ICS 35.240.40
A11

团　　体　　标　　准

T/PCAC 0009-2021

多方安全计算金融应用评估规范

Testing specification on secure multi-party computation financial application

2021-06-29 发布　　2021-06-29 实施

中国支付清算协会　发布

目　　录

前　言

本规范由中国支付清算协会提出。

本规范由中国支付清算协会安全与技术标准专业委员会归口。

本规范主要起草单位：中国支付清算协会、中国工商银行股份有限公司、中国农业银行、中国银行股份有限公司、交通银行股份有限公司、中国银联股份有限公司、中国金融电子化公司、华控清交信息科技（北京）有限公司、北京国家金融科技认证中心、国家金融科技测评中心（银行卡检测中心）、中金金融认证中心有限公司、国家应用软件产品质量监督检验中心、信息产业信息安全测评中心、上海富数科技有限公司、公安部第三研究所、支付宝（中国）网络技术有限公司、财付通支付科技有限公司、深圳市腾讯计算机系统有限公司、腾讯云计算（北京）有限责任公司、星环信息科技（上海）股份有限公司、北京百度网讯科技有限公司、北京数牍科技有限公司、微众银行、鼎铉商用密码测评技术（深圳）有限公司、中互金认证有限公司、北京瑞莱智慧科技有限公司、京东数字科技控股股份有限公司、同盾科技有限公司。

本规范主要起草人：陈波、于沛、相海飞、侯晓晨、高飞、薛宇、侯玉华、王潮、彭顺求、陈杭、汪星辰、郑德署、康鑫、谢谨、王光中、周雍恺、孙权、郭大圣、冯晓文、杨祖艳、王云河、何昊青、李浒、窦永金、王钊、渠韶光、于鸽、杨波、许中奇、郑峥、邱晓慧、尤萌、崔虎男、张鹏、翟耀超、刘健、董晶晶、卞阳、黄翠婷、胥怡心、张艳、宋铮、吴永强、蒋增增、罗松、章书、果伦、李逸、陈浩、谢国斌、蔡超超、单进勇、张天豫、严强、邹超、谭锐能、李增局、聂春祺、徐世真、顾松庠、彭南博、李晓林、彭宇翔等。

本规范为首次发布。

多方安全计算金融应用评估规范

1 范围

本标准规定了多方安全计算金融应用的评估要求。

本标准适用于多方安全计算的金融应用机构、技术服务和解决方案提供商。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

JR/T 0196-2020 多方安全计算金融应用技术规范

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

3 术语和定义

3.1 多方安全计算 Secure Multi-Party Computation（MPC）

基于多方数据协同完成计算目标的密码技术，实现除计算结果及其可推导出的信息之外不泄漏各方隐私数据。多方安全计算常采用的技术有混淆电路(Garbled Circuit)、不经意传输(Oblivious Transfer)、秘密分享(Secret Sharing)、同态加密（Homomorphic Encryption）等。

3.2 密钥交换 key exchange

在通信实体之间安全地交换密钥的方案，可以使通信双方在非安全通信线路上为信息传送安全地交换密钥。

3.3 密码协议 cryptographic protocol

两个或两个以上参与者使用密码算法，按照约定的规则，为达到某种特定目的而采取的一系列步骤。

3.4 密钥管理 key management

根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

3.5 数字签名 digital signature

签名者使用自己的私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.6 MPC 精度 MPC accuracy

用于衡量多方安全计算结果精确度。与相同数据明文计算结果相比，连续相同有效位数越多精度越高。对于计算结果存在多个数值的情况，可根据实际应用度量每个数值的精度或将多个数值拟合成一个数值后再计算精度。

来源：JR/T 0196-2020.

3.7 安全参数 security parameter

用以衡量多方安全计算协议安全强度或破解难度的一组参数。MPC安全参数主要包括不诚实门限、统计安全参数、计算安全参数。
来源：JR/T 0196-2020.

3.8 管理域 management domain

管理域是一些资源的集合，域内的行为服从于一个系统管理的政策。

3.9 计算节点 computation node

计算方执行多方安全计算协议或算法逻辑的软件、计算机、虚拟计算机或集群。一个计算方对应一个计算节点和管理域，对外提供一个交互接口，如IP地址、端口等。
来源：JR/T 0196-2020.

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）
TLS：传输层安全协议（Transport Layer Security）
MPC：多方安全计算（Secure Multi-Party Computation）
TPS：每秒处理任务数(Transactions Per Second)

5 技术评估

评估项的适用性分为三类：

1) M：指该评估项是必须评估项目；
2) O：指该评估项是可选评估项目；
3) C：指该评估项是条件可选评估项目，即根据产品所声明的能力或具体业务场景而需要满足的要求项。

5.1 参与方与工作时序

5.1.1 参与方

评估目的：产品技术框架是否涵盖任务发起方、调度方、算法提供方、数据提供方、计算方、结果使用方等参与方类型。

适用性：M

评估方法：

1) 查看产品技术文档中与参与方、参与方关系相关的描述；
2) 登陆系统，根据系统组成、角色组成判断参与方构成和关系。

通过标准：

1） 技术文档中对参与方有相关描述，并能涵盖全部6个参与方，其中数据提供方和计算方数量大于等于2；
2） 技术文档中具体描述了系统组成、角色等与参与方的对应关系；
3） 产品实现与系统描述一致。

5.1.2 工作时序

评估目的：产品中MPC任务的主要计算流程是否能够涵盖任务创建、任务分配、数据接入、任务执行、结果解析等步骤。

适用性：M

评估方法：

1) 查看产品技术文档中对MPC任务计算流程的描述；
2) 登陆系统，完成一个MPC任务计算流程。

通过标准：

1) 技术文档中对MPC任务计算流程进行了描述，能够涵盖任务创建、任务分配、数据接入、任务执行、结果解析等步骤；
2) 系统中MPC任务能够顺利执行，工作步骤与文档描述一致。

5.2 数据输入

5.2.1 数据输入转化

评估目的：数据提供方是否将隐私数据转化为输入因子并提供给指定的计算节点。

适用性：M

评估方法：

1) 执行MPC计算任务，记录数据提供方的输出数据和接收方；
2) 检查数据输入转化过程是否使用了随机数。

通过标准：

1) 输入因子生成过程采用了随机数，且随机数生成算法未存在公开漏洞；
2) 数据提供方按照MPC任务配置信息将输入因子发送给了指定计算节点（该计算节点被该数据提供方持有的情况可除外）。

5.2.2 数据源接入

评估项：数据源类型

评估目的：数据提供方是否支持数据源接入，包括但不限于数据库和文件，数据库类型如关系型数据库、列式数据库、数据仓库等，文件类型如txt、csv、xml、key-value。

适用性：M

评估方法：

1) 查看相关技术文档中关于可支持数据源类型的描述；
2) 在数据提供方上执行相关类型数据源的导入操作。

通过标准：

1) 技术文档中对可支持数据源类型进行了明确的描述；
2) 数据提供方能够导入技术文档中描述的数据源类型。

评估项：类型扩展

评估目的：数据提供方是否扩展支持新的数据类型。

适用性：O

评估方法：

1) 查看相关技术文档中关于对数据源类型扩展的支持方式，如配置文件、配置指令、SDK接口等；
2) 查看与数据源类型扩展相关的配置文件、指令或接口；
3) 执行可扩展类型的数据源的导入操作。

通过标准：

1) 技术文档中对可支持数据类型进行了明确的描述；
2) 数据提供方能够导入配置文件中描述的数据源类型。

5.2.3 数据集管理

评估项：添加与删除

评估目的：数据提供方是否支持数据集添加、删除。

适用性：M

评估方法：

1） 查看相关技术文档对数据提供方在数据集管理方面功能的要求；

2） 在数据提供方上执行数据集添加、删除操作。

通过标准：

1) 相关技术文档描述了数据提供方在数据集管理方面的功能；
2) 数据提供方提供了本地数据集的添加、删除功能。

评估项：指定使用方

评估目的：数据提供方是否支持指定数据集的使用方；

适用性：M

评估方法：

1) 查看数据方指定数据集使用方的方式，如一次性指定数据使用方，或者对数据使用方的每次申请进行单独审批，并按相应的方式进行操作。

通过标准：

2) 数据提供方能够对数据集的使用指定使用方。

评估项：指定用途用量

评估目的：数据提供方是否支持指定数据集用途和用量；

适用性：O

评估方法：

1) 查看数据方指定数据集用途和用量的方式，如一次性指定，或者对数据使用方的每次申请进行单独审批，并按相应的方式进行操作。

通过标准：

1） 数据提供方能够指定数据集的用途和用量。

评估项：任务接入状态查询

评估目的：数据提供方是否支持查询数据集任务接入状态；

适用性： M

评估方法：

1) 任务发起方发起一个任务，符合数据提供方的数据使用授权条件，或者由数据提供方进行单独授权；
2) 在数据提供方上查看数据集当前的任务接入状态，如是否已绑定计算任务。

通过标准：

1） 能够在数据提供方查看已授权数据集的任务接入状态。

评估项：执行状态查看

评估目的：数据提供方是否支持监控数据集参与计算的状态，如正在参与计算、使用完毕等。

适用性： M

评估方法：

1）执行已授权数据使用的MPC任务；

2）查看正在执行任务、或已经执行完毕的数据集。

通过标准：

1）成功执行已授权数据使用的MPC任务；

2）数据提供方可查看到数据集的任务执行状态。

5.2.4 元数据管理

测试项：元数据查询

评估目的：

1) 数据提供方是否使用元数据描述数据集；

2) 数据提供方是否支持元数据查询功能，包括名称、标记、描述、大小、样例、类型等信息。

适用性：M

评估方法：

1) 在数据提供方上查看数据集的描述信息；

2) 在数据提供方上按照元数据查询数据集。

通过标准：

1) 数据提供方在展示数据集时给出了各类元数据信息；

2) 数据提供方能够按照元数据查询本地数据集。

测试项：元数据同步

评估目的：数据提供方是否支持向数据需求方提供数据集的元数据信息。

适用性：O

评估方法：

1) 在数据提供方上提交数据集的元数据信息给调度方（供其他数据需求方查询）或直接给数据需求方。

通过标准：

1）数据提供方能够将元数据信息提供给数据需求方。

5.2.5 数据预处理

评估目的：评估数据提供方是否具备数据存储格式转换等数据预处理功能。

适用性：O

评估方法：

1) 查看相关技术文档中关于数据预处理、数据格式转换等方面的描述；

2) 在数据提供方导入数据源，查看数据格式转换等数据预处理效果。

通过标准：

1）数据通过预处理后可满足后续计算任务要求。

5.2.6 取消授权

评估目的：数据提供方能否在任务执行完成前取消数据的使用授权。

适用性：C

评估方法：

1) 在数据提供方上对已经接入任务、尚未执行的数据集取消任务接入。

通过标准：

1) 数据提供方能够对已接入任务的数据集取消数据使用授权。

5.2.7 存证

评估目的：数据提供方是否对发送数据进行存证。

适用性：M

评估方法：

1) 执行MPC任务，查看数据提供方的存证记录；

通过标准：

1) 数据提供方在MPC任务执行时对发送数据给计算节点的记录进行了存证（该计算节点被该数据提供方持有的情况可除外）；
2) 存证记录中至少有时间戳、数据接收方、所用密码算法等信息。

5.3 算法输入

5.3.1 算法逻辑类型

评估项：查询算法

评估目的：评估是否支持常见的查询算法，如Select、Sort、Join等。

适用性：C

评估方法：

1) 查验相关技术文档，获取支持的查询算法列表；
2) 执行MPC联合查询任务，查看查询结果。

通过标准：

1) 支持常见的查询算法，如Select、Sort、Join等；
2) 查询结果与明文查询功能保持一致。

评估项：统计分析

评估目的：评估是否支持常见的统计分析算法，如均值、方差、中位数等。

适用性：C

评估方法：

1） 查验相关技术文档，获取支持的统计分析算法列表；

2） 执行MPC统计分析操作，查看统计分析结果。

通过标准：

1） 统计分析结果与明文计算结果相比，差异满足应用对MPC精度的要求。

评估项：机器学习

评估目的：评估是否支持常见的机器学习算法，如线性回归、逻辑回归、神经网络、K-Means、PCA、决策树、XGBoost等，以及是否支持梯度下降等常见的机器学习模型优化算法。

适用性：C

评估方法：

1) 查看技术文档获取支持的机器学习算法列表与模型优化算法列表；

2) 执行机器学习相关的MPC任务；

3) 评估预测结果（准确率/AUC等指标）与明文预测结果的一致性。

通过标准：

1) MPC机器学习任务的训练结果与明文训练结果相比，准确率和AUC等模型评估指标的差异满足应用对MPC精度的要求。

评估项：特征工程

评估目的：评估是否支持常见的特征工程算法，如采样、特征选择、分箱、WOE计算、one-hot编码等。

适用性：O

评估方法：

1） 查验相关技术文档，获取支持的特征工程算法列表；

2） 执行MPC特征工程操作，查看特征被处理后的结果正确性。

通过标准：

1） 特征被处理后结果与明文特征处理结果相比，结果一致。

5.3.2 算法输入方式

评估项：高级语言输入

评估目的：评估是否支持以一种或多种常用的算法逻辑语言输入，如C/C++、Python、Java等。

适用性：C

评估方法：

1) 查验相关技术文档，获取支持的算法逻辑语言类型；

2) 使用声明的算法逻辑语言编写代码，执行MPC任务。

通过标准：

1) 按照语言类型能够编写代码并生成MPC任务，任务输出正确结果。

评估项：算法参数输入

评估目的：评估是否支持将算法中的重要参数作为数据进行输入，如查询条件、机器学习中的模型参数等。

适用性：C

评估方法：

1) 查验相关技术文档，检查算法参数的输入形式，是否支持输入算法的重要参数，以何种形式输入；

2) 实际验证。运行一个任务实例，对已知模型进行数据预测，将模型的参数作为隐私数据输入。

通过标准：

1) 模型参数作为隐私数据输入后能够正确执行MPC任务并输出正确结果。

评估项：输入交互

评估目的：评估是否支持常见输入交互方式，如Web网页、命令行、OpenAPI等。

适用性：O

评估方法：

1) 查验相关技术文档，确认支持的交互方式；

2) 实际验证交互方式是否可用。

通过标准：

1) 输入交互指令后，Web端、命令行、OpenAPI等能够返回正确的结果，且符合交互形式对于内容、格式的要求。

评估项：在线编程

评估目的：评估是否支持算法在线编写、修改、调试、提交等。

适用性：C

评估方法：

1) 查看相关技术文档，查验是否支持算法在线编程功能（编写、修改、调试、提交等）；
2) 实际验证算法在线编程功能是否能正常执行。

通过标准：

1) 能够正确完成技术文档中声明的在线编程功能。

5.3.3 算法逻辑管理

评估项：MPC引擎算法交互

评估目的：评估是否将算法逻辑进行处理后交给MPC引擎进行运算。

适用性：C

评估方法：

1) 对于具有在线编程功能的MPC应用，通过编写代码逻辑确定并启动MPC计算任务。

通过标准：

1) 应能输出算法逻辑并启动MPC引擎进行计算。

评估项：算法逻辑交互

评估目的：评估是否对输入的算法逻辑进行列表显示、运行状态查看、删除等。

适用性：O

评估方法：

1) 查看计算任务及相应的算法逻辑；
2) 查看任务运行状态，通过删除任务删除算法逻辑。

通过标准：

1) 能够对计算任务或算法逻辑进行列表显示；
2) 能够查看算法逻辑所对应任务的执行状态，能够删除任务。

5.4 协同计算

评估项：运算类型

评估目的：计算引擎是否支持加、乘、比较等常见运算。

适用性：C

评估方法：

1) 查看技术文档关于支持的应用类型和基本运算类型；
2) 执行MPC计算任务，涵盖声明的基本运算类型；
3) 执行完毕后，查看相应的输出数据；
4) 与明文计算结果比对，检验输出数据是否正确。

通过标准：

1) 能够成功执行声明的基本运算类型；
2) 输出数据正确。

评估项：数值计算

评估目的：计算引擎是否支持常见数值计算。

适用性：M
评估方法：
1) 执行常见的数值计算类（如abs、sqrt、exp、count、max、min等）MPC任务；
2) 在系统处理完后，查看相应的输出数据；
3) 检验输出数据是否正确。
通过标准：
1) 能够正常执行常见多方数值计算任务；
2) 输出数据正确。

评估项：计算一致性
评估目的：评估运算结果与相同数据明文计算结果是否一致。
适用性：M
评估方法：
1) 执行MPC任务；
2) 在系统处理完后，查看相应的输出数据；
3) 对应明文按照同样计算逻辑进行计算。
通过标准：
1) 能够正常产生输出数据；
2) 输出数据跟明文计算的结果一致。

评估项：数据类型
评估目的：计算引擎是否支持整数、小数、常见字符、字符串在内的一种或多种基本数据类型。
适用性：M
评估方法：
1) 查看技术文档声明支持的数据类型；
2) 发起计算任务，对声明的数据类型逐一进行测试。
通过标准：
1) 能够输入特定数据类型的一种或多种，如整型（integer、bigint、tinyint、smallint）、浮点型（float、double、decimal、real）、字符串（char、varchar）等；
2) 能够执行特定数据类型的计算任务；
3) 任务能够正常完成，输出结果正确。

评估项：数据单元
评估目的：计算引擎是否支持标量、矢量、矩阵、多维数组在内的一种或多种基本数据单元。
适用性：O
评估方法：
1) 查看技术文档声明支持的数据单元类型；
2) 发起计算任务，对声明的数据单元类型逐一进行测试。
通过标准：
1) 能够输入标量、矢量、矩阵、多维数组在内的一种或多种基本数据单元；
2) 能够执行所支持数据单元的MPC任务；
3) MPC任务能够正常完成，输出结果正确。

评估项：管理域
评估目的：每个计算节点是否有独立的管理域。
适用性：C

评估方法：

1) 查看节点网络环境、物理环境和安全管理策略，记录环境数据；
2) 查看节点主体归属。

通过标准：

1) 能确保每个节点有独立的管理域，即归属为不同的主体方，由各主体方分别控制。

评估项：算法匹配

评估目的：各计算节点是否能够将数据提供方提供的输入因子匹配算法逻辑。

适用性：M

评估方法：

1) 执行一个或多个MPC任务，查看任务执行结果。

通过标准：

1) 各任务匹配成功，输出结果正确。

评估项：运算

评估目的：保证直接在计算因子上完成运算，得到输出因子。

适用性：M

评估方法：

1) 执行MPC任务，通过抓包查看计算节点输入数据，检查用于运算的数据是否全部为计算因子；
2) 通过抓包查看计算节点发送给结果使用方的数据。

通过标准：

1) 计算节点从数据提供方获得输入因子，并难以从中提取或推导出任何隐私数据，计算完成后发送输出因子给结果使用方。

评估项：缓存清除

评估目的：计算节点是否能清除计算过程缓存的计算因子

适用性：M

评估方法：

1) 查看技术文档关于清除计算因子的说明；
2) 查看清除计算因子的源代码；
3) 执行MPC任务，查看源代码执行情况；
4) 查看计算因子缓存状态，检查是否清除。

通过标准：

1) 计算节点能够清除计算因子缓存。

评估项：接收调度

评估目的：计算节点是否能够接收调度方的任务调度。

适用性：O

评估方法：

1) 执行MPC任务；
2) 在调度方上查看任务调度情况（计算节点的使用情况）；
3) 观察参与计算的节点运行日志或状态。

通过标准：

1) MPC任务成功执行，参与计算的节点有相关任务执行日志或其它输出，并能通过日志或其它输出查看其任务参与情况。

评估项：并发处理

评估目的：计算节点是否能并发处理不同的计算任务。

适用性：O

评估方法：

1) 同时发起多个 MPC 任务，查看任务执行情况；

通过标准：

1) 计算节点能够成功接收多个任务并发调度且计算成功，结果显示正确；
2) 检查多个计算任务的执行日志和执行时间，确认是多个任务是真正同时并行执行的。

评估项：输出因子发送

评估目的：计算节点是否支持将输出因子发送给结果使用方进行解析。

适用性：M

评估方法：

1) 执行MPC任务，查看结果使用方是否获得输出因子；
2) 检查结果使用方获得的输出因子是否与计算节点发送的输出因子内容一致（该计算节点被该结果使用方持有的情况可除外）。

通过标准：

1) 结果使用方可以成功获得输出因子，且内容与计算节点发送的内容一致。

5.5 结果输出

评估项：接收因子

评估目的：结果使用方是否能够接收计算方的输出因子。

适用性：M

评估方法：

1) 执行MPC任务，在结果使用方上查看接收的数据，并与计算节点发送的数据进行对比。

通过标准：

1) 结果使用方接收的数据与计算节点发送的一致（该计算节点被该结果使用方持有的情况可除外）。

评估项：输出正确性

评估目的：结果使用方是否能够解析、输出正确的计算结果。

适用性：M

评估方法：

1) 执行MPC任务，查看结果使用方的输出结果；
2) 将输出结果和基于明文数据的计算结果进行比对，验证结果的正确性。

通过标准：

1) 结果使用方将输出因子解析为输出结果；
2) 输出结果满足MPC正确性要求。

评估项：存证

评估目的：结果使用方是否能够对接收的输出因子进行存证。

适用性：M

评估方法：

1) 执行MPC任务；
2) 查看结果使用方的存证记录。

通过标准：

1) 结果使用方在MPC任务执行时对接收计算方输出因子的记录进行了存证（该计算方与该结果使用方是同一参与主体的情况可除外）。
2) 存证记录中至少有时间戳、数据发送方、所用密码算法等信息。

5.6 调度管理

5.6.1 参与方管理

评估目的：调度方是否具备对MPC各参与方的管理功能，统一管理接入的计算节点以及数据提供方接入的数据源，如新加入、撤销、上下线等。

适用性：O

评估方法：

1) 在调度方上查看其他参与方情况，如计算节点以及接入的数据源；
2) 对已添加的计算节点或数据源进行上线或下线操作，在调度方上进行查看；
3) 计算节点或数据源退出MPC计算，在调度方进行查看。

通过标准：

1) 调度方具备对MPC各参与方的管理功能，如对计算节点、数据源的加入、撤销、上下线的管理。

5.6.2 任务配置

评估项：生成任务配置

评估目的：调度方是否支持与用户交互创建任务，生成任务配置信息。

适用性：O

评估方法：

1) 通过与调度方交互创建MPC任务，包括指定可用的数据源、以及其他参与方等；
2) 任务创建成功后可查看配置信息，包括所用数据源、其他参与方等。

通过标准：

1) 调度方提供了与任务发起方的交互接口，能够创建MPC任务。

评估项：发送任务配置

评估目的：调度方是否能够将具体任务配置信息分发给数据提供方、计算方、结果使用方。

适用性：M

评估方法：

1) 创建任务，查看任务配置信息；
2) 执行任务，查看任务执行结果。

通过标准：

1) 数据提供方、计算方、结果使用方能够按照统一的任务配置信息成功执行任务、获得任务结果。

5.6.3 任务执行

评估项：多任务调度

评估目的：调度方是否对多任务执行进行统一调度，如任务排队、负载以及优先级调度。

适用性：C

评估方法：

1) 对于支持多任务处理的MPC系统，同时发起多个MPC任务，查看任务执行情况；

通过标准：

1) 多任务处理系统能够对任务进行调度管理，如排队、负载、优先级调度等；
2) 多任务都能够执行成功，输出执行结果。

评估项：任务执行结果保存

评估目的：调度方是否能够保存任务的执行结果，如执行结果成功等。

适用性：O

评估方法：

1) 执行MPC任务，查看任务执行情况；

通过标准：

1) 能够查看已经完成的任务的执行结果，如执行成功或失败情况。

评估项：任务执行监控

评估目的：调度方是否监控、管理任务执行过程，直至任务执行结束并展示执行结果。

适用性：M

评估方法：

1) 执行MPC任务，查看任务的执行过程和执行结果；
2) 查看已发生过的执行记录。

通过标准：

1) 能够展示任务的执行过程和最后结果；
2) 能够展示已发生任务的执行结果。

评估项：任务动态分配

评估目的：

1) 调度方是否支持基于计算节点动态发现、任务动态分配；
2) 调度方是否支持任务量动态变化。

适用性：O

评估方法：

1) 添加计算节点，执行多任务，查看任务分配情况；
2) 查看任务量发生变化时的任务执行情况。

通过标准：

1) 能够发现新添加的计算节点，并给新节点分配计算任务，能将新节点纳入整体任务分配体系中；
2) 任务量发生变化时通过增加服务能力仍能保证任务正常执行；
3) 当某个计算节点空闲时能够自动分配剩余任务执行。

6 安全评估

6.1 协议安全

6.1.1 基本安全要求

评估项： 隐私数据安全

评估目的：MPC协议保证除计算结果及其可推导出的信息之外，不泄漏各方隐私数据。

适用性：M

评估方法：

1） 查阅产品手册、设计文档、原理说明等材料，确认所采用的协议能够保证隐私数据安全；
2） 访谈MPC金融应用主要技术负责人，及检查代码，确认采用上述协议；
3） 提供MPC协议安全性论证材料，包括已发表的论文证明或由专家对协议安全进行评审；
4） 执行MPC计算任务，查看所有系统过程信息以及系统日志，确认没有隐私数据泄露。
通过标准：
1） 提供的资料能够证明所采用的MPC协议能够保证除了计算结果及其可推导出的信息之外，不泄露各方隐私数据；
2） 人员访谈及代码检查，均确认采用上述MPC协议；
3） MPC协议安全性具备已发表的论文证明或由专家对协议安全进行评审并出具证明材料；
4） MPC计算任务成功执行，系统过程信息及日志，均没有隐私数据泄露。

评估项： 计算结果正确
评估目的：MPC协议保证除异常终止外输出计算结果的正确性。
适用性：M
评估方法：
1） 查阅产品手册、设计文档、原理说明等材料，确认计算逻辑正确性和计算结果的准确性；
2） 访谈MPC金融应用主要技术负责人及检查代码，确认采用上述协议；
3） 提供MPC协议安全性论证材料，包括已发表的论文证明或由专家对协议安全进行评审；
4） 执行MPC计算任务，查看计算结果的正确性。
通过标准：
1） 提供的资料能够证明所采用的MPC协议，能够保证计算结果的正确性；
2） 人员访谈及代码检查，均确认采用上述MPC协议；
3） MPC协议计算结果正确性具备已发表的论文证明或由专家对协议安全进行评审并出具证明材料；
4） MPC计算任务成功执行，计算结果符合预期。

评估项： 协议公平性
评估目的：MPC协议，是否保证协议的公平性，仅当诚实的参与方获得计算输出的时候，不诚实的参与方才能获得计算输出。
适用性：O
评估方法：
1) 查阅产品手册、设计文档、原理说明等材料，确认协议的公平性；
2) 访谈MPC金融应用主要技术负责人，及检查代码，确认采用上述协议；
3) 组织专家评审，确认MPC协议满足公平性要求；
4) 提供MPC协议公平性论证材料，包括已发表的论文证明或由专家对协议安全进行评审。
通过标准：
1) 提供的资料能够证明所采用的MPC协议，能够保证协议公平性；
2) 人员访谈及代码检查，均确认采用上述MPC协议；
3) MPC协议公平性具备已发表的论文证明或由专家对协议安全进行评审并出具证明材料。

评估项： 输入数据独立性
评估目的：MPC协议，是否保证输入数据的独立性，多个数据提供方在构建输入数据时是相互独立。
适用性：O
评估方法：
1） 查阅产品手册、设计文档、原理说明等材料，确认输入数据的独立性；

2） 访谈MPC金融应用主要技术负责人，及检查代码，确认采用上述协议；

3） 组织专家评审，确认MPC协议满足输入数据独立性要求。

通过标准：

1) 提供的资料能够证明所采用的MPC协议，能够保证输入数据的独立性；

2) 人员访谈及代码检查，均确认采用上述MPC协议；

3) MPC协议的输入数据独立性具备已发表的论文证明或由专家对协议安全进行评审并出具证明材料。

6.1.2 安全模型

评估项：半诚实模型

a) 评估目的： 在MPC应用中应根据相应的安全模型选择和管理各参与主体，MPC的金融业务系统应保证半诚实模型下MPC协议的使用场景中相应参与方均为半诚实。

适用性：C(如果MPC应用支持半诚实模型，必测)

评估方法：

1） 查阅产品手册、设计文档、原理说明等材料，分析在半诚实模型下，是否所有参与方均是半诚实的；

2） 访谈MPC金融应用主要技术负责人，确认采用上述方案；

3） 查看系统，包括参与方的配置文件、参数设置、网络配置等，确认采用上述方案。

通过标准：

1) 半诚实模型下，各参与方都是半诚实。

b) 评估目的：在MPC金融应用中，在半诚实模型下采用的MPC协议的安全性是否满足要求。

适用性：C(如果MPC应用支持半诚实模型，必测)

评估方法：

1） 提供MPC协议在半诚实模型下的安全性论证材料，包括已发表的论文证明或由专家对协议安全进行评审；

2） 运行MPC计算任务，查看任务执行的计算因子，是否与协议声明一致。

通过标准：

1） MPC协议在半诚实模型下的安全性论证具备已发表的论文证明或由专家对协议安全进行评审并出具证明材料；

2） MPC计算任务产生的计算因子与协议声明一致。

评估项：恶意模型

a) 评估目的： 在MPC金融应用，可以根据相应的安全模型选择和管理各个参与主体。其中在实际应用场景中，MPC金融业务系统应保证恶意模型下MPC协议的使用场景中不诚实参与方的数量不超过协议的不诚实门限。

适用性：C(如果MPC应用支持恶意模型，必测)

评估方法：

1） 查阅资料，包括协议设计文档和技术文档，检查在实际应用场景中，可能合谋的参与方数量，是否超过MPC协议的不诚实门限；

2） 访谈多方安全金融应用主要技术负责人，确认采用上述方案；

3） 查看系统，包括参与方的配置文件、参数设置、网络配置等，确认采用上述方案。

通过标准：

1) MPC金融业务系统中不诚实参与方数量不会超过MPC协议的不诚实门限。

b) 评估目的：在MPC金融应用中，在恶意模型下采用的MPC协议的安全性是否满足要求

适用性：C(如果MPC应用支持恶意模型，必测)

评估方法：

1） 提供MPC协议在恶意模型下的安全性论证材料，包括已发表的论文证明或由专家对协议安全进行评审；

2） 运行MPC计算任务，查看任务执行的计算因子，是否与协议声明一致；

3） 系统应提供恶意参与方模拟测试功能，披露相关设计和代码，模拟恶意计算节点随机将正确的计算因子替换成随机数，实现错误注入，运行MPC计算任务，评估系统是否能检测错误并中止，拒绝输出结果。

通过标准：

1） MPC协议在恶意模型下的安全性论证具备已发表的论文证明或由专家对协议安全进行评审并出具证明材料；

2） MPC计算任务产生的计算因子与协议声明一致；

3） MPC计算任务在错误注入之后中止，拒绝输出结果，错误注入功能的代码与恶意参与方模拟的设计一致。

6.1.3 安全参数

评估项： 统计安全参数（l）

评估目的： 在MPC金融应用中，采用的MPC协议，统计安全参数(l)应不低于30。

适用性：C

评估方法：

1） 查阅资料，包括MPC协议设计文档，原理资料，统计安全参数(l)论证材料等，确定统计安全参数(l)的大小；

2） 测试系统，根据上述协议，对输入数据进行计算因子生成测试。

通过标准：

1） 通过资料分析与论证，采用的MPC协议的统计安全参数(l)不低于30；

2） 通过理论推导，确定根据输入数据产生的计算因子的概率分布，与不知道输入数据随机模拟的计算因子的概率分布，两者在统计上不可区分（统计距离不高于2^{-30}）。

评估项： 计算安全参数（k）

评估目的：在MPC金融应用中，采用的MPC协议，计算安全参数(k)应不低于112

适用性：M

评估方法：

1） 查阅资料，包括MPC协议设计文档，原理资料，计算安全参数(k)论证材料等，确定计算安全参数(k)的大小；

2） 测试系统：基于上述协议，推导多项式时间攻击者破解MPC协议的计算复杂度。

通过标准：

1) 通过资料分析与论证，采用的 MPC 协议的计算安全参数(k)不低于 112；

2) 通过原理推导，确定多项式时间攻击者破解 MPC 协议的计算复杂度不低于 $O(2^{112})$。

6.2 隐私数据安全

隐私数据包括数据提供方输入的数据、结果使用方获得的数据，以及算法参数和模型参数中需要被保护的数据。

在实施评估工作前，根据被测系统的文档描述及相关评估报告，确定隐私数据范围，确定包括算法参数及模型参数在内的隐私数据的整个生命周期是否在设计文档中详细描述，需要依据 《GBT

37988-2019 信息安全技术 数据安全能力成熟度模型》。确定文档中描述的MPC协议与专家评审中通过的MPC协议一致。

6.2.1 应用过程隐私安全要求

评估目的：每个计算节点在整个计算过程中是否都无法提取或推导其他参与方的任何隐私信息，最终的输出结果也不会出现在计算节点内，确保应用过程的隐私性。

适用性：M

评估方法：

1） 查阅产品所使用的安全交互模型、安全报告，以及运行的配置文件等信息；

2） 利用专业工具，通过对目标系统的扫描、探测、抓包等操作，使其产生特定的响应等活动，通过分析响应结果，获取证据以证明对端获取的网络报文是否存在隐私数据的泄露。

通过标准：

1） 根据产品配置信息和配置文件，确定计算节点，分析计算节点的日志中不含有未授权的隐私数据；

2） 根据产品配置信息和配置文件，确定结果节点，分析结果节点的日志中不含有未授权的隐私数据；

3） 运行系统，监听网络通信接口，截获数据流，分析非数据方节点的数据，其中不含未授权的隐私数据。

6.2.2 其他参与方安全要求

评估目的：保证计算过程中是否不出现其他参与方的隐私信息。

适用性：M

评估方法：

1） 利用专业工具，通过对目标系统的扫描、探测等操作，使其产生特定的响应等活动，通过分析响应结果，获取证据以证明信息系统的基本要求、性能、安全性是否得以有效实施。

通过标准：

1） 运行系统，监听网络通信接口，截取数据流，分析数据中不含有隐私数据。

6.2.3 隐私数据获取安全要求

评估目的：保证数据提供方的隐私数据不被其他参与方获取，结果使用方从结果信息推导出的信息除外。

适用性：M

评估方法：

1） 查阅设计文档、系统配置文件等相关材料；

2） 利用专业工具，通过对目标系统的扫描、探测等操作，使其产生特定的响应等活动，通过分析响应结果，获取证据以证明信息系统的安全性是否得以有效实施。

通过标准

1） 查看设计文档，系统设计中采用的算法是可信的MPC算法；

2） 查看系统配置文件，确定各个参与方已经正确配置，权限合理；

3） 运行系统，监控非数据方的网络通信接口，截取数据流，分析数据中不含有隐私数据。

6.2.4 计算结果隐私安全要求

评估目的：保证计算结果只被结果使用方获取，而不会被其他参与方知晓，保障结果隐私性。

适用性：M

评估方法：查阅资料、测试系统

1） 查阅设计文档、系统配置文件等相关材料；
2） 利用专业工具，通过对目标系统的扫描、探测等操作，使其产生特定的响应等活动，通过分析响应结果，获取证据以证明信息系统的基本要求、性能、安全性是否得以有效实施。

通过标准：

1） 查看设计文档，系统设计中采用的算法是可信的MPC算法；
2） 查看系统配置文件，确定各个参与方已经正确配置，权限合理；
3） 运行系统，查看任务列表，结果方下载计算结果。监控各方的网络通信接口，截取数据流，分析除结果方外数据中不含有隐私数据；
4） 仅结果使用方获得计算结果，非结果方无法获得计算结果。

6.2.5 防单点故障扩散要求

评估目的：采取措施加强每个节点的隐私保护能力，不应因单点出现故障而泄露任何一方的有关信息。

适用性：M

评估方法：

1） 利用专业工具，通过对目标系统的扫描、探测等操作，使其产生特定的响应等活动，通过分析响应结果，获取证据以证明信息系统的基本要求、性能、安全性是否得以有效实施。

通过标准：

1） 根据系统配置，逐一将数据提供方子节点、计算方子节点、算法方子节点、结果方子节点进行故障模拟配置；
2） 运行系统，查看任务列表中任务状态，监控数据流，隐私数据不应有泄露的情况。

6.2.6 模型隐私安全要求

评估目的：是否能将算法参数、模型参数作为隐私数据来保证算法和模型的安全。

适用性：M

评估方法：

1） 查阅审计报告、自查报告、外部评估报告、设计文档、开发文档、用户文档、管理文档、产品检测报告等相关材料；
2） 查看系统日志、配置文件、参数设置、产品版本、网络配置等；
3） 利用专业工具，通过对目标系统的扫描、探测等操作，使其产生特定的响应等活动，通过分析响应结果，获取证据以证明信息系统的基本要求、性能、安全性是否得以有效实施。

通过标准：

1） 查看产品设计手册及产品自检报告，确定各参与方采用的安全模型种类及参数；
2） 查看系统配置，确定与产品设计手册一致；
3） 运行测试系统记录安全模型的整个执行流程及相关数据，备案；
4） 确认算法参数、模型参数可以作为隐私数据来保证算法和模型的安全。

6.2.7 算法逻辑安全要求

评估目的：在MPC金融应用中，输入的应用算法逻辑是否存在安全漏洞导致隐私数据泄露。

适用性：O

评估方法：

1） 查阅产品手册、设计文档、原理说明等材料，分析是否具有应用算法逻辑安全性审查机制；
2） 访谈MPC金融应用主要技术负责人和查看系统，确认采用上述方案；
3） 运行不安全的MPC应用算法逻辑，确认系统是否有安全性审查机制。

通过标准：

1) 提供的资料能够证明具有应用算法逻辑安全性审查机制；
2) 人员访谈及系统检查，均确认采用上述应用算法逻辑安全性审查机制；
3) 运行不安全的MPC应用算法逻辑后，系统能够进行相应的算法逻辑安全性审查，识别出MPC应用算法逻辑的安全性问题，并执行相应的处理机制。

6.2.8 个人金融信息保护

评估目的：MPC金融应用所涉及的其他数据应符合国家法律法规与行业主管部门有关规定的要求。
适用性：C（业务系统检测）
评估方法：
1) 查阅业务系统的隐私数据保护策略、公司管理规定等材料，从个人信息的收集、传输、存储和使用等个人信息的全生命周期，分析是否符合《JRT 0171-2020 个人金融信息保护技术规范》；
2) 访谈 MPC 金融应用业务系统负责人，确认符合上述管理规定和保护策略的要求；
通过标准：
1) 提供MPC金融应用业务系统个人金融信息保护的评估报告；
2) 人员访谈及系统检查，个人信息的收集、传输、存储和使用均符合个人金融信息保护技术规范要求；

6.3 认证授权

6.3.1 身份认证要求

a) 评估目的：检查多方安全计算应用各参与方之间进行通信时相互之间是否进行身份认证。
适用性：M
评估方法：
1） 查看系统设计说明文档，是否提供各参与方之间进行通信时的双向身份认证的机制；
2） 启动一个多方安全计算任务，抓取参与方之间进行通信的数据包，分析、确认是否正确采用了文档中描述的身份认证机制。
通过标准:
1） 设计文档说明了各参与方之间的通信采用了基于密码技术的双向身份认证机制；
2） 经测试，参与方之间通信时采用了基于密码技术的双向身份认证机制。

b) 评估目的：检查多方安全计算应用是否具备对接入系统用户的身份鉴别能力。
适用性：M
评估方法：
1） 检查对接入系统的用户是否提供身份鉴别能力，例如，口令认证、证书认证、令牌认证等；
2） 以正确的鉴别信息和错误的鉴别信息，分别尝试进入系统，检查是否仅在输入正确的鉴别信息才能进入系统并执行相关操作。
通过标准:
1） 系统对用户进入系统要求进行身份鉴别；
2） 系统具有明确的错误鉴别次数；
3） 仅允许输入正确的鉴别信息才能进入系统并执行相关操作。

c) 评估目的：检查多方安全计算应用是否对各参与方进行相应的权限设置和控制，避免出现信息泄露或操作风险。
适用性：M
评估方法：

1) 按照说明文档，以系统管理员身份对各参与方设置权限控制策略；
2) 启动一个多方安全计算任务，以参与方身份访问权限范围内的数据，查看是否访问成功；
3) 以参与方身份尝试绕过权限设置访问权限范围外的数据，查看是否存在权限控制策略被绕过的情形。

通过标准:

1） 为各参与方分配相应的权限，设置了权限控制策略；
2） 经测试，各参与方能够成功访问权限范围内的数据；
3） 经测试，各参与方的访问权限不超过预定义的范围，无法访问权限范围外的数据。

d) 评估目的：检查多方安全计算应用对接入系统用户的身份鉴别是否采用两种或两种以上组合的认证方式实现用户身份认证。

适用性：0

评估方法：

1）查阅技术文档，确定系统是否支持两种或两种以上组合认证方式实现用户身份认证；
2）测试验证同一用户身份认证方式是否采用两种或两种以上的身份认证方式，如口令+数字证书或口令+令牌等。

通过标准：

1) 系统支持两种或两种以上组合认证方式实现用户身份认证；
2) 同一用户采用两种或两种以上组合的认证方式实现用户身份认证。

6.3.2 数据使用授权要求

a) 评估目的：检查多方安全计算应用的调度方是否能够对未被授权的计算请求协调发起数据使用授权申请，申请内容应包含数据使用方证书、数据使用范围、数据使用期限等。检查多方安全计算应用是否在数据提供方同意后向使用方发送授权，用于后续计算时的权限认证。

适用性：O

评估方法:

1） 验证调度方是否可以对未被授权的请求协调发起数据使用权限申请；
2） 验证授权使用申请的内容是否包含了数据使用方证书、数据使用范围、数据使用期限等条件；
3） 验证数据提供方是否可以对申请内容进行验证并授权。

通过标准：

1） 调度方可以对未授权的计算请求协调使用授权申请；
2） 申请的内容包含了数据使用方证书、数据使用范围、数据使用期限；
3） 数据提供方可以根据申请内容进行授权，同意后可以向使用方发送授权用于后续计算时的权限认证。

b) 评估目的：检查多方安全计算应用的调度方是否对每个任务请求验证其数据使用授权的合法性，包括授权是否有效、数据使用范围和使用期限是否合理等。

适用性：M

评估方法：

1） 发起多个多方安全计算任务，查看调度方是否针对每个任务请求的数据使用授权进行验证；
2） 检查数据使用授权、使用范围和使用期限是否合理有效。

通过标准：

1) 调度方应对每个任务请求验证其数据使用授权、使用范围和使用期限合理有效。

c) 评估目的：检查多方安全计算应用的数据提供方是否能取消数据使用授权。

适用性：O

评估方法：

1） 查看数据提供方是否能够对自己已经授权使用的数据取消授权。

通过标准：

1) 数据提供方能够对自己的数据使用授权执行取消操作。

6.4 密码安全

6.4.1 密码算法

评估目的：检查多方安全计算应用使用的密码算法是否符合国家密码管理部门的要求。

适用性：C

评估方法：

1） 检查设计文档中包含的密码算法种类；

2） 检查系统中密码算法 API 是否与设计文档中的描述一致；

3） 检查系统中密码算法的代码实现是否符合国家、行业标准和相关要求。

通过标准：

1） 设计文档中包含的密码算法符合国家密码管理部门的要求；

2） 系统中的密码算法 API 与设计文档中的描述一致；

3） 系统中的密码算法实现符合国家、行业相关标准和要求。

6.4.2 密钥长度

评估目的：检查多方安全计算应用使用的密码算法的密钥长度是否符合国家密码管理部门的要求。

适用性：M

评估方法：

1） 检查技术文档中涉及的密码算法对应的密钥长度描述；

2） 检查系统中使用密码算法的密钥长度是否与设计文档中的描述一致。

通过标准：

1） 设计文档中密码算法的密钥长度符合国家密码管理部门的要求；

2） 系统中使用密码算法的密钥长度与设计文档中的描述一致。

6.4.3 密钥管理

评估目的：检查多方安全计算应用中密钥管理是否符合国家密码管理部门的要求。

适用性：M

评估方法：

1） 检查设计文档中对产品涉及的密钥管理生命周期相关环节（如生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等）的描述；

2） 检查产品代码中涉及的密钥管理环节是否与设计文档一致。

通过标准：

1） 设计文档涉及的密钥管理环节的描述符合国家密码管理部门的要求。

2） 系统中各类密钥管理的程序代码与设计文档中一致。

6.4.4 密码产品

评估目的：检查多方安全计算应用采用的密码产品是否符合国家密码管理部门的要求。

适用性：O

评估方法：

1） 检查设计文档包含的密码产品是否通过国家密码管理部门核准；

2） 检查系统中密码产品的使用是否与设计文档中的描述一致。

通过标准：

1） 设计文档包含的密码产品应通过国家密码管理部门核准；

2） 系统中密码产品的使用与设计文档中的描述一致。

6.5 通信安全

6.5.1 通信双方的身份认证和密钥交换

评估目的：检查多方安全计算应用在通信节点建立连接之前是否使用符合国家密码标准的密钥交换技术来产生双方共享的认证密钥，并进行双向身份认证，确保通信节点是信息的真实授权方。

适用性：M

评估方法：

1） 检查设计文档中通信双方进行双向身份认证的密码技术是否符合国家密码标准；

2） 检查设计文档中在通信节点建立连接之前使用的密钥交换技术是否符合国家密码标准；

3） 检查系统中使用的进行密钥交换、身份认证的密码技术是否与设计文档中的描述一致。

通过标准：

1） 设计文档中通信双方进行双向身份认证的密码技术符合国家密码标准；

2） 设计文档中在通信节点建立连接之前使用的密钥交换技术符合国家密码标准；

3） 系统中用于密钥交换、身份认证的密码技术与设计文档中的描述一致。

6.5.2 安全通信通道的建立

评估目的：检查多方安全计算应用是否使用符合国家密码标准的技术来建立安全通信通道，避免因传输协议受到攻击而出现的信息被窃取或篡改。

适用性：M

评估方法：

1） 检查设计文档中安全通信通道建立采用的密码协议（包括建立连接前的密钥交换协议）等技术是否符合国家密码标准；

2） 检查系统中安全通信通道建立采用的密码协议等技术是否与设计文档中的描述一致；

3） 检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；

4） 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设计文档中的描述一致。

通过标准：

1） 设计文档中安全通信通道建立采用的密码协议等技术符合国家密码标准；

2） 系统中安全通信通道建立采用的密码协议等技术与设计文档中的描述一致；

3） 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；

4） 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。

6.5.3 通信数据的机密性和完整性保护和验证

评估目的：检查多方安全计算应用中是否使用了符合国家密码标准的数字签名等技术对通信中的数据进行机密性、完整性保护和验证。

适用性：M

评估方法：

1） 检查设计文档中包含的对通信数据进行机密性和完整性保护和验证的数字签名等技术是否符合国家密码标准；

2） 检查系统中使用的对通信数据进行机密性和完整性保护和验证的数字签名等技术是否与设计文档中的描述一致；

3） 抓取通信数据包，解析数据格式或内容，判断是否与设计文档中描述的机密性和完整性保护和验证机制一致。

通过标准：

1） 设计文档中包含的对通信数据进行机密性和完整性保护和验证的数字签名等技术符合国家密码标准；

2） 系统中使用的对通信数据进行机密性和完整性保护和验证的数字签名等技术与设计文档中的描述一致；

3） 获取的通信数据包中对数据进行的机密性和完整性保护和验证机制与设计文档中的描述一致。

6.5.4 通信数据被篡改后的识别和异常处理机制

评估目的：检查多方安全计算应用中，通信数据被篡改后数据接收方是否能够识别并立即采取异常处理。

适用项：C

评估方法：

1） 检查设计文档中是否包含数据接收方对通信数据包被篡改后的识别和异常处理机制；

2） 检查系统中数据接收方对通信数据包被篡改后的识别和异常处理机制与设计文档的描述是否一致。

通过标准：

1） 设计文档包含数据接收方对通信数据包被篡改后的识别和异常处理机制；

2） 系统中数据接收方对通信数据包被篡改后的识别和异常处理机制与设计文档的描述一致。

6.5.5 通信延时、中断等异常情况的处理与恢复机制

评估目的：检查多方安全计算应用中是否具备通信延时、中断等异常情况的处理与恢复机制。

适用项：M

评估方法：

1） 检查设计文档是否包含对网络延时、中断等网络通讯异常情况下的异常处理与恢复机制；

2） 检查系统提供的对网络延时、中断等网络通讯异常情况的异常处理与恢复机制是否与设计文档描述一致。

通过标准：

1） 设计文档包含对网络延时、中断等网络通讯异常情况下的异常处理与恢复机制；

2） 系统提供的对网络延时、中断等网络通讯异常情况下的异常处理与恢复机制与设计文档中的

描述一致。

6.5.6 重新获取信息的能力

评估目的：检查多方安全计算应用中各参与方在检测到数据完整性被破坏时，是否具有从发送方重新获取信息的能力。

适用性：O

评估方法：

1） 检查设计文档中是否包含各参与者检测到数据完整性被破坏后从发送方重新获取信息的机制；

2） 检查系统提供的从发送方重新获取信息的机制是否与设计文档中的描述一致。

通过标准：

1） 设计文档中包含各参与者检测到数据完整性被破坏后从发送方重新获取信息的机制；

2） 系统提供的从发送方重新获取信息的机制与设计文档中的描述一致。

6.6 存证与日志

6.6.1 用户日志保存要求

评估目的：各参与方应保存用户的操作日志。

适用性：M

评估方法：

1） 查阅产品手册和设计文档，查看日志保存功能；

2） 启动MPC计算任务,记录并结合审计日志分析多方安全计算。

通过标准：

1） 查看相关文档（如设计文档等），对用户日志保存进行了要求，对保存日志的要求进行了明确，包括但不限于对日志保存的方式、日志包括的内容、日志的留存期限、日志文件大小、日志能否被任意篡改/删除都有明确的要求；

2） 各参与方安全计算过程中均能产生对应过程的日志且日志记录正确，同时保存的日志中在非必要的情况下不允许包括关键/敏感等信息，如果必须包含关键/敏感等信息，需要对日志采用密码技术或脱敏技术进行保护，且采用的密码技术应符合国家密码管理部门相关要求，日志保存期限满足6个月以上。

6.6.2 存证要求

评估目的：在MPC金融应用中，各参与方应对计算过程中的相关结果和信息进行存证。

适用性：M

评估方法：

1） 查阅产品手册和设计文档，查看过程信息存证设计；

2） 查看系统和配置文件，检查过程信息存证系统配置；

3） 启动MPC计算任务, 记录并结合审计日志分析多方安全计算。

通过标准：

1） 查看相关文档（如设计文档等），应对结果和信息的存证方式、内容、位置等要素提出要求；

2） 存证内容的生成采用了密码技术（如数字签名），起到防伪造、防篡改、防抵赖的效果；

3） 对各参与方计算过程的结果及关键操作产生的日志进行了留存，且涉及关键/敏感等信息的留存结果应采用密码技术保护，采用的密码技术应符合国家密码管理部门相关要求；

4） 存证的结果和信息不能被任意篡改、删除、丢弃或被覆盖等，有完整的规则对存证内容进行要求；

5） 对存证的结果如果需要再使用（提供第三方进行分析），应将关键/敏感等信息进行脱敏处理；
6） 计算结果及信息的存证能满足审计需求。

6.6.3 日志及存证审计要求

评估目的：在MPC金融应用中，具备对各参与方的用户操作日志和结果存证的审计能力，对于违背约定的数据提供方、计算方和结果使用方应能通过存证、审计等方法发现和追踪。

适用性：M

评估方法：

1） 查阅产品手册和设计文档，查看日志和存证审计设计；
2） 查看系统审计记录。

通过标准：

1） 参与方的操作权限与系统设置的一致；
2） 审计可筛选（如选择审计的业务项），日志和存证结果真实、完整；
3） 审计结果能够输出为文件或其他形式；
4） 审计记录的内容包括但不限于审计事件的日期、时间、事件类型等审计要素，同时具有定期备份功能，审计记录保存在6个月以上。

6.6.4 存证及溯源要求

评估目的：在MPC金融应用中，对数据提供方和结果使用方的每次计算任务角色进行存证和记录，保证信息安全性与结果可追溯性。

适用性：M

评估方法：

1） 查阅产品手册和设计文档，查看过程信息存证设计；
2） 查看系统记录，验证对数据提供方和结果使用方的每次计算任务角色进行存证和记录。

通过标准

1） 检查数据提供方和结果使用方节点启用了存证功能；
2） 能提供审计记录文档，对数提供方和结果使用方的每次计算任务角色和结果进行了证据留存，并保留了详细的审计痕迹（记录），且存证的结果和信息不能被任意篡改、删除、丢弃或被覆盖等，有完整的规则对存证内容进行要求；
3） 能提供证明材料来监管存证和结果的真实性；
4） 查看历史记录，且历史记录可追溯性满足要求（能实际追溯源头）；
5） 查看历史审计记录，且历史审计记录能被妥善保存。

7 性能评估

为保证MPC产品的质量，应在统一的测试环境配置下进行性能测试。环境配置参数至少包括：CPU核数、内存、网络带宽等。推荐的环境配置参数参考附录。

应根据MPC技术方案提供商对其产品适用范围的声明，选择相应的场景种类进行性能测试。对于具体的MPC金融应用系统，可根据相应的业务需求选择合适的指标进行测试和评估。

7.1 资金实时类计算性能

评估目的：评估MPC在资金实时类金融应用中的整数万次乘法性能指标

适用性：C

评估方法：

1） 查阅设计文档，查看整数万次乘法的计算时延、吞吐量（TPS）、计算精度的设计要求；

2） 在测试环境中开展测试，记录整数万次乘法的计算时延、吞吐量（TPS）、计算精度；
通过标准：
系统测试结果与设计文档一致，且满足：
1） 整数万次乘法计算时延≤100ms，TPS≥100，计算结果精度≥22比特位；

评估目的：评估MPC在资金实时类金融应用中的整数万次比较性能指标
适用性：C
评估方法：
1） 查阅设计文档，查看整数万次比较的计算时延、吞吐量（TPS）的设计要求；
2） 在测试环境中开展测试，记录整数万次比较的计算时延、吞吐量（TPS）；
通过标准：
系统测试结果与设计文档一致，且满足：
1） 整数万次比较的计算时延≤200 ms，TPS≥10。

7.2 资金非实时类计算性能

评估目的：评估MPC在资金非实时类金融应用中的浮点数万次乘法性能指标
适用性：C
评估方法：
1） 查阅设计文档，查看浮点数万次乘法计算时延、吞吐量（TPS）、计算精度的设计要求；
2） 在测试环境中开展测试，记录浮点数万次乘法的计算时延、吞吐量（TPS）、计算精度；
通过标准：
系统测试结果与设计文档一致，且满足：
1） 浮点数万次乘法计算时延≤1000ms，TPS≥500，计算结果精度≥32比特位；

评估目的：评估MPC在资金非实时类金融应用中的浮点数万次比较性能指标
适用性：C
评估方法：
1） 查阅设计文档，查看浮点数万次比较的计算时延、吞吐量（TPS）的设计要求；
2） 在测试环境中开展测试，记录浮点数万次比较的计算时延、吞吐量（TPS）；
通过标准：
系统测试结果与设计文档一致，且满足：
1） 浮点数万次乘法的计算时延≤10000ms，TPS≥100。

7.3 非资金实时类计算性能

评估目的：评估MPC在非资金实时类金融应用中的浮点数万次乘法性能指标
适用性：O
评估方法：
1） 查阅设计文档，查看浮点数万次乘法的计算时延、吞吐量（TPS）、计算精度的设计要求；
2） 在测试环境中开展测试，记录浮点数万次乘法的计算时延、吞吐量（TPS）、计算精度；
通过标准：
系统测试结果与设计文档一致，且满足：
1） 浮点数万次乘法计算时延≤200ms，TPS≥100，计算结果精度≥26比特位；

评估目的：评估MPC在非资金实时类金融应用中的浮点数万次比较性能指标
适用性：O
评估方法：

1） 查阅设计文档，查看浮点数万次比较的计算时延、吞吐量（TPS）的设计要求；
2） 在测试环境中开展测试，记录浮点数万次比较的计算时延、吞吐量（TPS）；
通过标准：
系统测试结果与设计文档一致，且满足：
1） 浮点数万次乘法的计算时延≤300ms，TPS≥10。

7.4 非资金非实时类计算性能

评估目的：评估MPC在非资金实时类金融应用中的浮点数万次乘法性能指标。
适用性：O
评估方法：
1） 查阅设计文档，查看浮点数万次乘法的计算时延、吞吐量（TPS）、计算精度的设计要求；
2） 在测试环境中开展测试，记录浮点数万次乘法的计算时延、吞吐量（TPS）、计算精度；
通过标准：
系统测试结果与设计文档一致，且满足：
1） 浮点数万次乘法计算时延≤1000ms，TPS≥500，计算结果精度≥26比特位；

评估目的：评估MPC在非资金实时类金融应用中的浮点数万次比较性能指标。
适用性：O
评估方法：
1） 查阅设计文档，查看浮点数万次比较的计算时延、吞吐量（TPS）的设计要求；
2） 在测试环境中开展测试，记录浮点数万次比较的计算时延、吞吐量（TPS）；
通过标准：
系统测试结果与设计文档一致，且满足：
1） 浮点数万次乘法的计算时延≤1000ms，TPS≥500。

7.5 总体处理时延

评估目的：评估MPC计算任务处理时延是否满足设计要求或业务需求。
适用性：C
评估方法：
1） 查阅设计文档中关于MPC计算任务的计算精度要求和时延要求；
2） 在测试环境下执行给定的计算任务（如联合查询、统计分析等），记录从明文输入、明文转化成计算因子、基于因子计算、因子转化成明文、明文输出的总体处理时延；
3） 运行相应的明文计算任务，对比精度和时延结果。
通过标准：
1） 总体时延和计算精度满足设计要求或业务需求。

参考性附录

测试环境配置参数推荐值如下：

测试环境参数	半诚实模型	恶意模型
CPU核数	64C	128C
内存	128GB	256GB
网络带宽	千兆	千兆

其中CPU应采用主流型号。

MPC产品应在该测试环境中同时满足计算时延、吞吐量、计算精度等相关指标要求。

在实际评估过程中，可采用物理机部署或云部署，但在进行性能评估和安全通信评估时，宜采用不同物理机模拟参与方，将网络安全通信作为计算负载的一部分。

为进一步对MPC产品的计算能力进行考核，可在评估环境中通过调节降低带宽（如百兆）的方式进一步测试产品性能指标。