地点：北京市海淀区花园北路 52 号
检验日期：2021 年 06 月 08 日-2021 年 06 月 16 日

1 技术构架

1.1 第三方安全性验证

测试编号	UseCase101
测试项目	第三方安全性验证
测试目的	验证第三方安全性
测试环境	部署完成的隐私计算系统
前置条件	● 输入多方数据已接入或已配置 ● 多方安全计算任务已配置
测试步骤	1、 提供产品技术构架图 2、 记录是否存在第三方，哪些算法涉及第三方 3、 记录第三方是否参与秘钥等加密信息的分发交互及交互过程 4、 记录第三方是否参与原始数据加密状态的交互及交互过程 5、 记录第三方是否参与中间数据加密状态的交互及交互过程
预期结果	1、 如无第三方，需提供结构图等相关证明 2、 第三方如果参与数据交互，需要能保证原始数据和中间数据安全 3、 第三方不能留存原始数据和中间数据或其加密状态 4、 如有汇聚加密数据，并同时拥有秘钥的第三方，需要有措施保证其安全性，不会解密并泄露或留存数据
测试结果	1、 是否存在第三方，哪些算法涉及第三方：是 2、 第三方是否参与秘钥等加密信息的分发交互：否 3、 第三方是否参与原始数据加密状态的交互：否 4、 第三方是否参与中间数据加密状态的交互：是 5、 相关证明：架构和描述 华清交 PrivPy 多方计算平台采用代理计算架构，各个数据方通过数据服务组件 DS（data service）接入数据、数据加密后发给隐私计算引擎 ES(executive service)计算，ES 完成计算将结果发给 DS，DS 从 ES 获取结果并在本地解密结果。各数据参与方并不直接参与计算，而是由一组“计算去中心化，管理中心化”的服务器代理执行计算协议。 该架构的特点是数据参与方与计算方解耦，数据方之间无直接互联，系统扩展性好，能满足任意多参与方、大数据分布式计算和任意隐私计算，具有规模经济效应，同时具有高可用性和监管友好性。

	
备注	此处第三方主要指代理计算方，非任务协调方，相关概念辨析如下： 1 代理计算方 是指隐私计算过程中，需要对全量的原始数据的或者基于原始数据的中间计算因子（如梯度、loss）进行加密后计算的参与方。代理计算方可能是独立的第三方，也可能和其他参与方并存。 2 任务协调方 指仅仅参与任务计算顺序的协调，但不参加具体计算的协调方。任务协调方的主要作用是协调隐私计算任务按照计算协议，有序进行。

2 通用安全性

2.1 通信安全

测试编号	UseCase201
测试项目	通信信道安全性测试
测试目的	隐私计算的通信信道安全性功能
测试环境	部署完成的隐私计算系统
前置条件	● 输入多方数据已接入或已配置 ● 多方安全计算任务已配置
测试步骤	1、 启动和运行安全计算任务 2、 扫描安全计算节点的网络端口情况 3、 监听参与计算任务的多个计算节点的网络通信 4、 抓取相关的网络通信包
预期结果	1、 安全节点只监听配置的网络端口 2、 安全计算节点只和参与计算的节点和辅助安全计算的节点（如果有）进行通信 3、 节点间有认证和密钥协商流程（例如 TLS 协议相关流程） 4、 抓取数据包经过加密，无法被解析出原始数据
测试结果	以下是计算节点和任务调度系统的通信过程抓包： 1、 在节点网卡上截取报文，查看报文目的地址：