ICS 35.240.99
L67

团　　体　　标　　准

T /CCIASC XXXX-XXXX

高性能可靠多方安全计算产品技术要求及测试评价方法

Technical requirements and testing estimation methods of high performance and reliability secure multi-party computation products

XXXX－XX －XX 发布　　XXXX－XX－XX 实施

中国计算机行业协会发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国计算机行业协会提出。

本文件由中国计算机行业协会归口。

本文件主要起草单位：中国软件评测中心（工业和信息化部软件与集成电路促进中心）、数据安全关键技术与产业应用评价工业和信息化部重点实验室、成都卫士通信息安全技术有限公司、北京瑞莱智慧科技有限公司、清华大学、中车信息技术有限公司、中铁建设集团有限公司、中铁建网络信息科技有限公司、福州大学、国家计算机网络应急技术处理协调中心、北京锐服信科技有限公司、上海观安信息技术股份有限公司、联通华盛通信有限公司、云盾智慧安全科技有限公司。

本文件主要起草人：李尤、白利芳、林青、李泽村、唐刚、张德馨、刘思思、牛凯剑、杨晓琪、张浩男、张莉、刘西蒙、贾佩衡、陈建林、张晓娜、曹占涛、杜岚、郭潇、李月、林通、孙玉龙、周大兴、于程水、陈绮语、吴碧莹、常凯、张晓杰、李思逸、谢江、包宏宇、王安宇、包佳奇、董晓阳、丛天硕、雷术梅、曹祎南、王宇航、潘宇。

引　言

数据已成为我国第五大生产要素，数据价值属性凸显，数据要素市场化配置进程不断深入，数据流通需求加速释放，但同时隐私保护也面临空前挑战，而多方安全计算技术是平衡隐私保护与数据流通的有效方式之一。工业、电信等领域数据量级大、类型多、场景复杂，数据开发利用需求旺盛，亟需具备强大性能与优秀可靠性的多方安全计算产品保障数据流通安全。为落实《数据安全法》《网络安全法》等法律法规的相关规定，促进高性能可靠多方安全计算产品标准化发展，编制本文件，提出高性能可靠多方安全计算产品的技术要求和相应测试方法，为相关研发、测试机构提供参考与指导，旨在提升产品质量、提高数据安全流通保障能力、助推数据要素价值释放。

高性能可靠多方安全计算产品技术要求及测试评价方法

1 范围

本文件规定了高性能可靠多方安全计算产品功能、性能以及安全性等技术要求内容，并给出了技术要求相应的测试评价方法。

本文件适用于相关研发机构对高性能可靠多方安全计算产品的研发、测试和评估，以及第三方机构的相关检查、测试和评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GM/Z 4001-2013 密码术语

IEEE 2842-2021 Recommended Practice for Secure Multi-Party Computation

ISO/IEC CD 4922-1:2023 Information security – Secure multiparty computation – Part 1: General

3 术语和定义

3.1 多方安全计算 secure multi-party computation

一种密码协议，支持多个参与实体基于隐私输入共同完成一个任务函数的计算，同时确保各参与实体除了计算结果或可预期公开的信息外，无法获得其他参与实体的任何额外信息。

[来源：IEEE2842-2021，3.1，有修改]

3.2 参与方 parties

参与到多方安全计算中的实体。根据参与方在多方安全计算任务中扮演不同角色，将参与方划分为数据方、计算方和结果方。

注：数据方将编码形式的输入提供给计算方，计算方执行任务函数，结果方解码从计算方接收的函数计算结果从而获得想要的多方安全计算结果。

[来源：ISO/IEC CD 4922-1:2023，3.4-3.7，有修改]

3.3 安全模型 security model

一种对攻击者攻击能力、攻击方式的抽象以及假设。

注：多方安全计算协议遵循的前提假设。

3.4 半诚实模型 semi-honest model

安全模型的一种，参与方在协议执行过程中会遵循协议约定，但会试图通过其他参与方的输入或中间结果挖掘额外的信息。

3.5 恶意模型 malicious model

安全模型的一种，参与方在协议执行过程中可能会偏离协议，通过不合法的输入或恶意篡改数据等手段达到某种恶意目的。

3.6 抗合谋攻击 anti-collusion attack

指任何数量的非法接收者在合谋串通的情况下，无法解密获得有用信息。

3.7 秘密分享 secret sharing

将秘密分解成多个子秘密，使用超过阈值数目的子秘密才能恢复该秘密的机制。
[来源:GM/Z 4001-2013,2.59]

3.8 不经意传输 oblivious transfer

一种密码学协议，消息发送者持有两条或多条待发送的消息，接收者选择一条进行接收，事后发送者不能得知接收者选择了哪一条消息，接收者对于未选择的消息也无法获取信息。

3.9 混淆电路 garbled circuits

一种通过将多方参与的安全计算函数编译成电路的形式，并将其真值表加密、扰乱，从而实现多方安全计算的底层技术。

3.10 同态加密 homomorphic encryption

一种满足密文同态运算性质的加密算法，即对密文进行特定的计算，得到的密文计算结果经过同态解密后，其结果等同于对明文数据直接进行相应的计算。

注：半同态加密和全同态加密是同态加密的两种不同级别，全同态加密支持在加密状态下进行任意多次的加法和乘法运算，同态解密后可得到与明文计算相同的结果；半同态加密只支持在加密状态下进行一种运算，通常是加法或乘法。

4 缩略语

下列缩略语适用于本文件：
ID:身份标识 Identity Document
MPC:多方安全计算 Secure Multi-Party Computation
TLS:传输层安全协议 Transport Layer Security
WOE:证据权重 Weight of Evidence
IV:信息值 Information Value

5 技术要求

5.1 通用技术要求

5.1.1 技术架构要求

多方安全计算产品的技术架构应体现其能够满足高性能、可靠的指标要求，如有代理计算方，其需要有加密措施或手段；如有任务协调方，其仅可协调任务计算顺序，不可参与具体计算。

5.1.2 平台管理要求

多方安全计算产品应具备平台管理能力，包括用户管理功能、节点管理功能、数据管理功能、任务管理功能、系统日志功能等。

a) 用户管理功能：应具备对用户的管理能力，应支持用户的权限管理，阻止用户的非法越权操作；

b) 节点管理功能：应具备节点管理能力，包括节点的增加、删除、修改、查找等；

c) 数据管理功能：应具备数据管理能力，包括数据的增加、删除、修改、查找等；

d) 任务管理功能：应具备任务管理能力，包括任务的创建、调度、监控、销毁等；

e) 审计监控功能：应具备审计和监控能力，审计记录应包括事件的日期和时间、参与者信息、事件类型及其他相关信息，应支持生成安全警报、阻止未授权的访问等；

f) 系统日志功能：应具备系统日志相关能力，对关键信息进行记录，包括用户的操作日志、系统运行日志、任务运行日志、节点生命周期日志等。

5.1.3 通用安全要求

多方安全计算产品应满足以下通用安全要求：

a) 通信安全：系统建立的安全通信通道版本应符合当前通信安全规范，安全节点应只监听配置的网络端口，且只和参与计算与辅助安全计算的节点进行通信；

b) 身份认证：应对所有参与方进行身份认证与权限鉴别，身份鉴别信息应具有复杂度要求并定期更换，应通过技术措施保证鉴别信息重置过程安全，对敏感认证信息具备存储保护措施，应对任务请求信息进行签名与验证；

c) 加密安全：使用的密码学算法计算安全强度不低于 128 位，统计安全强度不低于 40 位；公钥不可被伪造，私钥不能泄露给私钥生成方以外的其他参与方，用于通信的对称密钥不能泄露给一对通信方之外的其他参与方；

d) 结果安全：仅结果方可获取计算结果，除预期结果与可预期公开的信息外，不输出其他额外信息；

e) 数据备份与恢复：应进行重要数据的本地备份并支持数据恢复，应提供异地数据备份与恢复功能并在必要时启用；

f) 审计安全：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；应对审计进程进行保护，防止未经授权的中断。

5.1.4 其他基础要求

多方安全计算产品还需具备兼容性、可扩展性、容错性以及恢复性等基础要求。

a) 兼容性：多方安全计算产品使用的第三方库、加密算法和安全工具在集成和使用过程中的兼容性和稳定性。

b) 可扩展性：多方安全计算产品在不同参与方数量下的性能表现，包括计算效率和通信延迟等，以评估产品的可扩展性和适用范围。

c) 容错性：多方安全计算产品在面临部分故障或异常情况时，能够保持稳定性。

d) 恢复性：多方安全计算产品在面临部分故障或异常情况时，能够快速恢复，确保计算任务的持续进行。

5.2 底层技术要求

多方安全计算产品应保证上层应用的可靠性，采用的底层技术和和依赖库等应满足可靠性要求。

a) 底层技术包括但不限于支持秘密分享、混淆电路、不经意传输和同态加密等；

b) 依赖库包括但不限于 MP-SPDZ、MASCOT、ABY、ABY3、CBMC-GC、EMP-toolkit、FRESCO、JIFF、MPyC、Obliv-C、OblivVM、PICCO、SCALE-MAMBA、Sharemind MPC、TinyGarble 等。

5.3 算法功能要求

多方安全计算产品应支持可证明安全的安全统计、安全查询、安全求交、特征工程、安全建模、联合预测等算法功能。

a) 数据量达到 1 亿量级及以上；

b) 密文计算准确率应达到相比同样条件下明文计算满足结果误差小于 2^{-32}；

c) 支持跨行业或跨机构 1 亿条以上数据安全融合；

d) 模型评价指标应达到 0.8 以上，预测准确率与明文计算准确率相比应达到 85%以上。

5.4 安全模型要求

多方安全计算产品应支持一种或多种安全模型，如：半诚实模型、恶意模型、抗合谋攻击等。

5.5 算法性能要求

由于性能表现与环境配置、数据集大小相关，下列性能要求对应的推荐配置为：服务器 16 核 CPU、256G 内存、1T 硬盘，网络带宽 100Mbps；除特殊说明外，测试数据集应至少包含 1 亿条数据，单条数据不小于 4 字节。

5.5.1 基础运算性能

多方安全计算产品在以下场景应支持加法、乘法、比较等基础运算，其性能要求如表 5-1 所示。

表 5-1 基础运算性能

测试算法	参与方数量	计算类型	数据集大小	耗时
基础运算	两方	加法	每方有至少 1 亿条数据，均是一列	10min
		乘法		10min
		比较		10min
	三方	加法		20min
		乘法		20min

5.5.2 安全统计性能

多方安全计算产品在以下场景应支持方差、中位数等统计运算，其性能要求如表 5-2 所示。

表 5-2 安全统计性能

测试算法	参与方数量	计算类型	数据集大小	耗时
安全统计	两方	方差	每方有 1 亿条以上数据，均是一列	10min
		中位数		10min
	三方	方差		20min
		中位数		20min

5.5.3 安全查询性能

多方安全计算产品在以下场景应支持安全查询功能，其性能要求如表 5-3 所示。

表 5-3 安全统计性能

测试算法	参与方数量	计算类型	数据集大小	耗时

测试算法	参与方数量	计算类型	数据集大小	耗时
安全查询	两方	百级不可区分	从被查询数据集（1亿 ID）中随机抽取10000个ID值	30min
		百万级不可区分	从被查询数据集（1亿ID）中随机抽取1个ID值	1min

5.5.4 安全求交性能

多方安全计算产品在以下场景应支持安全求交功能，其性能要求如表5-4所示。

表5-4 安全求交性能

测试算法	参与方数量	计算类型	数据集大小	耗时
安全求交	两方	平衡	均为至少1亿行，两方数据的相交率为50%，即5000万	80min
		非平衡	一方至少1亿行、一方至少10万行，两方数据的相交率为50%，即5万	25min

5.5.5 特征工程性能

多方安全计算产品的每个参与方各持有部分特征，只有一个数据方持有标签，在保护标签信息不被泄露的前提下进行WOE和IV计算，其性能要求如表5-5所示。

表5-5 特征工程性能

测试算法	参与方数量	计算类型	数据集大小	耗时
特征工程	两方	WOE和IV计算	两方共有至少100万行 /50维特征，一方持有标签	30min

5.5.6 安全建模性能

多方安全计算产品应支持安全建模功能，其性能要求如表5-6所示。

表5-6 安全建模性能

测试算法	参与方数量	数据来源	数据集大小	性能要求
安全建模	两方	实际场景	两方均为1亿行，特征数大于等于 1，两方数据进行建模	准确率0.8以上，明密文建模在同等条件下模型评价指标误差小于1%。

5.5.7 联合预测性能

多方安全计算产品应支持联合预测功能，其性能要求如表5-7所示。

表5-7 联合预测性能

测试算法	参与方数量	计算类型	数据集大小	单次迭代耗时
联合预测	两方	逻辑回归	两方共有至少 100 万行 / 50 维特征，一方持有标签	5min

6 测试评价方法

6.1 通用技术测试方法

6.1.1 技术架构测试

测试项目	技术架构验证
测试目的	验证多方安全计算产品采用的技术架构及其安全性
测试环境	部署完成的多方安全计算系统
前置条件	1) 获取多方安全计算产品的技术架构图 2) 获取多方安全计算产品的技术设计文档
测试步骤	1) 查阅产品技术架构图并记录技术架构图采用的分发和交互方式 2) 查看相关技术设计文档
预期结果	代理计算方和任务协调方的运行方式符合技术架构的要求
备注	无

6.1.2 平台管理测试

6.1.2.1 用户管理

测试项目	用户管理
测试目的	验证多方安全计算产品用户管理的合法性
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 点击用户管理 2) 点击用户的权限管理，分为超级管理员、管理员、用户等 3) 点击用户的功能，增加、删除、查找、修改等
预期结果	1) 用户功能完善 2) 已授权的用户可以添加到多方安全计算任务中 3) 可查看和验证用户的访问权限和功能
备注	无

6.1.2.2 节点管理

测试项目	节点管理
测试目的	验证多方安全计算产品节点管理的合法性
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 点击节点管理功能，包括增加、删除、修改、查找

	2) 点击各节点的管理功能，查看节点访问权限
预期结果	1) 节点管理功能完善 2) 已授权的节点可以添加到多方安全计算任务中 3) 可查看和验证节点的访问权限
备注	无

6.1.2.3 数据管理

测试项目	数据管理
测试目的	验证多方安全计算产品数据管理的合法性
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 点击数据管理功能，包括增加、删除、修改、查找 2) 测试各功能是否正常 3) 分析结果
预期结果	数据管理功能完善
备注	无

6.1.2.4 任务管理

测试项目	任务管理
测试目的	验证多方安全计算产品任务管理的合法性
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 点击任务管理功能，包括创建、调度、监控、销毁 2) 点击各个任务的执行情况
预期结果	1) 任务管理功能完善 2) 未授权、授权到期或被取消授权的任务资源无法加入多方安全计算任务中 3) 可查看和验证任务资源的访问权限和授权记录
备注	无

6.1.2.5 审计监控

测试项目	审计监控
测试目的	测试多方安全计算产品审计监控的合法性
测试环境	已部署完成的多方安全计算环境，包括多个计算节点和辅助安全计算的节点
前置条件	1) 多方安全计算系统可正常运行，已经通过基本功能测试 2) 系统中的节点间通信采用了通信信道安全措施 3) 系统已经配置了安全审计和监控机制
测试步骤	1) 模拟一次计算任务的运行 2) 记录所有与计算任务相关的事件，如节点通信、任务分配和结果 3) 分析系统生成的安全审计日志，验证是否记录了所有关键事件信息 4) 触发一个安全事件，检查系统是否能够及时检测并生成相应的安全警报 5) 尝试访问受限资源或功能，验证系统是否阻止未授权的访问

预期结果	1) 系统能够准确记录与计算任务相关的事件 2) 安全审计日志中记录了关键事件和操作的详细信息，包括日期和时间、参与者信息、事件类型等 3) 系统能够根据安全审计日志提供完整的操作追踪和审计能力 4) 系统能够及时检测并生成安全警报，以响应安全事件的发生 5) 系统能够阻止未授权的访问，确保受限资源或功能只能由授权用户访问
备注	无

6.1.2.6 系统日志

测试项目	系统日志
测试目的	验证多方安全计算产品系统日志的合法性
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 查看系统日志模块，日志查看功能 2) 查看系统日志模块，清空日志功能 3) 查看系统日志模块，导出日志功能 4) 查看系统日志模块，日志审计功能
预期结果	1) 允许系统日志查看 2) 允许系统日志清空 3) 允许系统日志导出 4) 允许系统日志审计
备注	无

6.1.3 通用安全测试

6.1.3.1 通信安全

测试项目	通信信道安全
测试目的	验证节点通信时是否建立安全的通信通道
测试环境	部署完成的多方安全计算环境
前置条件	1) 多方安全计算系统正常运行 2) 多方安全任务配置完成 3) 密钥交换的协议是安全的
测试步骤	1) 核查系统中通信双方在通道建立之前是否使用密码技术进行身份认证 2) 核查系统建立的安全通信通道（如 TLS）版本是否符合当前通信安全规范 3) 扫描安全计算节点的网络端口开放情况 4) 监听参与计算任务的多个计算节点的网络通信 5) 抓取并解析通信建立时的数据包，判断安全通信通道建立的过程是否与文档中的描述一致
预期结果	1) 通信双方在通道建立之前使用密码技术进行身份认证 2) 系统建立的安全通信通道（如 TLS）版本符合当前通信安全规范 3) 通信数据包中包含的安全通信通道建立的过程与设计文档中的描述一致 4) 安全节点只监听配置的网络端口 5) 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（如有）进

	行通信
备注	无

6.1.3.2 身份认证

测试项目	用户身份认证
测试目的	验证用户身份认证功能的可用性与安全性
测试环境	部署完成的多方安全计算系统
前置条件	1) 已正确添加一个用户身份 2) 启动多方安全计算系统
测试步骤	1) 使用用户身份及其身份鉴别信息进行系统登录认证 2) 连续多次使用错误的用户身份及其身份鉴别信息进行登录 3) 使用正确的用户身份及其身份鉴别信息进行登录 4) 在用户身份信息管理页面修改用户身份鉴别信息或等待用户身份鉴别信息失效后重新登录系统 5) 检查用户身份认证信息的存储保护机制 6) 任务发起方请求任务 7) 运行计算任务 8) 结果方请求计算结果
预期结果	1) 使用正确的用户身份及其身份鉴别信息能正常登录 2) 用户身份标识具有唯一性，用户身份鉴别信息具有复杂度要求且支持定期更换 3) 用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全 4) 对用户敏感认证信息有保护存储措施 5) 任务发起方对任务请求信息进行签名，协调方或任务接收方对其进行验证 6) 结果方请求计算结果时，协调方对任务接收方进行身份认证和权限鉴别 7) 各参与方之间进行通信时相互进行身份认证，并建立安全通道
备注	无

6.1.3.3 加密安全

a)密码算法安全强度

测试项目	密码算法安全强度
测试目的	验证密码算法的计算安全强度
测试环境	部署完成的多方安全计算环境
前置条件	多方安全计算系统正常运行
测试步骤	1) 核查对称密码算法的密钥长度、工作模式 2) 核查非对称密码算法的密钥长度 3) 核查密码杂凑算法的密码长度、盐值等 4) 说明文档与代码交叉验证
预期结果	1) 产品使用的密码学算法，计算安全强度不低于 128 位，统计安全强度不低于 40 位 2) 未使用存在安全问题或安全强度不足的密码算法 3) 未使用未经验证的加密算法 4) 交叉验证结果符合报告中描述内容

备注	无

b)密码算法使用正确性

测试项目	密码算法使用正确性
测试目的	验证密码算法使用的正确性
测试环境	部署完成的多方安全计算环境
前置条件	多方安全计算系统正常运行
测试步骤	1) 采集对称密码算法加解密数据 2) 采集非对称密码算法加解密数据 3) 采集密码杂凑数据 4) 通过密码算法检测工具对加解密数据、签名验签数据、杂凑数据进行正确性检测
预期结果	密码算法使用正确
备注	输入不同类型，大小的数据，验证加密生成密文，密文处理，以及密文解密、生成的杂凑数据是否与预期结果相符

6.1.3.4 结果安全

测试项目	结果安全
测试目的	验证非结果方是否能获取计算结果
测试环境	部署完成的多方安全计算环境
前置条件	1) 多方安全计算系统正常运行 2) 多方安全任务配置完成 3) 参与方数据输入完成
测试步骤	1) 创建并启动多方安全计算任务 2) 查看结果方和参与方任务列表界面 3) 结果方获取计算结果
预期结果	1) 结果方和参与方均能查看本次多方安全计算任务记录 2) 仅结果方能获得计算结果，非结果方无法获得计算结果（除非结果方同意协作方可以获取结果） 3) 除预期结果外，不应输出额外的信息
备注	无

6.1.3.5 数据备份与恢复

测试项目	数据备份与恢复
测试目的	验证多方安全计算产品数据备份与恢复能力
测试环境	部署完成的多方安全计算系统
前置条件	1) 多方安全计算系统正常运行 2) 多方安全任务配置完成 3) 参与方数据输入完成
测试步骤	1) 配置备份策略，执行本地数据备份 2) 核查是否按照备份策略进行本地备份 3) 对数据进行修改，模拟数据被破坏，执行数据恢复 4) 核查是否完成数据恢复 5) 核查是否具备异地数据备份与恢复功能

预期结果	1) 本地数据备份与恢复功能可用，备份与恢复结果正确 2) 具备异地数据备份与恢复功能
备注	无

6.1.3.6 审计安全

测试项目	审计安全
测试目的	验证多方安全计算产品审计安全能力
测试环境	部署完成的多方安全计算系统
前置条件	1) 多方安全计算系统正常运行 2) 多方安全任务配置完成 3) 参与方数据输入完成 4) 系统已开启审计功能
测试步骤	1) 核查是否采取保护措施保护审计记录 2) 核查是否对审计记录进行定期备份 3) 核查是否采取措施对审计进程进行保护
预期结果	1) 采取措施保护审计记录并定期备份 2) 采取措施保护审计进程
备注	无

6.1.4 其他基础要求测试

6.1.4.1 支持的数据类型

测试项目	支持的数据类型测试
测试目的	验证支持的数据类型
测试环境	部署完成的多方安全计算系统
前置条件	1) 多方安全计算系统正常运行 2) 多方安全计算任务已配置 3) 提供整数型、浮点型、字符型和布尔型的数据 4) 提供设计开发文档
测试步骤	1) 查阅设计开发文档 2) 逐个测试整数型、浮点型、字符型和布尔型的数据 3) 查看计算结果
预期结果	1) 设计开发文档中明确支持的数据类型 2) 多方安全计算产品支持各数据类型 3) 计算结果准确
备注	数据类型包括但不限于：整数数据类型（byte、short、int、long）、浮点数据类型（float、double）、字符数据类型（char）、布尔数据类型（boolean）等

6.1.4.2 容错性和恢复性

测试项目	容错性和恢复性测试
测试目的	验证系统在面临部分故障或异常情况时，能够保持稳定性和快速恢复，确保计算任务的持续进行
测试环境	已部署完成的多方安全计算环境，包括多个计算节点和辅助安全计算的节点
前置条件	1) 多方安全计算系统可正常运行，已经通过基本功能测试 2) 系统中的节点间通信采用了通信信道安全措施

	3) 系统已经配置了容错和恢复性机制
测试步骤	1) 断开一个计算节点的网络连接，模拟节点故障 2) 监控系统日志，验证系统能否检测到节点故障并进行相应处理 3) 尝试提交一个计算任务，验证系统是否能够自动调整任务分配，继续完成计算 4) 恢复被断开的计算节点的网络连接，观察系统是否自动将其重新纳入计算环境 5) 引入网络延迟，并逐渐增加，模拟节点通信不断变慢的情况 6) 提交一个计算任务，并监测系统的响应时间和任务完成情况
预期结果	1) 系统能够迅速检测到节点故障并通过备用节点继续完成计算任务 2) 日志中记录了节点故障的信息以及系统的响应措施 3) 计算任务在节点故障后能够自动切换节点并成功完成 4) 节点恢复后，系统能够自动将其重新整合到计算环境中 5) 系统能够在逐渐增加的通信延迟下保持一定的稳定性和性能 6) 系统能够在有一定网络延迟的情况下仍然完成计算任务
备注	无

6.1.4.3 可扩展性和兼容性

测试项目	可扩展性和兼容性测试
测试目的	验证多方安全计算产品在不同参与方数量下的表现，包括计算效率和通信延迟等，以及使用的第三方库、加密算法和安全工具在集成和使用过程中的兼容性和稳定性
测试环境	已部署完成的多个参与方的多方安全计算环境，包括多个第三方库和加密算法安全工具的集成环境
前置条件	1) 多方安全计算系统可正常运行，已经通过基本功能测试 2) 系统中集成了第三方库，加密算法和安全工具并且投入使用
测试步骤	1) 加入至少 8 个参与方的多方安全计算系统互联互通传输数据 2) 在多方安全计算产品中集成第三方库 3) 在多方安全计算产品中使用加密算法和安全工具进行数据传输
预期结果	1) 系统能够稳定兼容至少 8 个参与方的系统互联互通，并完成计算任务 2) 系统能够兼容第三方库，并可以在使用加密算法和安全工具进行计算时保持稳定
备注	无

6.2 底层技术测试

6.2.1 底层技术

测试项目	底层技术
测试目的	验证多方安全计算产品是否支持相应底层技术
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台 3) 部署恶意模型或抗合谋攻击模型
测试步骤	1) 根据不同的测试场景，选择不同的测试工具 2) 运行测试工具模拟恶意模型和合谋攻击 3) 验证协议能否正确运行，并检测是否能够抵御恶意行为和合谋攻击 4) 收集测试结果并进行详细分析，评估多方安全计算模型在面对恶意模

	型和合谋攻击时的性能和安全性表现
预期结果	算法支持恶意模型、抵抗合谋攻击的多方安全计算底层技术，包括但不限于秘密分享、不经意传输、混淆电路、同态加密等
备注	无

6.2.2 依赖库

测试项目	依赖库
测试目的	测试多方安全计算产品依赖库是否合法
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 测试加解密算法及基本密码学组件 2) 测试秘密拆分算法 3) 测试密文存储量，明文和解密后明文精确度的差别
预期结果	1) 依赖库的基本加解密算法正确 2) 秘密拆分算法结果正确 3) 密文解密后与明文精确度无明显差别
备注	无

6.3 算法功能测试

6.3.1 可证明安全

测试项目	算法的可证明安全
测试目的	验证采用可证明安全算法
测试环境	部署完成的多方安全计算系统
前置条件	1) 在不同参与方部署算法 2) 提供可证明安全底层算法的列表和设计文档
测试步骤	1) 记录所使用的底层算法和日志 2) 对比现有的算法列表和设计文档
预期结果	1) 算法所使用的底层算法和日志包含在现有的可证明安全底层算法的列表中 2) 多方安全计算产品采用可证明安全算法
备注	无

6.3.2 安全统计

测试项目	安全统计
测试目的	验证对安全统计功能的支持能力
测试环境	部署完成的多方安全计算产品系统
前置条件	1) 在不同参与方部署安全统计模块并启动安全统计系统 2) 分别设置两个参与方：数据拥有者与数据统计者
测试步骤	1) 准备安全统计相关数据，执行安全统计任务 2) 参与方数据拥有者生成密钥并将数据进行安全共享或者秘密分享 3) 参与方数据统计者向参与方数据拥有者发送请求，要求进行统计操作 4) 数据拥有者接收到数据统计者的请求并使用密钥进行安全计算并生成加密结果

	5) 数据统计者接收加密结果并解密得到统计结果 6) 观察记录两个参与方的行为及统计结果和异常情况
预期结果	1) 相关数据准备妥当并且安全统计任务成功执行 2) 系统能够及时发现并记录异常行为及潜在的安全隐患 3) 在计算的全流程中没有泄露任何明文给其他参与方 4) 准确性相比同样条件下明文计算满足结果误差小于 2^{-32}
备注	无

6.3.3 安全查询

测试项目	安全查询
测试目的	验证对安全查询功能的支持能力
测试环境	部署完成的多方安全计算系统
前置条件	1) 在不同参与方部署安全查询模块并启动安全查询系统 2) 分别设置两个参与方：数据拥有者与数据查询者
测试步骤	1) 准备安全查询相关数据，执行安全查询任务 2) 数据拥有者生成密钥并将数据进行安全共享或秘密分享 3) 数据查询者向数据拥有者发送查询请求，要求获取特定数据或执行特定查询操作 4) 数据拥有者接收查询请求并使用密钥进行安全计算，生成加密结果 5) 数据查询者接收加密结果并解密得到查询结果 6) 观察参与方的行为及统计结果，并记录异常情况
预期结果	1) 相关数据准备妥当并且安全查询任务成功执行 2) 系统能够及时发现并记录异常行为及潜在的安全隐患 3) 计算全流程中没有泄露任何明文给其他参与方 4) 准确性相比同样条件下明文计算满足结果误差小于 2^{-32}
备注	无

6.3.4 安全建模

6.3.4.1 数据预处理

测试项目	数据预处理
测试目的	验证安全建模功能数据预处理可用性
测试环境	部署完成的多方安全计算系统
前置条件	1) 合作多方准备好测试数据集 2) 完成多方的数据授权准备
测试步骤	1) 将多方异构数据进行融合，创建融合数据集 2) 对融合数据集进行数据分析，查看数据的基本情况 3) 查看数据的分布情况，包括数据的最大值、最小值、标准差、中位数等 4) 对数据进行自动/手动分箱，查看数据的 IV 值等指标 5) 基于数据集启动多方安全计算任务
预期结果	1) 多方的数据集能够融合成功并且数据基本情况展示符合预期 2) 能正确地展示数据的基本情况、分布图 3) 正确显示分箱结果、IV 值等指标 4) 多方安全计算任务正确执行
备注	无

6.3.4.2 监督学习算法：分类算法

测试项目	分类算法
测试目的	验证监督学习分类算法
测试环境	部署完成的多方安全计算环境
前置条件	1) 输入数据已整理成符合的格式 2) 计算任务和结果输出/呈现方式已配置 3) 在已标签的训练数据中构建分类模型，并在此基础上，对新数据进行分类
测试步骤	1) 按产品的分类算法类型清单，逐一创建训练任务 2) 查看任务结果
预期结果	产品支持的分类算法类型的计算任务均能正确完成
备注	无

6.3.4.3 监督学习算法：回归算法

测试项目	回归算法
测试目的	验证监督学习回归算法
测试环境	部署完成的多方安全计算环境
前置条件	1) 输入数据已整理成符合的格式 2) 计算任务和结果输出/呈现方式已配置 3) 回归算法找到一个线性函数，使得它能够最好地拟合输入和输出之间的关系
测试步骤	1) 按产品的分类算法类型清单，逐一创建训练任务 2) 查看任务结果
预期结果	产品支持的回归算法类型的计算任务均能正确完成
备注	无

6.3.4.4 无监督学习算法：聚类算法

测试项目	聚类算法
测试目的	验证无监督学习聚类算法
测试环境	部署完成的多方安全计算环境
前置条件	1) 输入数据已整理成符合的格式 2) 计算任务和结果输出/呈现方式已配置 3) 把数据分成几个类别，根据数据点之间的相似度
测试步骤	1) 按产品的分类算法类型清单，逐一创建训练任务 2) 查看任务结果
预期结果	产品支持的聚类算法类型的计算任务均能正确完成
备注	无

6.3.4.5 实现安全性

测试项目	实现安全性测试
测试目的	验证算法协议及其系统实现的安全性和隐私保护特性
测试环境	部署完成的多方安全计算系统
前置条件	1) 输入数据已接入或已配置 2) 多方安全计算任务、结果输出/呈现方式和审计日志已成功配置

	3) 提供安全性原理材料，包括参考论文、专家审查报告等 4) 提供系统的设计文档，包括算法协议、数据交互流程图、安全设计说明等
测试步骤	1) 审查安全性原理材料和系统设计文档的安全性 2) 通过审核日志、核心代码、抓包等方式，审核各环节计算及数据出入的处理逻辑，确认是否符合算法协议及数据交互流程图
预期结果	1) 安全性原理材料证明计算过程不会泄露数据隐私 2) 系统设计文档符合安全要求（不会泄露各方数据且计算结果符合算法预期结果） 3) 系统日志（核心源码）、通信报文与安全性原理材料、系统设计文档保持一致
备注	无

6.3.4.6 模型评价

测试项目	模型评价
测试目的	验证测试模型评价指标达到 0.8 以上
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 确定评价指标：确定用于评估多方安全计算模型的具体评价指标。分类模型的评价指标精确率、准确率、召回率、F1、AUC-ROC 曲线、PR 曲线；回归模型的评价指标 SSE、MSE、RMSE、MAE、R2 2) 数据准备：数据集中包含不同情况下的输入和期望输出，以及真实的输出结果，数据集应该能够涵盖模型可能遇到的各种情况 3) 测试模型：使用测试集对训练好的模型进行测试。将测试集中的输入数据输入到模型中，并与期望输出进行比较，计算评价指标的数值。如果评价指标达到 0.8 以上，则模型的性能符合要求
预期结果	模型评价指标达到 0.8 以上
备注	无

6.3.4.7 模型预测准确率

测试项目	模型预测准确率
测试目的	验证测试模型预测准确率与明文计算准确率相比达到 85%以上
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 准备一个包含输入数据和对应的真实输出的测试数据集。 2) 将测试集中的输入数据输入到多方安全计算模型中运行测试，获取模型的预测输出结果 3) 计算准确率：将模型的预测输出与测试集中的真实输出进行比较，并计算准确率。准确率的计算方法是将正确预测的样本数除以总样本数 4) 分析结果：分析准确率的数值来评估多方安全计算模型的性能。如果准确率达到 85％以上，则说明模型的性能符合要求
预期结果	模型预测准确率与明文计算准确率相比达到 85%以上
备注	无

6.3.5 安全求交

测试项目	安全求交
测试目的	验证对安全求交功能的支持能力
测试环境	部署完成的多方安全计算系统
前置条件	1) 在不同参与方部署多方安全计算节点并启动多方安全计算系统 2) 准备安全求交测试样本数据并执行安全求交任务
测试步骤	启动多方安全计算产品系统的安全求交任务
预期结果	1) 安全求交任务成功执行 2) 参与方只获得交集 ID，任何一方无法获得交集以外的其他参与方的 ID 且准确性相比同样条件下明文计算满足结果误差小于 2^{-32}
备注	无

6.3.6 特征工程

6.3.6.1 特征预处理

测试项目	特征预处理
测试目的	验证对特征预处理功能的支持能力
测试环境	部署完成的多方安全计算环境
前置条件	1) 输入数据已整理成符合的格式 2) 计算任务和结果输出/呈现方式已配置
测试步骤	创建特征预处理训练任务并查看任务结果
预期结果	1) 产品支持的特征预处理任务可以正确完成 2) 能够根据清洗的数据正确执行安全建模任务
备注	特征预处理包括异常值清洗、缺失值清洗、特征无量钢化（标准化、归一化）、特征分箱、特征编码等。

6.3.6.2 特征相关性分析

测试项目	特征相关性分析
测试目的	验证对特征统计分析功能的支持能力
测试环境	部署完成的多方安全计算环境
前置条件	1) 输入数据已整理成符合的格式 2) 计算任务和结果输出/呈现方式已配置
测试步骤	创建特征统计分析任务，查看任务结果
预期结果	1) 产品支持的特征统计分析功能可以在联邦状态下正确完成 2) 能够根据统计分析的结果进行可视化呈现
备注	特征相关性分析包括相关系数矩阵、协方差等，应至少有一种特征相关性分析在联邦状态下实现

6.3.6.3 特征选择

测试项目	特征选择
测试目的	验证特征选择过程用户数据隐私不被泄露
测试环境	部署完成的多方安全计算环境
前置条件	1) 输入数据已整理成符合的格式 2) 计算任务和结果输出/呈现方式已配置

测试步骤	1) 创建特征选择任务，查看任务结果 2) 查看执行特征选择任务过程中对用户隐私保护情况
预期结果	1) 产品支持的特征选择任务可以正确完成 2) 在执行特征选择过程中用户数据隐私不被泄露
备注	特征选择需要在联邦状态下实现

6.3.7 联合预测

测试项目	机器学习联合预测
测试目的	验证对联合预测功能的支持能力
测试环境	部署完成的多方安全计算系统
前置条件	1) 部署节点并启动多方安全计算系统 2) 准备机器学习测试模型和待测样本数据 3) 执行多方安全计算任务
测试步骤	按产品支持的机器学习算法（监督学习、无监督学习、半监督学习等），逐一启动安全计算任务
预期结果	在不泄露各方数据的前提下，预测结果与明文计算相比，AUC 等指标损失不大
备注	无

6.3.8 数据安全融合

测试项目	跨行业或跨机构 1 亿条以上数据安全融合
测试目的	验证跨行业或跨机构数据安全融合量是否达到要求
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 准备测试数据集，包含 1 亿条以上的数据 2) 配置参与方代理程序和环境 3) 进行跨行业互联互通测试 4) 验证数据融合的准确性和一致性，比较每个参与方计算得到的结果是否一致，并与明文计算结果进行对比 5) 检测系统的性能指标，包括计算时间、内存占用、网络带宽等
预期结果	1) 1 亿条以上数据安全融合可以正确处理并输出结果 2) 系统的性能和稳定性达到要求，且准确性相比同样条件下明文计算满足结果误差小于 2^{-32}
备注	无

6.4 安全模型测试

6.4.1 半诚实模型

测试项目	半诚实模型
测试目的	验证多方安全计算产品对半诚实模型的支持能力
测试环境	部署完成的多方安全计算系统
前置条件	1) 在不同参与方部署多方安全计算节点 2) 启动多方安全计算系统

	3) 设定参与方中的一方为不诚实实体
测试步骤	1) 启动多方安全计算任务 2) 半诚实模型占用大量的资源 3) 观察半诚实模型的行为，记录其对系统和其他参与方的影响 4) 在任务结束后，检查其他参与方的数据和结果，确认是否遭受不诚实实体的攻击或影响
预期结果	1) 多方安全计算任务成功执行 2) 其他参与方完成计算任务
备注	无

6.4.2 恶意模型

6.4.2.1 恶意模型（篡改输出密文）

测试项目	支持恶意模型（篡改输出密文，可选）
测试目的	验证可抵抗恶意模型的篡改输出密文攻击
测试环境	部署完成的多方安全计算系统
前置条件	1) 在不同参与方部署多方安全计算节点 2) 启动多方安全计算系统 3) 准备恶意模型篡改后的输出密文 4) 设定参与方中的一方为恶意实体
测试步骤	1) 启动多方安全计算任务 2) 恶意实体篡改输出密文 3) 观察并记录恶意行为对系统和其他参与方的影响 4) 在任务结束后，检查其他参与方的数据和结果，确认是否遭受恶意模型的攻击或影响
预期结果	1) 多方安全计算任务成功执行 2) 其他参与方的数据和结果没有遭受攻击或影响
备注	此测试评价方法为可选

6.4.2.2 恶意模型（发送错误数据）

测试项目	支持恶意模型（发送错误数据，可选）
测试目的	验证可抵抗恶意模型的发送错误数据攻击
测试环境	部署完成的多方安全计算系统
前置条件	1) 在不同参与方部署多方安全计算节点 2) 启动多方安全计算系统 3) 准备恶意模型要发送的错误数据 4) 设定参与方中的一方为恶意实体
测试步骤	1) 启动多方安全计算任务 2) 恶意实体发送错误数据 3) 观察并记录恶意行为对系统和其他参与方的影响 4) 在任务结束后，检查其他参与方的数据和结果，确认是否遭受恶意模型的攻击或影响
预期结果	1) 多方安全计算任务成功执行 2) 其他参与方的数据和结果没有遭受攻击或影响
备注	此测试评价方法为可选

6.4.2.3 恶意模型（拒绝服务攻击）

测试项目	支持恶意模型（拒绝服务攻击，可选）
测试目的	验证可抵抗恶意模型的拒绝服务攻击
测试环境	部署完成的多方安全计算系统
前置条件	1) 在不同参与方部署多方安全计算节点 2) 启动多方安全计算系统 3) 设定参与方中的一方为恶意实体
测试步骤	1) 启动多方安全计算任务 2) 恶意实体占用大量的资源 3) 观察并记录恶意行为对系统和其他参与方的影响 4) 在任务结束后，检查其他参与方的数据和结果，确认是否遭受恶意模型的攻击或影响
预期结果	1) 多方安全计算任务成功执行 2) 其他参与方完成计算任务
备注	此测试评价方法为可选

6.4.3 抗合谋攻击

6.4.3.1 抗合谋攻击（数据篡改）

测试项目	抗合谋攻击（数据篡改）
测试目的	验证可抵抗数据篡改的合谋攻击
测试环境	部署完成的多方安全计算系统
前置条件	1) 在不同参与方部署多方安全计算节点 2) 启动多方安全计算系统 3) 准备合谋攻击测试中需要篡改的数据 4) 设定参与方中的一方或多个方为合谋者
测试步骤	1) 启动多方安全计算任务 2) 合谋者共同篡改数据，以影响计算任务的正确性。 3) 观察并记录合谋攻击行为对系统和其他参与方的影响 4) 在任务结束后，检查其他参与方的数据和结果，确认是否遭受合谋攻击的影响
预期结果	1) 多方安全计算任务成功执行 2) 其他参与方的数据和结果没有遭受攻击或影响
备注	无

6.4.3.2 抗合谋攻击（拒绝服务攻击）

测试项目	抗合谋攻击（拒绝服务攻击）
测试目的	验证可抵抗拒绝服务的合谋攻击
测试环境	部署完成的多方安全计算系统
前置条件	1) 在不同参与方部署多方安全计算节点 2) 启动多方安全计算系统 3) 设定参与方中的一方或多个方为合谋者
测试步骤	1) 启动多方安全计算任务 2) 合谋者占用大量的资源 3) 观察并记录合谋攻击行为对系统和其他参与方的影响 4) 在任务结束后，检查其他参与方的数据和结果，确认是否遭受合谋攻击的影响

预期结果	1) 多方安全计算任务成功执行 2) 其他参与方完成计算任务
备注	无

6.5 算法性能测试

由于性能表现与环境配置、数据集大小相关，下列测试方法对应的推荐配置为：服务器16 核 CPU、256G 内存、1T 硬盘，网络带宽 100Mbps；除特殊说明外，各方测试数据集应至少包含 1 亿条数据，均为 1 列，单条数据不小于 4 字节。

6.5.1 基础运算性能

测试项目	基础运算性能
测试目的	验证基础运算耗时达到要求
测试环境	部署完成的多方安全计算系统
前置条件	1) 各参与方已上传测试数据集 2) 登录多方安全计算平台 3) 审计日志已开启
测试步骤	1) 两个参与方参与计算，分别执行求和、乘法、比较运算 2) 三个参与方参与计算，分别执行求和、乘法运算
预期结果	1) 正常产生输出结果 2) 两方运算耗时在 10min 之内，三方运算耗时在 20min 之内
备注	无

6.5.2 安全统计性能

测试项目	安全统计性能测试
测试目的	验证安全统计耗时达到要求
测试环境	部署完成的多方安全计算系统
前置条件	1) 各参与方已上传测试数据集 2) 登录多方安全计算平台 3) 审计日志已开启
测试步骤	1) 两个参与方参与安全统计，分别计算方差、中位数 2) 三个参与方参与安全统计，分别计算方差、中位数
预期结果	1) 正常输出结果 2) 两方计算耗时在 10min 之内，三方计算耗时在 20min 之内
备注	无

6.5.3 安全查询性能

测试项目	安全查询性能测试
测试目的	验证安全查询耗时达到要求
测试环境	部署完成的多方安全计算系统
前置条件	1) 各参与方已上传测试数据集，每方数据集包含至少 1 亿条 ID 2) 登录多方安全计算平台 3) 审计日志已开启
测试步骤	1) 执行百级不可区分计算任务，从被查询数据集中随机抽取 10000 个 ID 2) 执行百万级不可区分计算任务，从被查询数据集中随机抽取 1 个 ID

预期结果	1) 正常输出结果 2) 百级不可区分耗时在 30min 之内，百万级不可区分耗时在 1min 之内
备注	无

6.5.4 安全求交性能

测试项目	安全求交性能测试
测试目的	验证安全求交耗时达到要求
测试环境	部署完成的多方安全计算系统
前置条件	1) 各参与方已上传测试数据集 2) 登录多方安全计算平台 3) 审计日志已开启
测试步骤	1) 设置每个参与方数据集大小均为 1 亿行，两方数据的相交率为 50%，执行两方平衡的安全求交任务 2) 设置一个参与方数据集至少 1 亿行、另一个参与方至少 10 万行，两方数据相交率为 50%，执行两方非平衡的安全求交任务
预期结果	1) 正常输出结果 2) 两方平衡计算耗时在 80min 之内，两方非平衡计算耗时在 25min 之内
备注	无

6.5.5 特征工程性能

测试项目	特征工程性能测试
测试目的	验证特征工程耗时达到要求
测试环境	部署完成的多方安全计算系统
前置条件	1) 两个参与方已上传测试数据集，共至少 100 万行 / 50 维特征，一方持有标签 2) 登录多方安全计算平台 3) 审计日志已开启
测试步骤	1) 两个参与方启动特征工程任务 2) 进行特征工程 WOE 与 IV 计算 3) 分析输出结果
预期结果	1) 正常输出结果 2) 计算耗时在 30min 之内
备注	无

6.5.6 安全建模性能

测试项目	安全建模性能测试
测试目的	验证安全建模耗时达到要求
测试环境	部署完成的多方安全计算系统
前置条件	1) 两个参与方已上传测试数据集，两方均为 1 亿行，特征数≥1 2) 登录多方安全计算平台 3) 审计日志已开启
测试步骤	1) 两个参与方启动安全建模任务 2) 选择相应的模型 3) 执行安全建模任务 4) 分析输出结果

预期结果	1) 正常输出结果 2) 计算结果准确率在 0.8 以上，明密文建模在同等条件下模型评价指标误差小于 1%
备注	无

6.5.7 联合预测性能

测试项目	联合预测性能测试
测试目的	验证联合预测耗时达到要求
测试环境	部署完成的多方安全计算系统
前置条件	1) 两个参与方已上传测试数据集，共至少 100 万行 / 50 维特征，一方持有标签 2) 登录多方安全计算平台 3) 审计日志已开启
测试步骤	1) 两个参与方启动联合预测任务 2) 选择计算类型为逻辑回归 3) 执行联合预测任务 4) 分析输出结果
预期结果	1) 正常输出结果 2) 计算单次迭代耗时 5min 之内
备注	无

6.6 互联互通性能测试

由于性能表现与环境配置相关，下列测试方法对应的推荐配置为：服务器 16 核 CPU、256G 内存、1T 硬盘，网络带宽 100Mbps。

6.6.1 数据量级

测试项目	多方安全计算互联互通技术支持的数据量
测试目的	测试多方安全计算互联互通技术支持的数据量是否达到要求
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 准备测试数据集：生成包含 10 亿条以上的测试数据，单条数据大小≥4 字节，确保数据集的质量和多样性，覆盖不同场景 2) 配置参与方代理程序：针对多方安全计算互联互通技术的实现，配置相应的参与方代理程序，确保每个参与方代理程序能够处理大规模数据集 3) 进行互联互通测试：将上述 10 亿条以上的测试数据分配给各个参与方，并执行任务层面的互联互通操作。 4) 记录时间和资源消耗：在进行互联互通测试时，记录每个操作的耗时和资源消耗情况。这包括计算时间、内存占用、网络带宽等指标 5) 监测系统稳定性：在测试过程中，检测系统的稳定性和可靠性。注意检测是否存在内存泄露、崩溃或性能下降等问题
预期结果	系统能够处理 10 亿条以上的数据，同时保持正常的功能和性能
备注	无

6.6.2 参与方数量

测试项目	互联互通参与方测试
测试目的	测试是否最少支持至少 8 个参与方互联互通
测试环境	部署完成的多方安全计算系统
前置条件	1) 数据方已上传对应的数据资源 2) 登录多方安全计算平台
测试步骤	1) 准备测试环境：配置至少 8 个参与方的环境，并确保它们都能够相互通信和协作。每个参与方应具备执行多方安全计算算法所需的功能和资源 2) 设计测试场景：根据所选的多方安全计算算法，设计适当的测试场景。考虑数据共享、聚合、查询、建模等不同操作，并确定各个参与方在这些场景中的角色与任务 3) 进行互联互通测试：将测试数据分配给每个参与方，并执行任务层面的互联互通操作。确保数据在参与方之间进行加密、传输和解密，并进行相应的计算和处理 4) 测试通信和协议性能：监测并记录参与方之间的通信时间、延迟、带宽以及协议执行的效率。检查是否存在通信故障、丢包、重传等问题 5) 验证数据一致性和结果准确性：比较每个参与方计算得到的结果是否一致，并与明文计算结果进行对比。确保多方安全计算互联互通的结果准确无误 6) 测试稳定性和可扩展性：在测试过程中，检测系统的稳定性和可扩展性。检查是否存在内存泄露、资源竞争、性能下降等问题
预期结果	系统在多方互联互通场景中的表现满足预期要求
备注	无