ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0135—2024

多方安全计算　技术框架

Secure multi-party computation—Technical framework

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：中国科学技术大学、清华大学、华控清交信息科技（北京）有限公司、中国信息通信研究院、中电科网络安全科技股份有限公司、中移动信息技术有限公司、山东大学、兴唐通信科技有限公司、蚂蚁科技集团股份有限公司、中国电力科学研究院有限公司、三未信安科技股份有限公司、北京海泰方圆科技股份有限公司、北京数字认证股份有限公司、北京炼石网络技术有限公司、联想（北京）有限公司、复旦大学、中安网脉（北京）技术股份有限公司、中国石油昆仑数智科技有限责任公司、北京原语科技有限公司、中国科学院信息工程研究所、深圳市全同态科技有限公司、精华教育科技股份有限公司、浙江智贝信息科技有限公司、武汉大学。

本文件的主要起草人：林璟锵、徐葳、李智虎、高志权、王伟、王云河、郭娟娟、李艺、黄熹之、王琼霄、茹志强、赵原、昌文婷、孔凡玉、张立廷、靳晨、王现方、白小勇、韩伟力、梁心茹、杨国强、张嵩、王学进、何德彪、白玉真、林齐平、袁博、王云浩、周伟、刘仁章、马逸龙、曹耀和、李雪岩、黄保华、郭陶。

引　言

数据作为新型生产要素，是数字化、网络化、智能化的基础，已融入生产、分配、流通、消费和社会服务管理等各环节，深刻改变着生产方式、生活方式和社会治理方式。多方安全计算，作为一种典型的密码技术，能够保证各参与方在不泄露原始输入的前提下，协同计算预期函数并得到最终结果。在多方安全计算协议执行过程中，原始输入数据经密码技术处理后得到计算因子，并进一步计算处理得到正确的最终结果，多方安全计算协议对计算因子的处理不会泄露多于最终结果的、有关原始输入的信息。计算因子处理过程满足“原始数据不出域、数据可用不可见”的要求；因此，多方安全计算将在数据流通体系中发挥重要的基础性作用，形成有效的数据流通安全保障技术，在避免原始数据流转的情况下，促进数据使用价值复用与充分利用、促进数据使用权交换和市场化流通。

本文件阐述了多方安全计算的协议框架和系统组成、协议安全要求和应用技术体系框架等。本文件凡涉及密码算法相关内容，按国家有关法规实施。

SMPC 协议由数据提供者、计算提供者和结果获取者等角色协同执行。数据提供者对原始输入进行处理得到输入因子，并发送给计算提供者。计算提供者利用输入因子进行计算、得到输出因子；或者计算提供者对输入因子进行处理、得到中间因子，然后在若干次中间因子处理之后再进一步计算获得输出因子。结果获取者从计算提供者获取输出因子，对其计算得到最终结果。输入因子、中间因子和输出因子统称为计算因子。某些 SMPC 协议还要求有受信辅助者为计算提供者、结果获取者等生成执行 SMPC 协议所必需的计算参数。

除了上述角色，在 SMPC 系统中，还包括可选的配置器和调度器：在 SMPC 协议执行之前，对 SMPC 系统的预期函数、实现预期函数的 SMPC 协议和执行 SMPC 协议的各角色进行配置和调度。

在给定的角色组成和敌手模型下，SMPC 协议以某一种安全程度（半诚实安全或恶意安全）满足基本属性（计算正确性和数据隐私性），且具备某一种输出属性（安全中止、输出公平或确保结果输出）。

SMPC 应用技术体系框架包括 SMPC 协议层、SMPC 设备层、SMPC 系统层、SMPC 应用支撑层等，各层有机结合组成 SMPC 应用技术体系。SMPC 协议层由通用计算功能 SMPC 协议、特定计算功能 SMPC 协议，以及 SMPC 协议组件和 SMPC 协议转换机制等组成。SMPC 设备层由不同类型、不同形式的 SMPC 设备组成，分别完成 SMPC 协议的一种或多种角色的功能；SMPC 设备可以是软件、固件、硬件或者混合密码模块的形式。SMPC 系统层调用 SMPC 设备层的不同角色功能来实现 SMPC 计算功能，包括利用 SMPC 协议实现的通用计算功能和特定计算功能。SMPC 应用支撑层由多种典型的 SMPC 应用支撑功能组成，为上层业务应用提供支撑。

多方安全计算　技术框架

1　范围

本文件规定了多方安全计算的协议框架和系统组成、协议安全要求和应用技术体系框架等内容。

本文件适用于多方安全计算系统和产品的设计、研制和应用，为密码行业的多方安全计算相关标准提供指导和参考。

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 37092　信息安全技术　密码模块安全要求

3　术语和定义

以下术语和定义适用于本文件。

3.1

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

保证各参与方在不泄露原始输入的前提下，协同计算预期函数并得到最终结果的密码技术。

3.2

预期函数　intended function

SMPC 协议对原始输入进行处理、得到最终结果的计算过程的函数表达。

3.3

参与方　party

参与执行 SMPC 协议计算过程的实体。

3.4

数据提供者　data provider

SMPC 协议的一种角色，持有原始输入，对原始输入进行处理得到输入因子，并将输入因子发送给计算提供者。

3.5

计算提供者　computing provider

SMPC 协议的一种角色，利用输入因子和中间因子进行计算、得到输出因子。

3.6

结果获取者　result obtainer

SMPC 协议的一种角色，从计算提供者获取输出因子、对其计算得到最终结果。

3.7

受信辅助者　trusted assistant

SMPC 协议的一种可选角色，为计算提供者、结果获取者等生成执行 SMPC 计算过程所必需的、与

原始输入无关的计算参数。

3.8

配置器　configurator

SMPC 系统的一种可选功能角色，设定 SMPC 系统的预期函数。

3.9

调度器　coordinator

SMPC 系统的一种可选功能角色，设定 SMPC 系统计算预期函数的 SMPC 协议和设定执行 SMPC 协议的各角色。

3.10

原始输入　original input

数据提供者所拥有的、用于输入 SMPC 计算过程的明文数据。

3.11

最终结果　final result

结果获取者所获得的、SMPC 计算过程输出的结果数据。

3.12

输入因子　input factor

数据提供者对原始输入进行处理后得到的变量；例如，按照秘密分享方案拆分后的份额、按照混淆电路方案生成的标签，或者按照同态加密方案计算得到的密文等。

3.13

中间因子　intermediate factor

计算提供者对输入因子进行计算后得到的中间变量。

3.14

输出因子　output factor

计算提供者对输入因子、中间因子进行计算后得到的变量，用于结果获取者计算获得最终结果。

3.15

计算因子　computation factor

输入因子、中间因子和输出因子的统称；在给定的敌手模型下，敌手不能从计算因子获得有关原始输入或最终结果的信息。

3.16

敌手　adversary

试图阻止 SMPC 协议计算过程达到其应满足的安全要求的实体。

3.17

半诚实敌手　semi-honest adversary

按照 SMPC 协议执行、不会背离协议，但是能对协议执行过程中所获得的信息进行任意处理的敌手，例如根据获得的信息推测其他参与方的输入和计算因子等。

3.18

恶意敌手　malicious adversary

能按照 SMPC 协议执行，也能在协议执行过程中任意地背离协议的敌手，例如不执行协议要求的操作、篡改协议执行过程中的数据、乱序执行协议的某些操作等。

3.19

腐化　corruption

敌手通过各种方式的网络攻击，控制 SMPC 系统的参与方。

4 缩略语

下列缩略语适用于本文件。

GC:混淆电路(Garbled Circuit)

HE:同态加密(Homomorphic Encryption)

OT:不经意传输(Oblivious Transfer)

PIR:隐匿信息检索(Private Information Retrieval)

PSI:隐私集合求交(Private Set Intersection)

SMPC:多方安全计算(Secure Multi-Party Computation)

SS:秘密分享(Secret Sharing)

5 SMPC 协议框架和系统组成

5.1 SMPC 协议框架

SMPC 协议框架如图 1 所示。

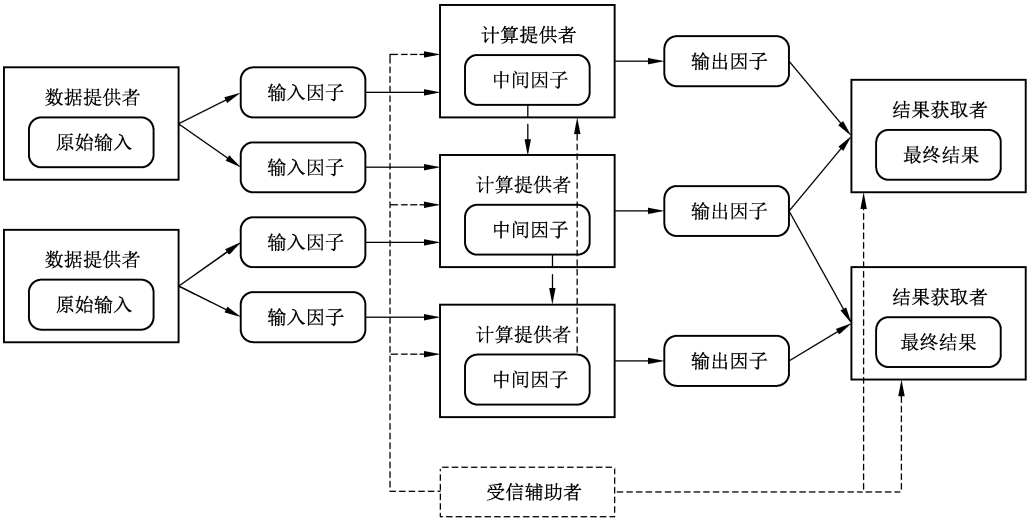

图 1 SMPC 协议框架

在 SMPC 计算过程中,数据提供者、计算提供者和结果获取者按照 SMPC 协议执行,过程如下:

a) 数据提供者持有原始输入,对原始输入进行处理得到输入因子,例如按照秘密分享方案拆分得到多个份额、按照混淆电路方案生成标签,或者按照同态加密方案计算密文,然后将其发送给计算提供者;

b) 计算提供者利用输入因子进行计算,得到输出因子,例如基于秘密分享方案计算原始输入的和的份额;或者,计算提供者先对输入因子进行处理、得到中间因子,然后在若干次中间因子处理之后再进一步计算获得输出因子,例如在基于秘密分享方案计算原始输入的乘积时,有中间因子的多次计算和多次交换;

c) 结果获取者从计算提供者获取输出因子,计算得到最终结果,例如从秘密分享方案的份额合成得到最终结果、利用混淆电路方案的标签解密混淆表得到最终结果;

d) 某些 SMPC 协议还要求有受信辅助者为计算提供者、结果获取者等生成执行 SMPC 协议所必

需的计算参数，例如在某些 SMPC 协议基于秘密分享的份额计算原始输入的乘积时，要求受信辅助者向计算提供者生成满足乘法关系的随机数三元组的秘密分享份额。

数据提供者的数量应大于或等于 2。

受信辅助者不应接收原始输入、输入因子、中间因子和输出因子，受信辅助者生成的计算参数应与原始输入无关。

5.2 SMPC 系统组成

SMPC 系统框架如图 2 所示。

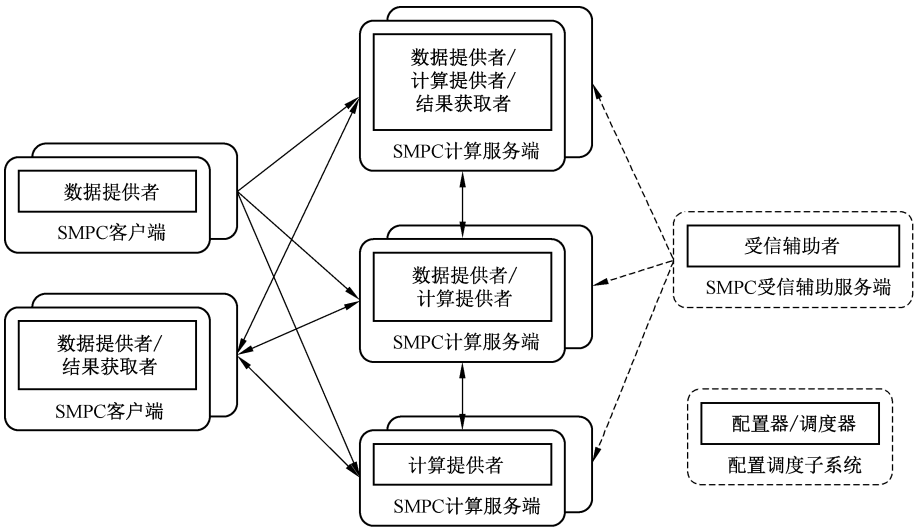

图 2 SMPC 系统框架

在 SMPC 系统中，各参与方按照 SMPC 协议执行，完成 SMPC 计算过程。一个参与方可承担一种或多种角色，但是一个参与方不能同时承担受信辅助者和其他角色。除了数据提供者、计算提供者、结果获取者、受信辅助者等角色，SMPC 系统还包括可选的配置器和调度器。在 SMPC 协议执行之前，配置器和调度器对系统的预期函数、SMPC 协议以及 SMPC 协议的各角色进行配置和调度。

常见的 SMPC 系统典型部署模式见附录 A。对于不同的 SMPC 协议，SMPC 系统可采取不同部署模式，由不同的 SMPC 设备作为参与方、承担相应的角色，说明如下：

a) 在对等模式下，SMPC 系统由若干 SMPC 计算服务端组成，SMPC 计算服务端承担数据提供者与计算提供者、部分或者全部 SMPC 计算服务端承担结果获取者；例如，多个 GC-SMPC 计算服务端协同执行混淆电路 SMPC 机制，或者多个 PSI 计算服务端协同执行隐私集合求交协议；

b) 在客户端-计算服务端模式和混合模式下，SMPC 系统由若干 SMPC 客户端和若干 SMPC 计算服务端组成，SMPC 客户端承担数据提供者、SMPC 计算服务端承担计算提供者、部分或者全部 SMPC 客户端承担结果获取者；例如，SS-SMPC 客户端和 SS-SMPC 计算服务端协同执行基于秘密分享的 SMPC 机制，HE-SMPC 计算服务端和 HE-SMPC 客户端协同执行基于同态加密的 SMPC 机制，或者 PIR 客户端和 PIR 计算服务端协同执行隐匿信息检索协议；

c) 在 a)和 b)所述的部署模式中，SMPC 系统还可包括 SMPC 受信辅助服务端，在某些特定 SMPC 协议中承担受信辅助者；

d) 配置器和调度器由 SMPC 系统的配置调度子系统实现，配置器设定 SMPC 系统的预期函数（例如，设定联合统计、联合建模/预测、隐匿查询、样本对齐等功能相对应的预期函数），调度器

设定计算预期函数的 SMPC 协议(例如,根据预期函数设定某种基于秘密分享或同态加密的通用计算功能 SMPC 协议,或某种特定计算功能 SMPC 协议),并设定执行该 SMPC 协议的数据提供者、计算提供者、结果获取者和受信辅助者等角色。

6 SMPC 协议安全要求

6.1 敌手模型

SMPC 协议应明确描述其敌手模型。敌手模型的描述应至少包括:敌手行为、敌手计算能力与敌手腐化情况。

a) 根据敌手行为,敌手分为半诚实敌手和恶意敌手:
   1) 半诚实敌手按照 SMPC 协议执行、不会背离协议,但是能对协议执行过程中所获得的信息进行任意处理,例如根据获得的信息推测其他参与方的输入和计算因子等;
   2) 恶意敌手能按照 SMPC 协议执行,也能在协议执行过程中任意地背离协议,例如不执行协议要求的操作、篡改协议执行过程中的数据、乱序执行协议的某些操作等。
b) 根据敌手具有的计算能力,可将敌手分为如下两类:
   1) 具有多项式时间计算能力的敌手,
   2) 具有无限计算能力的敌手。
c) 敌手腐化情况可采取如下的某一种方式来描述:
   1) 被敌手腐化的参与方的最大数量,
   2) 被敌手腐化的参与方数量占参与方总数量的最大比例,
   3) 列举所有可能的、被敌手腐化的参与方组合。

在 SMPC 协议中,未被敌手腐化的参与方是诚实参与方;被半诚实敌手腐化的参与方称为半诚实参与方,执行与半诚实敌手相同的行为;被恶意敌手腐化的参与方称为恶意参与方,执行与恶意敌手相同的行为。

被敌手腐化的多个参与方能相互合谋合作,例如共享信息、合作采取操作等。

6.2 安全属性

6.2.1 基本属性

SMPC 协议的基本属性包括计算正确性和数据隐私性。

a) 计算正确性:
   结果获取者获得的最终结果应与将数据提供者持有的原始输入按照预期函数进行计算得到的结果一致。SMPC 协议执行的最终结果与原始输入按照预期函数计算结果一致,是在指定的计算精度范围内二者的值相等。
b) 数据隐私性:
   参与方在执行 SMPC 计算过程中不能获得多于最终结果的、有关原始输入的任何信息。在给定的角色组成和敌手模型下,SMPC 协议的一个参与方即使承担一种或多种角色、获得每种角色的相应信息,也不能从计算因子中获得其他数据提供者的原始输入信息,敌手也不能利用被腐化的参与方从输入因子、中间因子或输出因子获得诚实数据提供者的原始输入信息。

6.2.2 输出属性

SMPC 协议的输出属性可以是安全中止、输出公平或确保结果输出。

a) 安全中止：
当存在恶意的数据提供者或计算提供者时，诚实的计算提供者或结果获取者应发现背离协议的恶意行为并输出中止。

b) 输出公平：
仅当诚实的结果获取者获得最终结果时，恶意的结果获取者才能获得最终结果。

c) 确保结果输出：
保证诚实的结果获取者能够获得最终结果。

6.3 安全要求

在给定的角色组成和敌手模型下，SMPC 协议应以如下某一种安全程度（半诚实安全或恶意安全）满足基本属性（计算正确性和数据隐私性），且应具备某一种输出属性（安全中止、输出公平或确保结果输出）。

a) 半诚实安全：
在仅存在半诚实敌手的情况下，SMPC 协议满足基本属性和所声称的输出属性，输出属性是确保结果输出。

b) 恶意安全：
在存在恶意敌手的情况下，SMPC 协议满足基本属性和所声称的输出属性，输出属性可以是安全中止、输出公平或确保结果输出的某一种。

根据能够抵御的敌手计算能力，SMPC 协议的安全程度还可进一步分为计算安全或信息论安全。计算安全的 SMPC 协议能够抵御具有多项式时间计算能力的敌手，敌手可以是半诚实或恶意敌手；信息论安全的 SMPC 协议能够抵御具有无限计算能力的敌手，敌手可以是半诚实或恶意敌手。

7 SMPC 应用技术体系框架

7.1 概述

SMPC 应用技术体系框架包括 SMPC 协议层、SMPC 设备层、SMPC 系统层、SMPC 应用支撑层等，各层有机结合组成 SMPC 应用技术体系，如图 3 所示。

SMPC 协议层规范了不同的 SMPC 协议机制。每一种 SMPC 设备实现了 SMPC 协议的部分或全部功能，承担 SMPC 协议的一种或多种角色，SMPC 系统层调用 SMPC 设备的功能、完成 SMPC 计算功能。SMPC 应用支撑层为业务应用提供典型的 SMPC 应用支撑，从而简化业务应用的调用过程，业务应用可以调用 SMPC 应用支撑层的功能，也可以直接调用 SMPC 系统层的 SMPC 计算功能。

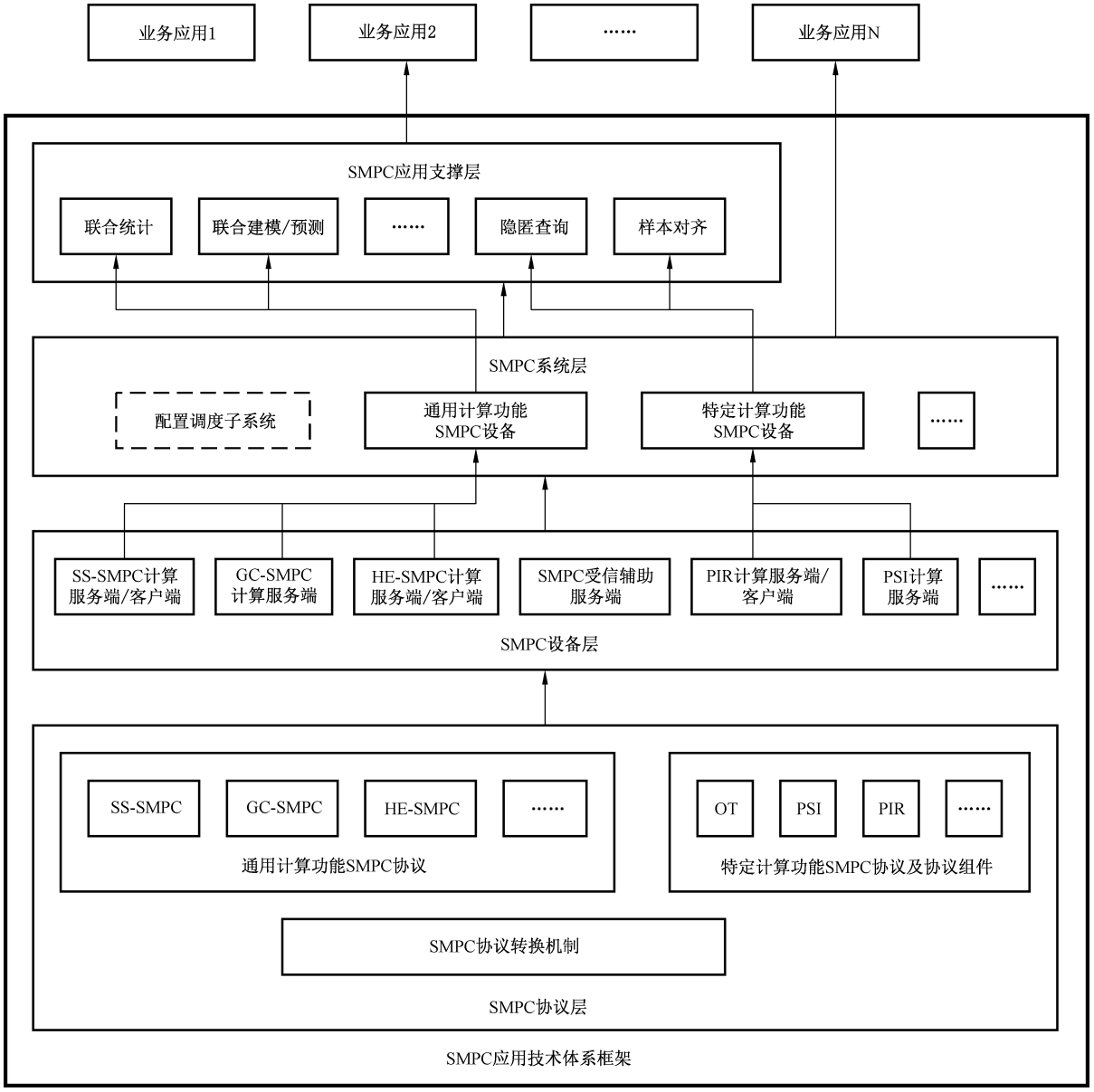

图 3　SMPC 应用技术体系框架

7.2　SMPC 协议层

SMPC 协议层由通用计算功能 SMPC 协议、特定计算功能 SMPC 协议、SMPC 协议组件以及 SMPC 协议转换机制等组成，包括如下：

a）　通用计算功能 SMPC 协议支持灵活定义的预期函数（例如，乘法、加法、布尔运算及其组合等），包括基于秘密分享的 SMPC 机制（SS-SMPC）、混淆电路 SMPC 机制（GC-SMPC）、基于同态加密的 SMPC 机制（HE-SMPC）等；

b）　特定计算功能 SMPC 协议只能支持固定类型的预期函数，包括隐私集合求交（PSI）协议、隐匿信息检索（PIR）协议，以及不经意传输（OT）协议等，其中 OT 协议作为特定计算功能 SMPC 协议，也可作为其他 SMPC 协议的组件；

c）　SMPC 协议转换机制将一种 SMPC 协议的计算因子转换成另一种 SMPC 协议的计算因子，例如 SS-SMPC 计算因子与 GC-SMPC 计算因子之间的转换，在计算因子的转换过程中，也应满足基本属性和输出属性的要求。

7.3 SMPC 设备层

SMPC 设备层由不同类型的 SMPC 设备组成，分别完成 SMPC 协议的一种或多种角色的 SMPC 协议功能。SMPC 设备应满足 GB/T 37092 规范的密码模块安全要求，可以是软件、固件、硬件或者混合模块的形式。常见的 SMPC 设备包括：SS-SMPC 客户端、SS-SMPC 计算服务端、GC-SMPC 计算服务端、SMPC 受信辅助服务端、PIR 客户端、PIR 计算服务端、PSI 计算服务端等。

a) SS-SMPC 客户端和 SS-SMPC 计算服务端，协同执行基于秘密分享的 SMPC 机制
SS-SMPC 客户端实现数据提供者和结果获取者的功能，处理原始输入、得到输入因子，获取输出因子、计算得到最终结果；SS-SMPC 计算服务端实现计算提供者的功能，多个 SS-SMPC 计算服务端协同处理输入因子和中间因子，直至最后得到输出因子。

b) 多个 GC-SMPC 计算服务端，协同执行混淆电路 SMPC 机制
GC-SMPC 计算服务端同时实现了数据提供者、计算提供者和结果获取者的功能；2 个 GC-SMPC 计算服务端协同处理原始输入、分别执行混淆电路机制的混淆器和评估器功能。

c) HE-SMPC 计算服务端和 HE-SMPC 客户端，协同执行基于同态加密的 SMPC 机制
HE-SMPC 计算服务端完成同态密文处理的计算功能，实现计算提供者的功能，HE-SMPC 客户端完成同态密码算法的加密操作和解密操作，实现数据提供者和结果获取者的功能。

d) SMPC 受信辅助服务端
作为某些特定 SMPC 协议的受信辅助者，配合其他 SMPC 设备协同执行 SMPC 计算功能。

e) PIR 客户端和 PIR 计算服务端，协同执行隐匿信息检索协议
PIR 客户端实现了数据提供者、计算提供者和结果获取者的功能，PIR 计算服务端实现了数据提供者和计算提供者的功能。

f) 多个 PSI 计算服务端，协同执行隐私集合求交协议
PSI 计算服务端同时实现了数据提供者、计算提供者和结果获取者的功能。

7.4 SMPC 系统层

SMPC 系统层调用 SMPC 设备层的不同角色功能来实现 SMPC 计算功能，包括利用 SMPC 协议实现的通用计算功能和特定计算功能，构建 SMPC 系统。SMPC 系统层通常还需要实现配置调度、身份鉴别与权限管理、数据授权管理、通信安全、存储安全、日志等功能。

a) 可选的配置器和调度器由 SMPC 系统的配置调度子系统实现，通常由 SMPC 系统的操作员发起执行配置调度功能，可静态或者动态地设定预期函数和 SMPC 协议。

b) 对于预期函数可配置的 SMPC 系统（例如，实现 SS-SMPC、GC-SMPC 或者 HE-SMPC 机制的通用计算功能 SMPC 系统），应先通过配置器、根据上层功能的要求来设定 SMPC 系统的预期函数。

c) 对于 SMPC 协议可调度的 SMPC 系统（例如，实现了多种 SS-SMPC 协议的 SMPC 系统，或实现了多种 PSI 协议的 SMPC 系统），应先通过调度器、根据上层功能的要求来设定 SMPC 系统所执行的 SMPC 协议。

SMPC 系统层通过 SMPC 服务接口为应用支撑层和业务应用提供与 SMPC 设备无关的、与 SMPC 协议无关的 SMPC 服务，将上层的应用支撑层和业务应用的计算请求转化为具体的 SMPC 协议操作请求。

7.5 SMPC 应用支撑层

SMPC 应用支撑是指利用 SMPC 计算功能完成的、处理用户数据的典型共性应用功能。SMPC 应用支撑层目前主要由联合统计、联合建模/预测、隐匿查询、样本对齐等组成，并将在将来的 SMPC 技术

应用过程中继续丰富。SMPC 应用支撑层通过调用 SMPC 服务接口访问 SMPC 系统来实现 SMPC 应用支撑功能。

a) 联合统计

完成多方数据的统计计算(例如总和、方差、极值等),除了输出的统计计算结果,不泄露输入数据的任何信息。持有输入数据的各方作为数据提供者,并根据所使用的不同 SMPC 机制、运行不同的 SMPC 设备:可以是 SS-SMPC 客户端、GC-SMPC 计算服务端或 HE-SMPC 客户端等。根据所使用的不同 SMPC 机制,结果获取者运行 SS-SMPC 客户端、GC-SMPC 计算服务端或 HE-SMPC 客户端等,获得联合统计的计算结果。如果使用 SS-SMPC 机制和 HE-SMPC 机制,还分别有 SS-SMPC 计算服务端和 HE-SMPC 计算服务端等,用于协同完成联合统计计算功能。

b) 联合建模

完成基于多方数据的模型训练(例如逻辑回归、梯度提升决策树等),除了输出的模型参数,不泄露输入数据的任何信息。持有用于模型训练的输入数据的各方作为数据提供者,并根据所使用的不同 SMPC 机制、运行不同的 SMPC 设备:可以是 SS-SMPC 客户端、GC-SMPC 计算服务端或 HE-SMPC 客户端等。根据所使用的不同 SMPC 机制,结果获取者运行 SS-SMPC 客户端、GC-SMPC 计算服务端或 HE-SMPC 客户端等,获得模型参数结果。如果使用 SS-SMPC 机制和 HE-SMPC 机制,还分别有 SS-SMPC 计算服务端和 HE-SMPC 计算服务端等,用于协同完成联合建模计算功能。

c) 联合预测

完成基于模型的预测计算并保护各方的数据隐私性,除了输出的预测结果,不泄露输入数据和模型参数的任何信息。持有预测模型和输入数据的各方均作为数据提供者,并根据所使用的不同 SMPC 机制、运行不同的 SMPC 设备:可以是 SS-SMPC 客户端、GC-SMPC 计算服务端或 HE-SMPC 客户端等。根据所使用的不同 SMPC 机制,结果获取者运行 SS-SMPC 客户端、GC-SMPC 计算服务端或 HE-SMPC 客户端等,获得联合预测结果。如果使用 SS-SMPC 机制和 HE-SMPC 机制,还分别有 SS-SMPC 计算服务端和 HE-SMPC 计算服务端等,用于协同完成联合预测计算功能。

d) 隐匿查询

查询方设定查询条件、完成查询操作,查询方不能获得除查询结果以外的任何信息,查询服务方不能获得查询条件参数的任何信息。查询方运行 PIR 客户端设备、获得查询结果,查询服务方运行 PIR 计算服务端、提供隐匿查询服务。

e) 样本对齐

完成多方样本数据集合的交集计算,除了输出的样本交集元素,不泄露各方样本数据集合的任何信息。各参与方持分别运行各自的 PSI 计算服务端设备,多个 PSI 计算服务端协同完成样本对齐计算功能。

附 录 A
（资料性）
SMPC 系统部署模式

A.1 对等模式

在对等模式下，如图 A.1 和图 A.2 所示，SMPC 系统包括多个对等的 SMPC 计算服务端节点，按照如下方式承担 SMPC 协议的角色、执行 SMPC 协议。

a） SMPC 计算服务端同时承担数据提供者与计算提供者。SMPC 节点将原始输入处理为输入因子并发送给其他 SMPC 节点，所有 SMPC 节点基于输入因子及计算过程中交换的中间因子进行计算，得到输出因子，并将输出因子发送给结果获取者。

b） 结果获取者（图中省略表示）可以是部分或者全部的 SMPC 计算服务端。例如，2 个参与方执行 GC-SMPC 协议，双方都同时是数据提供者与计算提供者，可以是单方获得结果，也可以是双方都获得结果；或者，多个参与方分别持有原始输入，各自将原始输入按照秘密分享方案拆分后的份额分别发送至各参与方，然后按照 SS-SMPC 协议执行，各参与方计算得到输出因子，从其他参与方获取足够输出因子后、计算最终结果；或者，多个参与方执行 PSI 协议，各参与方都同时持有各自的元素集合，协议执行之后部分参与方或全部参与方得到交集元素结果。

c） 在对等模式下，SMPC 系统各节点的通信方式如下：

1） SMPC 计算服务端节点可以是网状组网，如图 A.1 所示，例如，各参与方之间相互直接通信、协同执行 SMPC 协议；

2） SMPC 计算服务端节点可以是星状组网，如图 A.2 所示，例如，服务器分别和多个移动设备通信、协同执行 SMPC 协议；

3） 可选的 SMPC 受信辅助服务端与其他参与方可存在通信（图中省略表示）。

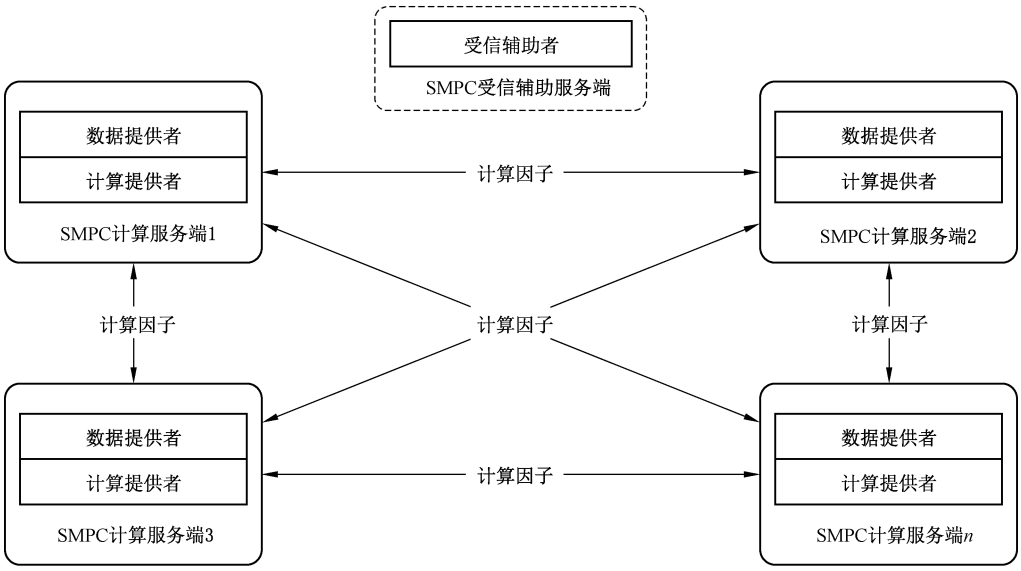

图 A.1 对等模式——网状组网方式

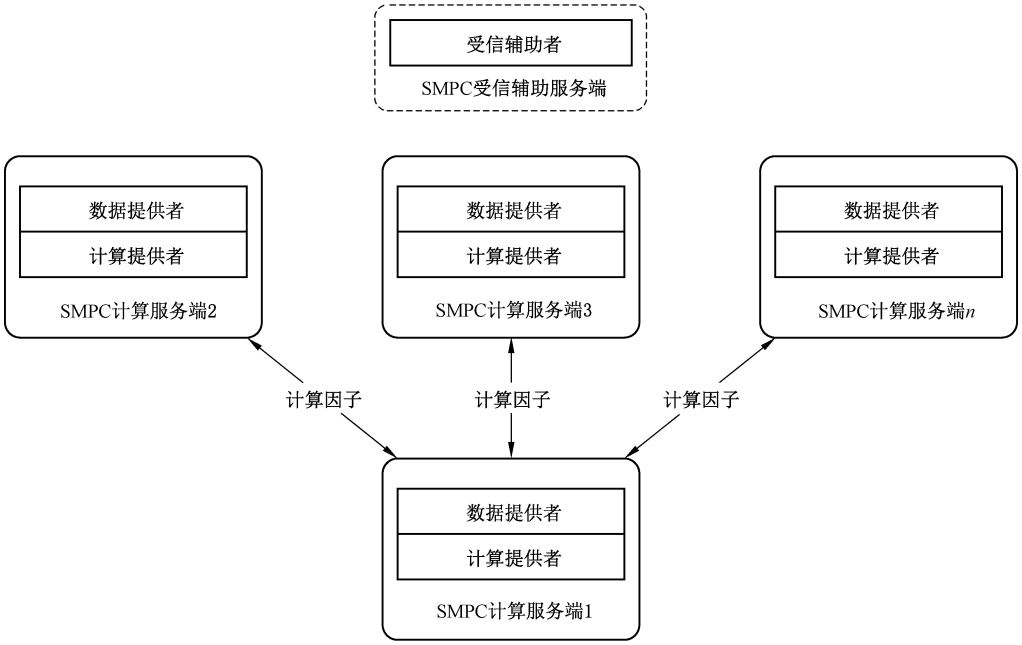

图 A.2　对等模式——星状组网方式

A.2　客户端-计算服务端模式

在客户端-计算服务端模式下，如图 A.3 和图 A.4 所示，SMPC 系统包括 SMPC 客户端和 SMPC 计算服务端，按照如下方式承担 SMPC 协议的角色、执行 SMPC 协议。

a）　SMPC 客户端承担数据提供者，SMPC 计算服务端承担计算提供者。SMPC 客户端将原始输入处理为输入因子并发送给 SMPC 计算服务端，多个 SMPC 计算服务端基于输入因子及中间因子进行计算，得到输出因子，并将其发送给结果获取者（图中省略表示）。例如，多个 SMPC 计算服务端按照 SS-SMPC 协议协同处理输入因子、直至得到输出因子。

b）　结果获取者可以是部分或者全部 SMPC 客户端。

c）　在客户端-计算服务端模式下，SMPC 系统各节点的通信方式如下：

1）　所有 SMPC 计算服务端可直接从 SMPC 客户端获得输入因子，如图 A.3 所示；

2）　或者，部分 SMPC 计算服务端直接从 SMPC 客户端获得输入因子，其他 SMPC 计算服务端从已获得输入因子的 SMPC 计算服务端获得对输入因子计算处理后得到的中间因子，如图 A.4 所示；

3）　可选的 SMPC 受信辅助服务端与 SMPC 计算服务端可存在通信（图中省略表示）。

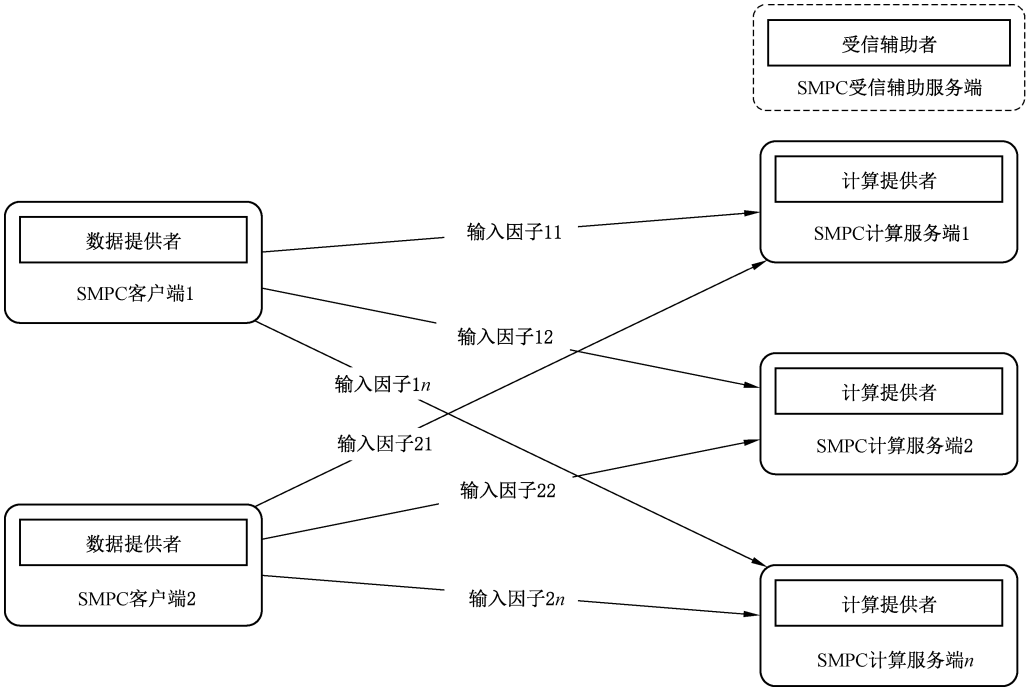

图 A.3　客户端-计算服务端模式：所有计算提供者与数据提供者通信

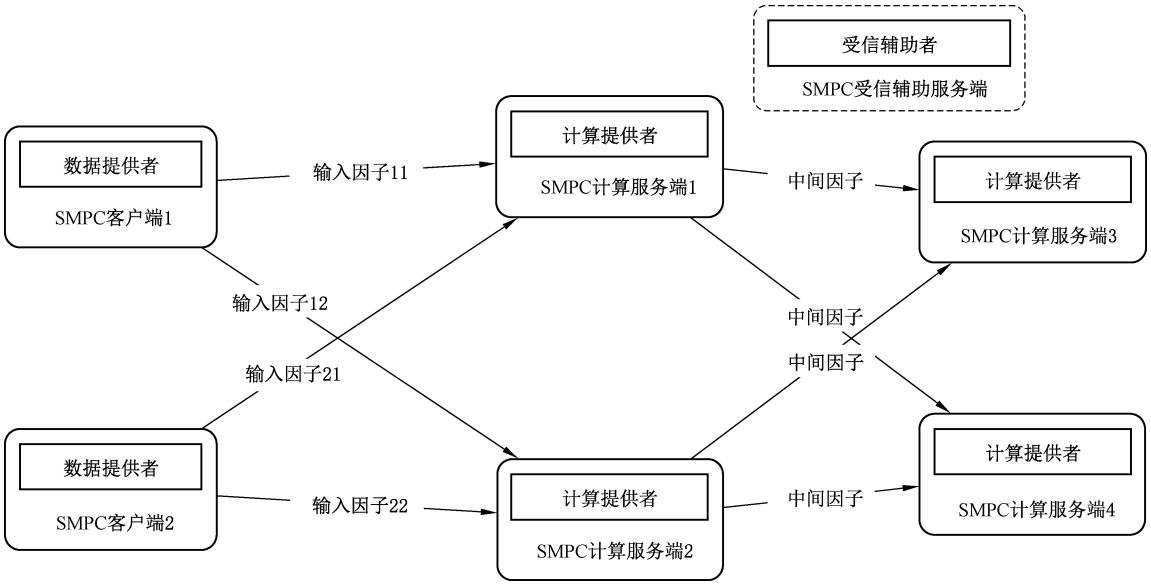

图 A.4　客户端-计算服务端模式：部分计算提供者与数据提供者通信

A.3　混合模式

在混合模式下，如图 A.5 所示，SMPC 系统包括 SMPC 客户端和 SMPC 计算服务端，按照如下方式承担 SMPC 协议的角色，执行 SMPC 协议。

a）　SMPC 客户端承担数据提供者，SMPC 计算服务端同时承担计算提供者和数据提供者。

b）　SMPC 客户端将部分原始输入处理为输入因子并发送给 SMPC 计算服务端，SMPC 计算服务端将部分原始输入处理为输入因子并发送给其他 SMPC 计算服务端。然后，SMPC 计算服务端基于来自于全部数据提供者（包括 SMPC 客户端和 SMPC 计算服务端）的输入因子进行计

算处理，最终获得输出因子，并将其发送给结果获取者（图中省略）。例如，数据提供者 1 和 2 将作为 SMPC 客户端按照 SS-SMPC 协议将输入因子发送给多个 SMPC 计算服务端（作为计算提供者），然后 SMPC 计算服务端（同时作为计算提供者和数据提供者）之间又按照 GC-SMPC 协议处理其中部分数据。

c） 可选的 SMPC 受信辅助服务端与 SMPC 计算服务端可存在通信（图中省略表示）。

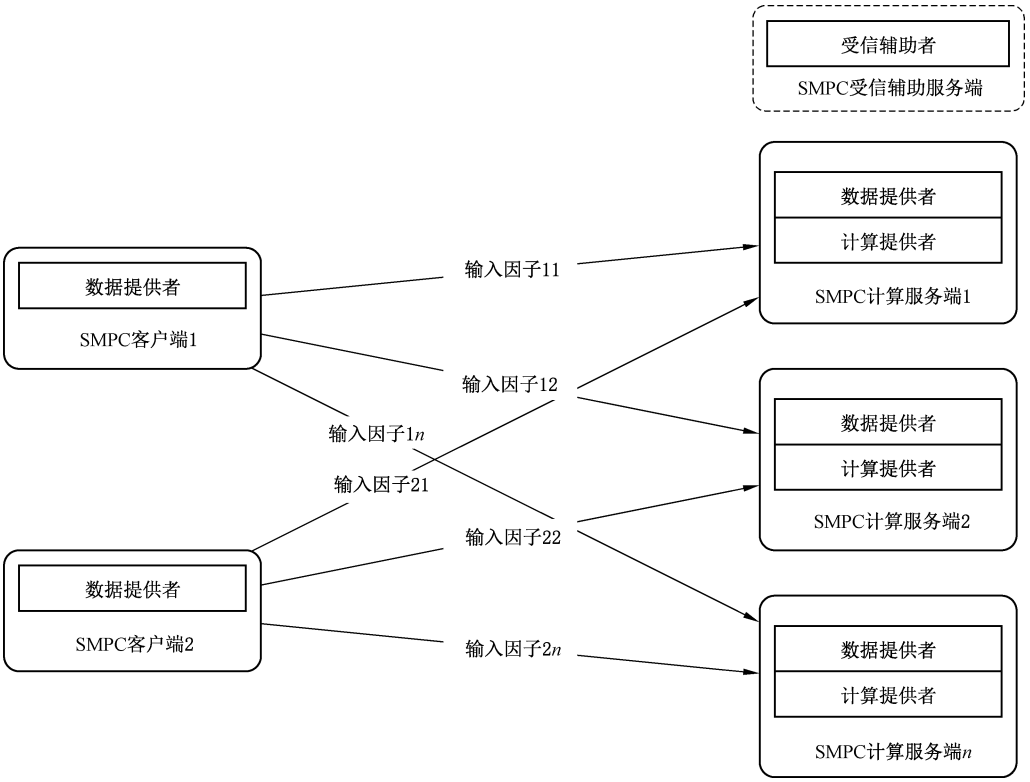

图 A.5　混合模式

参 考 文 献

[1] ISO/IEC 4922-1:2023 Information security—Secure multiparty computation—Part 1:General

[2] A.Yao.Protocols for Secure Computations.23rd Annual Symposium on Foundations of Computer Science (FOCS),1982.

[3] A.Yao.How to Generate and Exchange Secrets.27th Annual Symposium on Foundations of Computer Science (FOCS),1986.

[4] D.Beaver.Efficient Multiparty Protocols Using Circuit Randomization.11th Annual International Cryptology Conference (CRYPTO),1991.

[5] I.Damgard, V.Pastro, N.Smart, and S.Zakarias.Multiparty Computation from Somewhat Homomorphic Encryption.32nd Annual International Cryptology Conference (CRYPTO),2012.

[6] P.Bogetoft,D.Christensen,I.Damgard,et al..Secure Multiparty Computation Goes Live.13th International Conference on Financial Cryptography and Data Security (FC),2009.

[7] P.Mohassel, P.Rindal.ABY3: A Mixed Protocol Framework for Machine Learning.25th ACM Conference on Computer and Communications Security (CCS),2018.

中华人民共和国密码
行业标准
多方安全计算　技术框架
GM/T 0135—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.5　字数 31 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39083　定价 43.00 元

GM/T 0135-2024