ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0196—2020

多方安全计算金融应用技术规范

Secure multi-party computation financial application technical specification

2020－11－24 发布　　2020－11－24 实施

中国人民银行　　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专利的责任。

本文件由中国人民银行提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

多方安全计算金融应用技术规范

1 范围

本文件规定了多方安全计算技术金融应用的基础要求、安全要求、性能要求等。

本文件适用于金融机构开展多方安全计算金融应用的产品设计、软件开发。

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。

GB/T 18391.1—2009 信息技术 元数据注册系统（MDR） 第1部分：框架

GB/T 32400—2015 信息技术 云计算 概览与词汇

3 术语和定义

下列术语和定义适用于本文件。

3.1

多方安全计算 secure multi-party computation; MPC

一种基于多方数据协同完成计算目标，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的密码技术。

注：多方安全计算常采用的技术有混淆电路、不经意传输、秘密分享、同态加密等。

3.2

参与方 party

参与多方安全计算的自然人或法人。

[来源：GB/T 32400—2015，3.1.6，有修改]

3.3

计算因子 computation factor

基于多方安全计算输入数据产生的数据。

注：包括输入因子、输出因子和中间因子：输入因子是指数据提供方执行数据输入过程后可供计算方执行后续计算的数据；输出因子是指计算方执行计算后，返回给结果使用方用以恢复最终计算结果的数据；中间因子指计算方中间计算过程中产生的数据。

3.4

数据输入 data input

采用秘密分享、混淆电路、同态加密等技术对数据提供方提供的隐私数据进行处理，使数据转化为输入因子的过程。

3.5

数据输出 data output

采用秘密分享、混淆电路、同态加密等技术对输出因子进行处理从而获得计算结果的过程。

3.6

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。

注：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。

3.7

安全模型 security model

对参与方行为模式所做的假设。

注：不同的MPC协议可基于不同的安全模型，安全模型可分为半诚实模型和恶意攻击模型两类。半诚实模型是参与方在接触和处理其他参与方隐私数据时，在严格遵守协议规范基础上，尽其所能地从接触和处理的数据中挖掘出有效信息；恶意攻击模型是参与方可能做出任何行为，尽其所能地获得关于隐私数据的有效信息，如背离协议或与他人串通等，这样的参与方也称为不诚实参与方。

3.8

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。

注：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。不诚实门限是多方安全计算协议允许合谋的不诚实参与方的最大值，当该值小于参与方数量的一半时称协议是诚实大多数的，否则称协议是不诚实大多数的；统计安全参数是一个整数l,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，两者统计上不可区分（统计距离不高于2^{-l}）；计算安全参数是一个整数k，表示多项式时间攻击者破解多方安全计算协议的计算复杂度为$O(2^k)$。

3.9

数据集 dataset

一个或多个数据提供方参与多方安全计算的数据集合。

3.10

元数据 metadata

定义和描述其他数据的数据。

[来源：GB/T 18391.1—2009，3.2.16]

3.11

计算引擎 computation engine

各计算方通过网络连接形成的执行多方安全计算的一组计算节点。

3.12

隐私数据 private data

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。

3.13

有效位数 enob

对没有小数位且以若干个零结尾的数值，从非零数字最左一位向右数得到的位数减去无效零（即仅为定位用的零）的个数。对其他数值，从非零数字最左一位向右数而得到的位数。

3.14

MPC 精度 MPC accuracy

用于衡量多方安全计算结果精确度。

注：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。

3.15

正确性 correctness

用于衡量在一定MPC精度范围内，多方安全计算与相同数据明文计算结果的一致性。

4 缩略语

下列缩略语适用于本文件。

CA：认证中心（Certification Authority）

RA：注册中心（Registration Authority）

TPS：每秒处理的事务数（Transactions Per Second）

5 概述

5.1 MPC 参与方及工作时序

5.1.1 MPC 参与方

MPC 参与方说明如下：

a) 任务发起方：触发MPC任务，在任务执行前完成任务资源配置，并对资源到位情况进行核实。

b) 调度方：配置计算任务，管理和协调其他参与方执行任务。

c) 算法提供方：为MPC提供计算逻辑和算法参数，当算法参数有保护要求时，应将该算法参数视为隐私数据，该算法提供方视为数据提供方。

d) 数据提供方：为MPC提供所需隐私数据，通过MPC数据输入处理将隐私数据转化为输入因子并发送给计算方。一个MPC计算任务中数据提供方的数量大于等于2。

e) 计算方：为MPC提供算力支持，计算方接收数据提供方的输入因子并进行计算，计算结束后将输出因子发送给结果使用方。一个MPC计算任务中计算方的数量应大于等于2，并不能由同一实体承担多个计算方角色。

f) 结果使用方：接收MPC计算结果，一个MPC计算任务的结果使用方可以有1个或多个。

5.1.2 工作时序

MPC任务工作时序包括任务创建、任务分配、数据输入、任务计算、结果解析等步骤，见图1。MPC任务工作时序具体说明如下：

a) 任务创建：
   1）任务发起方配置、核实MPC任务计算所需资源，发起计算任务。
   2）数据提供方对所有的数据使用进行授权，任务发起方和数据提供方为同一实体的情况除外。数据提供方可委托调度方对数据进行使用授权，也可在任务创建前对数据进行预授权。数据使用授权和后续任务分配阶段可合并执行。
b) 任务分配：
   1）调度方验证任务请求信息的合法性，包括身份验证和数据授权的合法性。
   2）验证通过后生成任务配置信息，发送给数据提供方、计算方和结果使用方。
   3）数据提供方、计算方和结果使用方收到任务配置信息后进行验证。
   4）各参与方保存收发的任务配置信息。
c) 数据输入：
   1）数据提供方从数据源读取数据并生成输入因子，通过安全通道发送给指定计算方。
   2）数据提供方保存任务配置信息，并对发送的输入因子进行存证。
d) 任务计算：
   1）计算节点接收各数据提供方的输入因子，按照MPC协议进行协同计算生成输出因子。
   2）将输出因子发送至结果使用方。
e) 结果解析：
   1）结果使用方对输出因子进行解析得到计算结果。
   2）对结果进行存证。

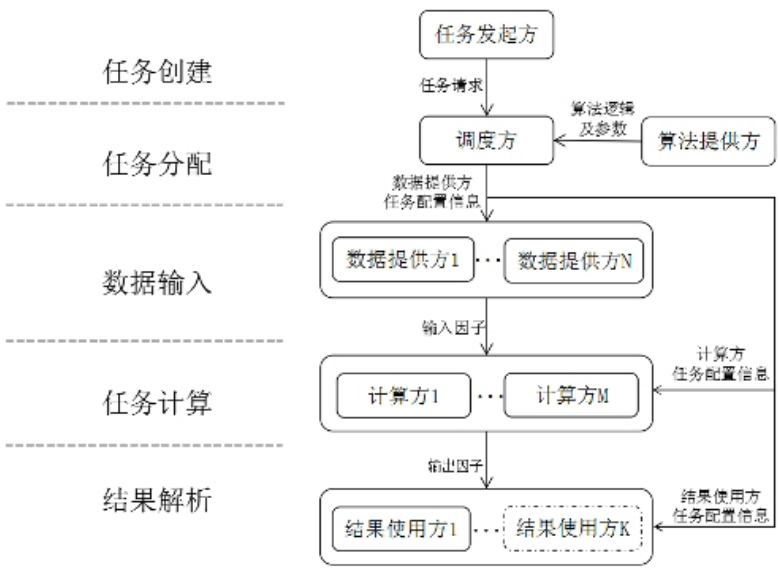

图 1　MPC 工作时序图

5.2　应用目标

MPC应满足数据隐私性、数据合法性、计算结果正确性、计算性能可接受性等要求，具体要求如下：

a) 各参与方的隐私数据不应被其他参与方获取或推知，结果使用方可从计算结果推导出的信息除外。

b) 计算过程中不应出现其他参与方的隐私数据原文。
c) 各参与方应按照计算任务约定的角色参与MPC计算。
d) 计算任务所使用的隐私数据应事先得到相应数据提供方的授权。
e) 计算结果应满足正确性要求，并只被结果使用方获取。
f) 计算性能应满足具体应用需求。

5.3 总体要求

MPC金融应用总体要求包括基础要求、安全要求和性能要求三部分，见图2。

基础要求包括数据输入、算法输入、协同计算、结果输出及调度管理等要求，分别主要针对数据提供方、算法提供方、计算方、结果使用方、调度方。

安全要求包括协议安全、隐私数据安全、认证授权、密码安全、通信安全、存证与日志等要求。

性能要求对MPC金融应用提出了计算延时、吞吐量、计算精度等性能指标要求。

图 2 MPC 金融应用总体要求

6 基础要求

6.1 数据输入

数据提供方数据输入具体要求如下：

a) 数据提供方应将隐私数据转化为输入因子，提供给指定计算节点，并确保在设定的安全模型下无法通过输入因子推算出输入数据。
b) 数据提供方应对数据源、数据集、元数据等进行统一管理：
   1）数据源管理：
      ——应支持不同类型的数据源接入，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 等；
      ——可扩展支持新的数据类型。

2）数据集管理：

——应支持对数据集的添加、删除操作；

——应支持指定数据集的使用方、用途和用量；

——应支持数据集接入状态查询功能，展示所有数据集接入任务的状态；

——应支持监控数据集参与计算状态的功能，如正在参与计算、使用完毕等。

3）元数据管理：

——应支持使用元数据描述数据集；

——应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；

——应支持向数据需求方提供数据集的元数据信息。

c） 应具备数据存储格式转换、数据预处理等功能。

d） 可在任务执行前取消数据的使用授权。

e） 应对发送数据进行存证。

6.2 算法输入

算法输入为金融应用提供算法逻辑和输入方式，并对算法逻辑进行管理，具体要求如下：

a） 算法逻辑类型：

1）应支持常见的查询操作，如 Select、Sort、Join 等。

2）应支持常见的统计分析算法，如均值、方差、中位数等。

3）应支持常用的机器学习算法，如线性回归、逻辑回归、神经网络、K-Means、PCA、决策树、XGBoost 等。

4）应支持梯度下降等常见的机器学习模型优化算法。

b） 算法输入方式：

1）应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。

2）应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。

3）应支持常见输入交互方式，如 Web 网页、命令行、OpenAPI 等。

4）应支持算法在线编写、修改、调试、提交等。

c） 算法逻辑管理：

1）将算法逻辑进行处理后应交给 MPC 引擎进行运算。

2）对输入的算法逻辑应能够进行列表显示、运行状态查看、删除等操作。

通用MPC能够满足上述所有要求。专用MPC根据金融应用需求选择满足部分要求。

不同MPC金融应用类型应符合附录A的要求；MPC典型应用场景见附录B；通用MPC系统参考架构见附录C。

6.3 协同计算

应由多个MPC计算节点组成MPC计算引擎，协同计算实现MPC协议。MPC计算节点提供基础运算，并能够通过基础运算组合实现复杂运算，具体要求如下：

a） 基础运算：

1）应覆盖加、乘、比较等常见运算。

2）应支持常见数值计算。

3）应保证运算结果与相同数据明文计算的结果一致。

4）宜支持整数、小数、常见字符、字符串在内的一种或多种基本数据类型。

5）宜支持标量、矢量、矩阵、多维数组在内的一种或多种基本数据单元。

b） MPC计算节点：

1）应确保每个计算节点均处于不同的管理域。
2）应能根据数据提供方提供的输入因子，匹配算法逻辑并执行计算任务。
3）应保证直接在计算因子上完成运算，得到输出因子。
4）应能清除计算过程缓存的计算因子。
5）应能接收调度方的任务调度。
6）应能并发处理不同的计算任务。
7）应能将输出因子发送给结果使用方进行解析。

6.4 结果输出

结果输出的具体要求如下：

a) 应能接收计算方输出因子。
b) 应对接收数据进行存证。
c) 应保证输出结果的正确性。

6.5 调度管理

调度管理的具体要求如下：

a) 应对 MPC 参与方进行管理。
b) 应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。
c) 应支持与用户交互创建任务，生成任务配置信息。
d) 应能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。
e) 应对多任务执行进行统一调度，包括任务排队、负载以及优先级调度等。
f) 应能监控、管理任务执行过程。
g) 应保存任务执行结果等。
h) 宜支持基于计算节点动态发现、任务动态分配。
i) 宜支持任务量动态变化。

7 安全要求

7.1 协议安全

7.1.1 基本安全要求

MPC协议基本安全要求如下：

a) 应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。
b) 应保证除异常终止外输出计算结果的正确性。
c) 宜保证协议的公平性，仅当诚实的参与方获得计算输出时，不诚实的参与方才能获得计算输出。
d) 宜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相互独立。

7.1.2 安全模型和安全参数要求

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协议的安全模型和安全参数的具体要求如下：

a) 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。
b) 应保证恶意攻击模型下 MPC 协议的不诚实门限不小于实际应用场景中可能合谋的参与方数量。
c) 统计安全参数（1）应不低于 30。

d） 计算安全参数（k）应不低于112。

7.2 隐私数据安全

MPC隐私数据安全的具体要求如下：

a） 应保证每个计算节点在整个计算过程中无法获取或推知其他参与方的任何隐私数据，最终输出结果也不应出现在计算节点内，确保应用过程的隐私性。

b） 应保证计算过程中不出现其他参与方的隐私数据。

c） 应保证数据提供方的隐私数据不被其他参与方获取或推知，结果使用方从结果信息推导出的信息除外。

d） 应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。

e） 应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相关信息。

f） 应能将算法参数、模型参数作为隐私数据来保证算法和模型的安全。

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要求。

7.3 认证授权

MPC认证授权的具体要求如下：

a） 应对任务计算过程中的关键环节进行身份认证，保证操作行为的合法性和抗抵赖性：

1）各参与方之间通信时应进行身份认证。

2）应具备对接入系统用户的身份鉴别能力。

3）应能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。

4）宜采用两种或两种以上组合的认证方式实现用户身份认证。

b） 应对数据提供方的数据使用进行严格控制，数据使用方应被授权：

1）调度方应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。数据提供方同意后应向使用方发送授权，用于后续计算时的权限认证。

2）调度方应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。

3）数据提供方应能取消数据使用授权。

7.4 密码安全

采用的密码算法、密钥长度及密钥管理方式等应符合国家密码管理部门与行业主管部门要求。

7.5 通信安全

MPC各参与方在信息传输时应保护传输通道与数据的安全，具体要求如下：

a） 各参与方之间进行通信时应建立安全通道，在通信节点建立连接之前应使用符合国家密码标准的密钥交换技术以产生双方共享的认证密钥，并进行双向身份认证，确保通信节点为信息的真实授权方。

b） 应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信息被窃取或篡改等风险。

c） 应使用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。

d） 当通信数据被篡改后数据接收方应能识别并立即采取异常处理。

e） 各参与方应具备对通信延时、中断等异常情况的处理机制与恢复机制。

f） 各参与方在检测到数据完整性被破坏时，应具有从发送方重新获取信息的能力。

7.6 存证与日志

MPC金融应用时应进行相应的存证与日志管理，具体要求如下：

a) 各参与方应保存用户的操作日志。

b) 各参与方应对计算过程中的相关结果和信息进行存证。

c) 应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、审计等方法进行发现、追踪。

d) 应对数据提供方和结果使用方的每次计算任务进行存证和记录，保证信息安全性与结果可追溯性。

8 性能要求

MPC金融应用的性能要求如下：

a) 应保证用户交互时延等通用指标满足具体应用需求。

b) 应声明主要计算任务的计算时延、TPS、计算精度。

c) 对于涉及实数运算的 MPC 金融应用，应保证以下指标满足具体应用需求：

——实数乘法、实数比较的 TPS，即：每秒钟能处理的实数乘法次数、实数比较次数；

——实数乘法、实数比较的计算时延，即：处理单个实数乘法和单个实数比较的处理时延；

——实数输入处理、输出处理时延；

——实数运算精度等。

d) 对于计算时延，还应给出与相同数据明文计算的时延比较结果。

根据MPC所保护的业务数据类型，将MPC应用划分为资金类和非资金类；依据业务时效性要求划分成实时类和非实时类。各类MPC应用场景的性能量化指标值见表1。

表1 MPC性能量化指标值表

场景		运算	计算时延[a]（ms）	TPS	MPC精度[b]
资金	实时	整数万次乘法	≤100	≥100	≥22
		整数万次比较	≤200	≥10	--
	非实时	浮点数万次乘法	≤1000	≥500	≥32
		浮点数万次比较	≤10000	≥100	--
非资金	实时	浮点数万次乘法	≤200	≥100	≥26
		浮点数万次比较	≤300	≥10	--
	非实时	浮点数万次乘法	≤1000	≥500	≥32
		浮点数万次比较	≤10000	≥500	--
注：非实时类应用场景含有大量数据，存在误差累计，精度要求一般高于实时类场景；非实时类应用场景单个任务的计算量一般比较大，包含很多“万次乘法和比较”运算，所以当TPS以“万次乘法和比较”为单位计算时，一般比实时类场景要大。					
[a] MPC计算节点间的计算时延，不包括输入和输出时延。 [b] 该项指标取值代表MPC计算结果与相同明文数据计算结果连续相同的有效位数（以二进制表示）。					

附 录 A
（规范性）
MPC 典型应用分类

A.1 联合查询

在联合查询应用中，查询方作为任务发起方，可以是结果使用方，同时也是算法提供方和数据提供方之一（其查询条件包含数据和算法逻辑）。查询方通过调度方查询一个或多个数据提供方的数据库，得到查询结果。联合查询应用具体要求如下：

a) 应用目标：
——查询方得到查询结果，但不暴露其查询输入（例如查询条件、数据样本）和查询结果；
——数据提供方不暴露其数据库存储的明文数据；
——查询结果与在明文数据库上查询的结果一致。

b) 工作时序：
——查询方作为任务发起方通过调度方提交查询计算任务请求；
——查询方作为数据提供方将其查询条件转化为输入因子，其他数据提供方将数据库待查询数据转化为输入因子，并将输入因子上传至事先约定的计算节点；
——计算方收到调度方分配的查询任务请求，根据获得的输入因子进行计算得到查询结果对应的输出因子，并把输出因子发送给结果使用方进行数据解析；
——结果使用方通过数据解析获得查询结果的明文。

A.2 联合建模

在联合建模应用中，算法提供方或数据提供方之一作为任务发起方触发计算任务，然后由算法提供方提供算法逻辑、数据提供方提供数据，基于MPC计算协议在多方数据集上训练机器学习模型（模型参数）。其中，计算方可以是算法提供方、数据提供方。结果使用方最后得到模型结果的明文。联合建模应用具体要求如下：

a) 应用目标：
——各数据提供方不暴露其数据集的明文；
——能保护模型参数在训练过程中的隐私安全，只有结果使用方才能得到训练后的模型明文；
——训练得到的模型与在明文数据集上训练得到的模型在新数据上具备预测结果的一致性。

b) 工作时序：
——任务发起方向调度方提交模型训练任务；
——算法提供方上传或指定模型训练所使用的算法逻辑，其算法参数或模型参数有保密需求的，可作为数据提供方之一以计算因子的方式提供；
——计算方收到调度方分配的建模任务请求，从各数据提供方获得数据集的计算因子，并利用训练算法在数据集上进行模型训练，将得到的输出因子发送至结果使用方进行解析；
——结果使用方通过解析获得训练所得的模型明文。

A.3 联合预测

在联合预测应用中，任务发起方可以同时是结果使用方。数据提供方提供样本数据集。任务发起方也可以作为数据提供方之一提供样本集。另一数据提供方提供预测模型（即模型参数）。算法提供方提供预测算法逻辑。结果使用方获得模型对样本数据集的预测结果。联合预测应用具体要求如下：

a) 应用目标：

——数据提供方不暴露其样本数据明文；

——模型提供方（数据提供方之一）不暴露其预测模型的参数；

——只有结果使用方才可以获得预测结果明文；

——预测结果与采用明文预测模型对明文样本数据的预测结果一致。

b) 工作时序：

——任务发起方向调度方提交计算任务，指定联合预测所使用的算法；

——提供样本数据的数据提供方将样本数据转化为输入因子，并提交给指定的计算方；

——提供模型的数据提供方将模型参数转化为输入因子并提交给指定的计算方，当模型参数不宜对外提供时，该数据提供方应作为计算方，避免提交模型参数；

——计算方接收调度方分配的预测任务请求，根据预测算法对样本数据的输入因子进行计算，将计算得到的预测结果的输出因子发送给结果使用方进行数据解析；

——结果使用方通过解析输出因子获得预测结果明文。

联合预测通常和联合建模复合应用，此情况下应将复合任务分解为两个 MPC 计算任务，一个任务的输出可作为另一个任务的输入，不必进行数据（如模型参数）输出后再重新输入的处理。

附 录 B
（资料性）
MPC 典型应用场景

B.1 基于 MPC 的生物特征识别

基于MPC技术的生物特征识别，可实现生物特征信息的安全共享，降低因生物特征信息泄露造成的个人信息和财产信息的风险。以刷脸付应用为例，框架图见图B.1。

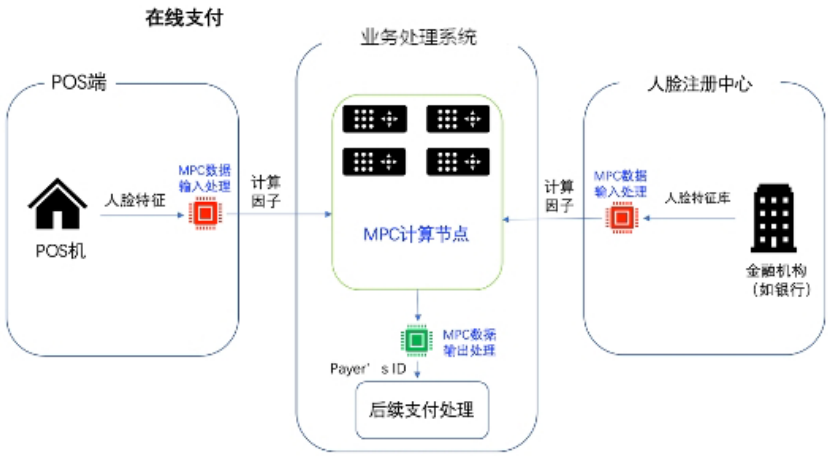

图 B.1 MPC 在刷脸付中的应用

金融机构将注册的人脸特征信息通过MPC数据输入处理后形成计算因子，并将计算因子提交给相关业务处理系统保存为人脸底库。

个人在终端设备支付时，终端设备将目标人脸特征信息也通过MPC数据输入处理后形成计算因子，并将计算因子上传至计算节点（MPC计算节点分域管理，其中的部分计算节点也可以由银行管辖）。各计算节点基于计算因子进行目标匹配和识别，最后将人脸识别结果返回并继续后续支付处理环节。

在该应用中，MPC调度方的功能嵌入到业务处理系统中，并最终获得MPC计算节点的人脸识别结果。算法逻辑即人脸识别算法已经提前预置在计算节点内。

注册环节获得的是以计算因子形式保存的人脸信息，而非原始图像，避免人脸原始图像信息共享。

识别环节自终端传输至人脸识别系统的人脸信息也是以计算因子形式呈现，避免人脸原始图像信息被获取。

B.2 基于 MPC 的联合风控

基于 MPC 的联合风控是多个金融机构之间通过 MPC 协议来交换风控数据，共同完成风控数据分析、风控模型训练和风险决策的任务，实现风控模型的精细化和个性化部署，保护风控数据的安全性，降低因金融机构间安全信息不互通、风控能力参差不齐等造成的欺诈风险。

基于 MPC 的联合风控示意图，见图 B.2。

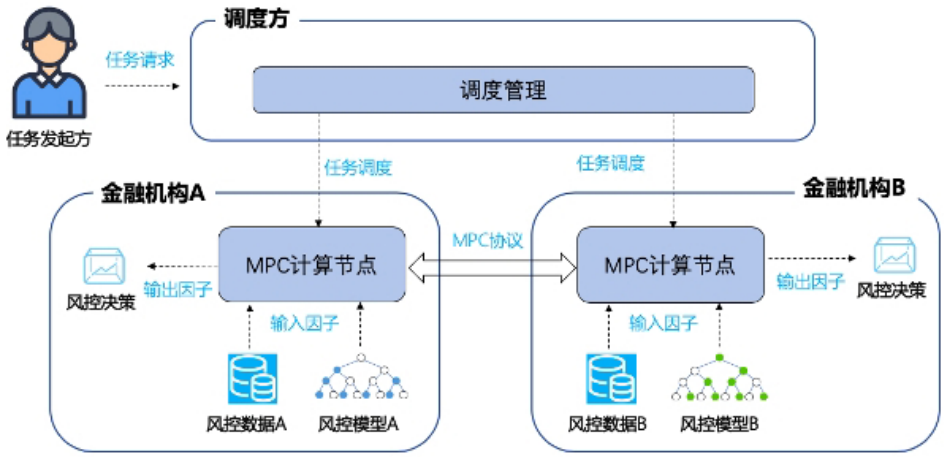

图 B.2　MPC 在联合风控中的应用

基于 MPC 的联合风控的流程如下：

a) 任务发起方向调度方发起联合风控建模和决策的任务。

b) 调度方对联合风控任务进行触发和协调，并将调度任务发送至不同的金融机构。

c) 金融机构读取本地的风控数据和风控模型，作为 MPC 输入因子。

d) 金融机构的 MPC 计算节点之间，基于 MPC 协议进行多次的随机数或加密参数交换，完成联合风控的建模和决策。

e) 金融机构各自得到联合风控的决策结果。

附 录 C
（资料性）
通用 MPC 系统参考架构

通用MPC系统参考架构见图C.1。

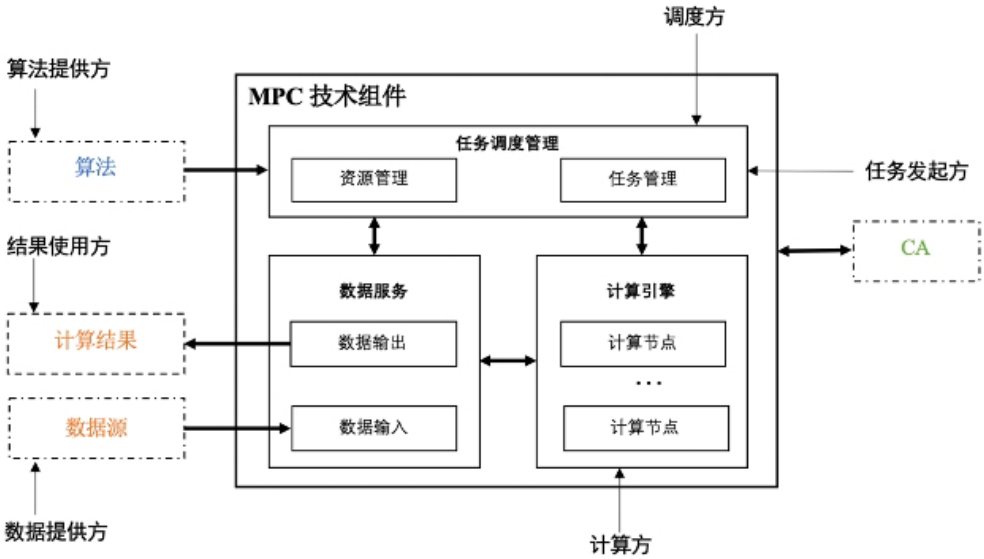

图 C.1 通用 MPC 系统参考架构

MPC系统为6个参与方角色提供操作接口，其技术组件包括任务调度管理、数据服务、计算引擎三部分。外围CA系统为各参与方进行注册和颁发证书，见GB/T 27928.1、JR/T 0118的相关要求，MPC系统可使用自建或第三方权威机构提供的CA服务。

任务调度管理组件部署在调度方，为算法方提供算法输入接口，为任务发起方提供任务触发接口，对计算节点、数据方的数据源进行统一管理，对多任务进行调度。任务调度管理可支持RA功能，从CA获取证书并分发给其他参与方。

数据输入组件部署在数据方，将数据方原始输入数据转化为输入因子。每个数据方拥有自己独立的数据输入组件。

数据输出组件部署在结果方，将输出因子转化为最终计算结果。每个结果方拥有自己独立的数据输出组件。当一个实体同时承担结果方与数据方时，可同时具有输入组件和数据输出组件。

计算引擎由多个计算节点组成，每个计算节点分别部署在不同的计算方上，协同完成MPC计算协议。

当一个实体同时承担多个参与方角色时，相应的技术组件可进行合并。

参 考 文 献

[1] GB/T 27928.1 金融业务 证书管理 第1部分：公钥证书
[2] JR/T 0118 金融电子认证规范
[3] JR/T 0171—2020 个人金融信息保护技术规范