ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 机密计算通用框架

Information security techniques-General framework for confidential computing

（征求意见稿）

（本稿完成日期：2023-4-26）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：华为技术有限公司、中国电子技术标准化研究院、中国移动通信集团有限公司、北京百度网迅科技有限公司、蚂蚁科技集团股份有限公司、北京冲量在线科技有限公司、北京数字认证股份有限公司、杭州安恒信息技术股份有限公司、腾讯云计算（北京）有限责任公司、阿里云计算有限公司、飞腾信息技术有限公司、中国科学院信息工程研究所、中国科学院软件研究所、中国联合网络通信集团有限公司、郑州信大捷安信息技术股份有限公司、长扬科技（北京）股份有限公司、上海交通大学、南湖实验室、浙江大华技术股份有限公司、中国民生银行、上海富数科技有限公司、北京国家金融科技认证中心有限公司、北京天融信网络安全技术有限公司、浪潮电子信息产业股份有限公司、北京信安世纪科技股份有限公司、新华三技术有限公司、北京火山引擎科技有限公司、北京数牍科技有限公司、电子科技大学、武汉大学、西安电子科技大学、中国信息通信研究院、陕西省信息化工程研究院、阿里巴巴（北京）软件服务有限公司、深信服科技股份有限公司、国网区块链科技（北京）有限公司、国网智能电网研究院有限公司、北京海泰方圆科技股份有限公司、北京神州绿盟科技有限公司、深圳市洞见智慧科技有限公司、华控清交信息科技（北京）有限公司、国网新疆电力科学研究、山东浪潮科学研究院有限公司、超威半导体产品（中国）有限公司、英特尔股份有限公司、曙光网络科技有限公司、联想（北京）有限公司、奇安信科技集团股份有限公司、北京银联金卡科技有限公司、中国软件测评中心、国家工业信息安全发展研究中心、深圳大学、山石网科通信技术股份有限公司等。

本文件主要起草人：葛小宇、王惠莅、邱勤、庞婷、江为强、于乐、杨朋霖、张东举、苏丹、肖俊贤、张晓蒙、周吉文、郭建领、陈浩栋、宋雨筱、李向锋、王吾冰、张振永、曲金宝、李克鹏、王新宇、郝世荣、谭琳、孙一品、王蕊、荆丽桦、张立武、张严、傅瑜、王莹、刘为华、梁松涛、赵华、张亚京、夏虞斌、杜东、张磊、严志超、张剑青、虞刚、牛博强、杨天雅、卞阳、李振、黄江、王龑、徐峥、麻付强、张宇、万晓兰、张尧、刘敬彬、裴超、张小松、牛伟纳、王鹃、严飞、陈晶、裴庆祺、赵搏文、孔松、张勇、赵晓荣、李世奇、鲍旭华、马红丽、王栋、杨珂、石聪聪、于鹏飞、王学进、王真、刘文懋、王湾湾、马博文、王云河、靳晨、邹振婉、李锐、罗清彩、张大江、王立刚、刘立、梅颖、黄建东、安锦程、郑峥、王天昊、郭永振、王冲华、余果、刘伟丽、何伊圣等。

引　言

机密计算是一种在受信任的硬件基础上，结合固件和软件构建密态、隔离、可验证的计算环境，保证环境内数据机密性、完整性，代码完整性以及运算过程机密性的计算模式，在某些场景下，也可以保护代码的机密性。机密计算通过隔离机制，将通用计算环境与机密计算环境隔离开来，非授权的实体不能访问机密计算环境；通过证明机制对机密计算环境及运行在其中的应用程序进行验证，保证应用程序的完整性；通过加密机制保证运行态的数据在机密计算环境外处于密文状态，防止特权软件甚至硬件的窥探。机密计算具有兼顾安全性、通用性和高效性的优势，不仅可以支持普通的计算和应用，而且计算性能基本和明文计算持平。它可以单独用于保护使用状态中的数据，也可以与其他密码学技术结合在一起来保护数据，尤其对于机器学习、联邦学习、区块链等涉及大数据、高性能的计算场景，是重要的数据保护技术手段，可以有效缓解数据在使用过程中面临的安全保护难题。

近几年，机密计算技术正经历快速发展的过程，目前和机密计算相关的产品、服务和解决方案众多，技术路线多样化，实现的原理和接口差异较大，能力也参差不齐，但国内外关于机密计算领域的标准仍属空白，缺乏统一的标准来规范机密计算的定义、技术架构等，不利于机密计算的技术发展和产业应用。因此，亟需通过科学、合理地开展机密计算标准化工作，统一机密计算的认识，规范和指导机密计算相关产品的设计、开发、部署和使用，以促进异构计算平台之间的互联互通，这对于机密计算产业生态的健康发展。

本文件主要目标是提出一种通用的机密计算框架，给出机密计算框架组成结构、具备的基础功能、由组件之间交互形成的安全服务以及面向应用程序所提供的安全服务接口类型，提高机密计算框架的易用性和安全性，为机密计算的技术发展和产业应用提供指导。

信息安全技术 机密计算通用框架

1 范围

本文件给出了机密计算通用框架，包括框架的核心组件、基础功能、安全服务以及服务接口类型。

本文件适用于指导机密计算相关产品、服务或解决方案的设计、研发、部署和使用，也适用于指导网络运营者对机密计算技术的应用，第三方测评机构也可参照使用。

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 25069—2022 信息安全技术 术语

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

组件 component

在系统中，实现其部分功能的可识别区分的部分。

[来源：GB/T 25069—2022，3.815]

3.2

安全服务 security service

根据安全策略，为用户提供某种安全功能及相关保障的服务。

[来源：GB/T 25069—2022，3.7，有修改]

3.3

安全信道 secure channel

为所交换消息提供机密性及真实性的通信信道。

[来源：GB/T 25069—2022，3.32，有修改]

3.4

机密性 confidentiality

采用密码技术保证信息不泄露的性质。

[来源：GB/T 25069—2022，3.259]

3.5

真实性 authenticity

一个实体是其所声称实体的性质。

[来源：GB/T 25069—2022，3.769]

3.6

完整性 integrity

准确和完备的的性质。

[来源：GB/T 25069—2022，3.612]

3.7

盐值 salt

作为辅助输入并入单向或加密函数，用于导出口令验证数据的随机变量。

[来源：GB/T 25069—2022，3.597]

3.8

机密计算 confidential computing

在受信任的硬件基础上，通过构建密态、隔离、可证明的计算环境，保护数据和代码的机密性、完整性以及计算过程机密性的计算模式。

注：计算过程是指程序运行过程，在该过程中会产生进程程序段、数据段、进程控制块以及进程通信涉及的所有数据。

3.9

机密计算平台 confidential computing platform

提供机密计算基础设施及配套软件的集合。

3.10

机密计算环境 confidential computing environment

在机密计算平台之上部署的软件及相关组件的集合。

3.11

机密计算服务 confidential computing service

通过已定义的接口提供一种或多种机密计算能力的服务。

3.12

机密计算应用程序 confidential computing application program

部署和运行在机密计算环境中的应用程序。

3.13

普通计算环境 general computing environment

不具备机密计算能力，仅提供基础功能和计算资源的软件及相关组件的集合。

注：普通计算环境是相对机密计算环境独立存在的运行环境。

4 缩略语

下列缩略语适用于本文件。

API：应用编程接口（application programming interface）

CPU：中央处理单元（central processing unit）

DMA：直接存储器访问（direct memory access）

VM：虚拟机（virtual machine）

5 参与角色

在机密计算的业务执行流程中，主要有五类角色：算法提供方、机密计算服务提供方、机密计算平台提供方、数据提供方和计算结果需求方，如图1所示。每个角色可以由一个或多个实体（个人或机构）担任，针对不同的机密计算服务和部署模式，上述角色中的某几个角色也可以由同一实体担任。

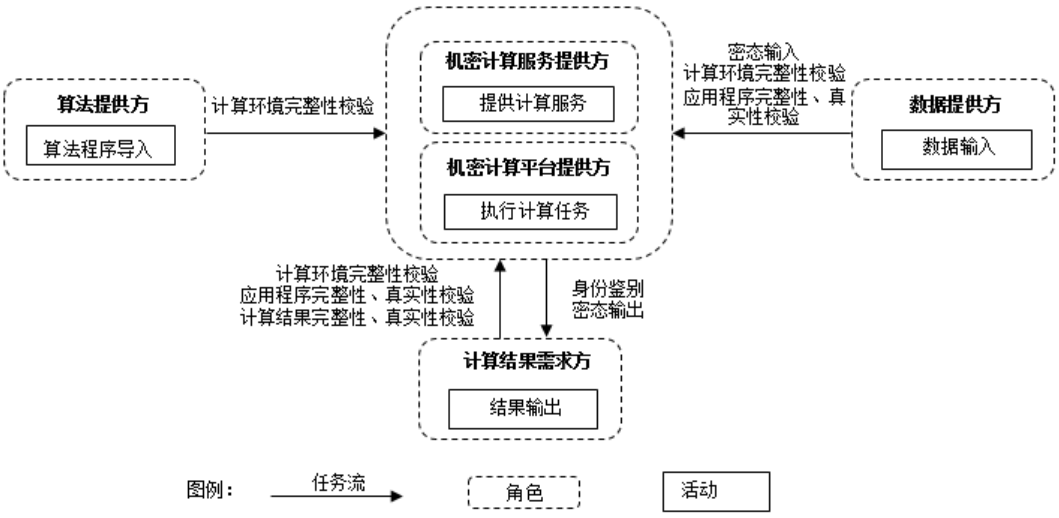


图1 机密计算业务执行流程图

各类角色描述如下：

a) 算法提供方：负责提供需要在机密计算环境中运行的算法程序，算法程序与计算结果需求方的需求描述相符；

b) 机密计算服务提供方：负责为计算结果需求方提供机密计算服务，服务提供方也提供服务的管理功能，如支持算法程序的录入与发布；

c) 机密计算平台提供方：负责提供机密计算环境所依赖的可信软硬件以及机密计算服务提供方所使用的接口，包括集成在机密计算平台内部的信任根、可信执行环境等，建立实现完整的度量存储报告机制，将信任链扩展到应用程序；

d) 数据提供方：负责提供计算任务所使用的计算数据，计算数据在传输过程中应保证机密性和完整性；

e) 计算结果需求方：负责提供具体的计算需求给机密计算服务提供方或者直接使用机密计算平台执行计算任务，包括需要运行的程序、程序运行时需要计算的数据等，并获得相应的机密计算结果。

6 框架组成

6.1 框架描述

本文件给出的机密计算通用框架如图2所示，包括硬件层、系统软件层、服务层、应用层和跨层管理模块五个部分。其中，硬件层基于硬件隔离实现受保护的资源不被开放系统访问，并基于硬件安全功能为机密计算提供受信任的硬件基础；系统软件层为机密计算提供基于软件的隔离机制、必要的硬件资源和基础服务；服务层为上层应用程序提供统一的机密计算服务接口及安全服务，安全服务是由底层的系统软件和硬件以及管理模块交互形成，机密计算统一服务接口用以屏蔽底层硬件架构和软件的开发接口差异；应用层是直接面向结果需求方的应用程序，结果需求方通过应用程序执行计算操作；跨层管理为机密计算服务提供方或结果需求方开展机密计算活动提供必要的管理模块。

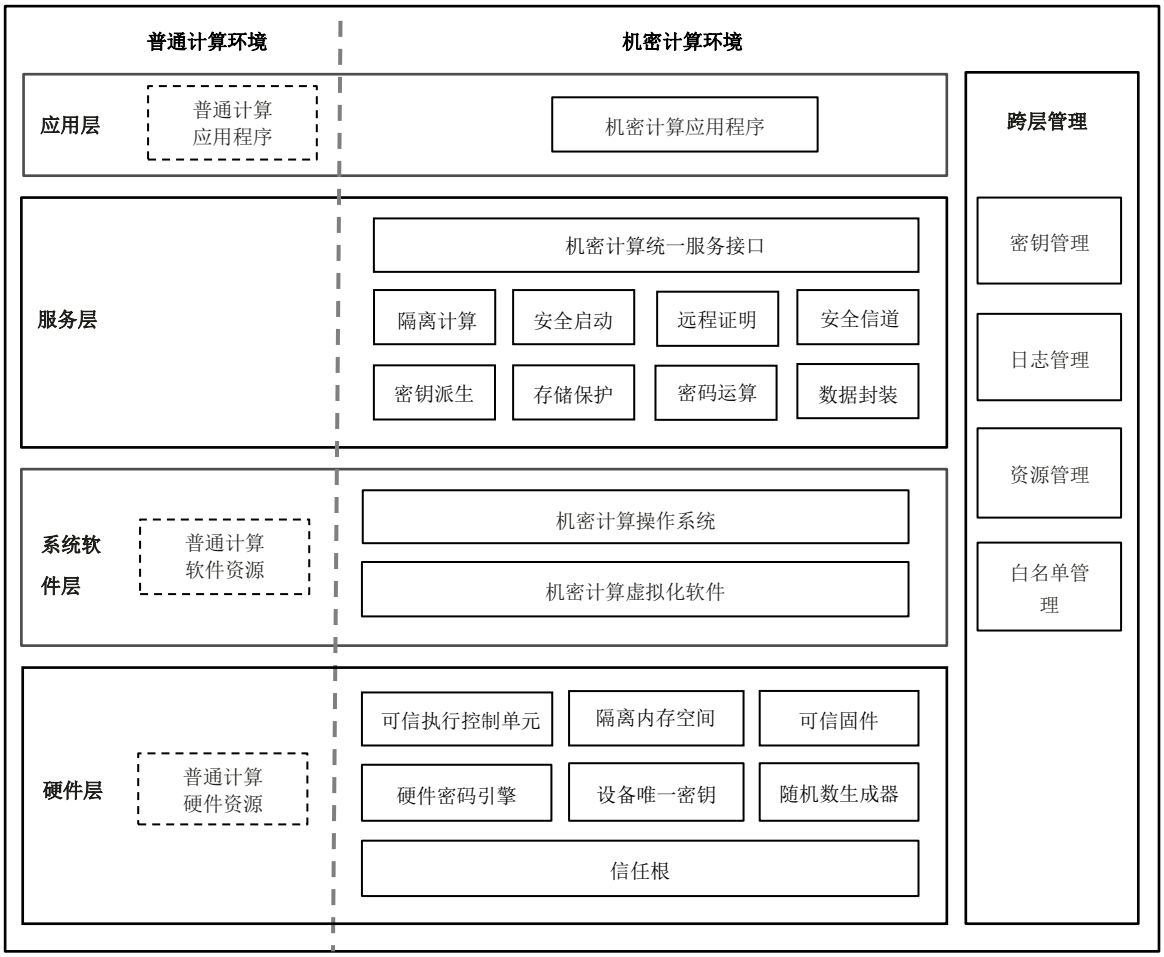


图2 机密计算通用框架图

注：图中纵向虚线用于区分机密计算环境和普通计算环境，实线框是机密计算环境的组件，虚线框是普通计算环境的组件。

6.2 框架组件

6.2.1 硬件层

机密计算环境中的硬件层组件主要包括：

a) 可信执行控制单元：在计算单元上定义安全加强的指令控制逻辑，以实现指令集执行隔离计算的目标，常见在缓存控制器、DMA控制器、中断控制器中加强，也有独立的控制单元；

b) 隔离内存空间：通过可信执行控制单元隔离出的内存空间，独立于通用内存空间；

c) 可信固件：提供识别硬件设备初始化信息、支持系统软件的完整性校验、升级维护以及配置机密计算环境资源等功能；

d) 硬件密码引擎：硬件密码引擎使用设备唯一密钥，为机密计算应用程序提供密钥派生能力；

e) 设备唯一密钥：在硬件中固化的一个唯一标识，设备制造阶段写入，设备唯一密钥由于具备唯一性，作为根密钥用于在机密计算环境中进行密钥派生；

f) 随机数生成器：用于在密钥生成和密码运算过程产生随机数，其中所生成的随机数应符合国家相关标准的要求；

g） 信任根：用于支撑机密计算环境自下而上信任链的建立，并提供安全存储、完整性度量、身份鉴别等安全功能。

6.2.2 系统软件层

机密计算环境中的系统软件层组件主要包括：

a） 机密计算操作系统：基于底层芯片的可信执行控制单元和指令集封装裁剪的操作系统，主要提供用于机密计算环境的计算资源调度、隔离内存空间管理以及和普通计算环境的通信机制等功能；

注：该组件可作为可选组件。

b） 机密计算虚拟化软件：部署在机密计算环境中的虚拟化软件，为机密计算虚拟机或机密计算容器的部署提供支撑。

注：该组件可作为可选组件。

6.2.3 服务层

机密计算环境中的服务层组件主要包括：

a） 机密计算统一服务接口：通过提供统一的编程接口，为应用程序提供与具体硬件架构解耦的统一机密计算安全服务，降低不同架构的开发与部署成本；

b） 隔离计算：区分普通计算环境和机密计算环境，提供统一的机密计算应用程序调用模式，支持计算参数的传入、计算状态的跟踪以及计算结果的获取，该服务是机密计算业务运行的前提，包含了机密计算环境的创建以及机密计算应用程序的部署；

c） 安全启动：保证机密计算环境的完整性和真实性；

d） 远程证明：对机密计算环境和机密计算应用程序进行完整性验证；

e） 安全信道：保证本地数据安全传输到机密计算环境中；

f） 密钥派生：保障在机密计算环境中所生成的密钥的安全性；

g） 存储保护：为用户提供敏感数据加密存储服务，这些敏感数据只能由机密计算服务授权的实体访问或修改；

h） 密码运算：在机密计算环境中执行密码运算操作；

i） 数据封装：为数据需求方提供敏感数据封装/解封装服务。

注：机密计算服务提供方可根据需求选择部署上述安全服务。

6.2.4 应用层

机密计算环境中的应用层组件主要包括：

机密计算应用程序：在机密计算环境中运行的应用程序，涉及敏感数据的处理逻辑都应在机密计算应用程序中完成。

6.2.5 跨层管理

机密计算环境中的跨层管理组件主要包括：

a） 密钥管理：对执行机密计算操作所涉及的密钥进行全生命周期管理；

b） 日志管理：对执行机密计算操作进行记录，提供日志回溯功能，并能保证日志的完整性；

c） 白名单管理：提供机密计算所涉及的固件版本、驱动程序、设备身份可信的清单；

d） 资源管理：对执行机密计算操作所需的CPU计算资源、内存资源等进行管理。

6.3 基础功能

6.3.1 硬件层

机密计算环境中的硬件层具备的基础功能主要包括：

a) 提供内存隔离机制，普通计算环境不能访问机密计算环境的内存原始明文数据；
b) 提供基于物理可信根的安全启动机制，对机密计算环境中的关键固件和关键系统软件进行完整性校验，校验通过方可加载和运行；
c) 提供基于硬件的密钥派生机制，保护被派生密钥的机密性；
d) 提供对普通计算环境和机密计算环境的通信指令调度机制；
e) 可以设置分配给机密计算环境的内存空间大小。

6.3.2 系统软件层

机密计算环境中的系统软件层具备的基础功能主要包括：

a) 保障普通计算环境仅根据其所分配的权限访问相应的机密计算应用程序，不能越权访问；
b) 提供多线程、多进程的计算能力；
c) 对机密计算应用程序进行完整性和真实性校验，验证通过后方可运行；
d) 使用符合国家密码管理部门相关要求的密码算法；
e) 具备适配主流编程语言的能力。

6.3.3 服务层

机密计算环境中的服务层具备的基础功能主要包括：

a) 提供应用程序集成开发接口和代码生成工具，提高开发机密计算应用程序的易用性；
b) 为服务提供方或结果需求方提供机密计算必要的安全服务；
c) 兼容不同的可信硬件架构。

6.3.4 应用层

机密计算环境中的应用层具备的基础功能主要包括：

a) 未经授权的应用程序不能查看正在机密计算环境中运行的代码和数据；
b) 未经授权的应用程序不能在机密计算环境内部添加、删除或更改运行的代码和数据。

6.3.5 跨层管理

机密计算环境中的跨层管理具备的基础功能主要包括：

a） 通过底层硬件保证密钥的机密性、不可篡改性和不可否认性；
b） 用于执行机密计算任务的密钥在机密计算环境内生成；
c） 确保机密计算环境内的加密密钥、签名密钥等密钥具有明确、单一的用途；
d） 对硬件资源状态、系统运行状态、接口适配情况、机密计算任务状态、网络状况等进行日志记录；
e） 对API调用、机密计算任务操作等进行日志记录和存储；
f） 保证只有被列入可信清单的实体才可以访问机密计算环境；
g） 保证机密计算应用程序仅根据分配的权限访问相应的资源，不能越权访问。

7 安全服务

7.1 隔离计算

7.1.1 普通计算应用程序和机密计算应用程序隔离计算

普通计算应用程序与机密计算应用程序之间的隔离计算流程如图 4 所示。

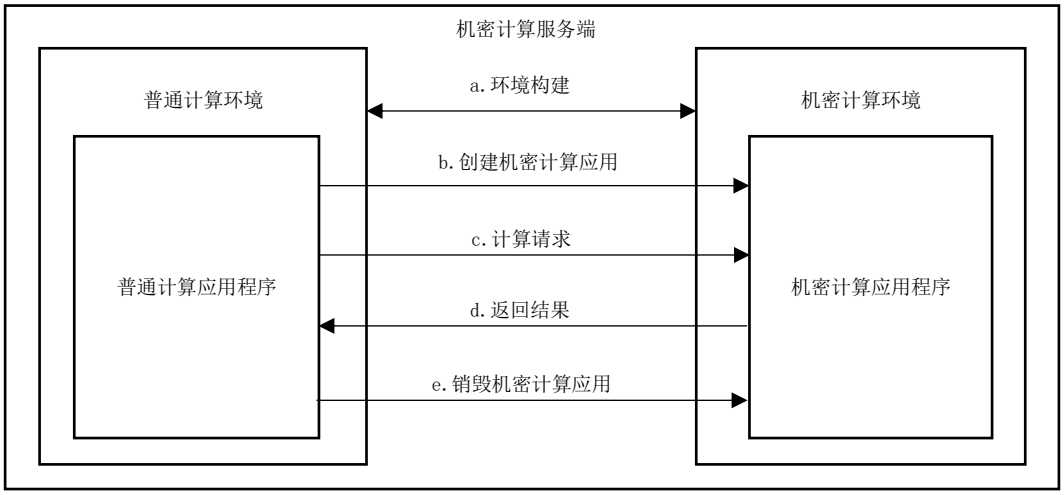


图4 普通计算应用程序与机密计算应用程序隔离通用流程图

普通计算应用程序与机密计算应用程序之间的隔离流程如下：

a） 普通计算应用程序在发起计算请求前，预先创建机密计算环境；

注：根据具体计算场景需求，机密计算环境也可在普通计算应用程序发起创建机密计算应用程序请求时，同步进行创建。

b） 普通计算应用程序调用机密计算应用程序创建接口申请创建机密计算应用程序，机密计算环境对普通计算应用程序的请求进行处理，并根据硬件层架构创建机密计算应用程序，并将机密计算应用程序部署并运行在机密计算环境中；

c） 普通计算应用程序向机密计算应用程序发起计算请求；

d） 机密计算应用程序完成计算任务，并向普通计算应用程序传输机密数据或返回计算结果；

e） 完成所有计算任务后，普通计算应用程序发出销毁机密计算应用程序的请求，机密计算环境销毁机密计算应用程序，会话结束。

7.1.2 机密计算应用程序和机密计算应用程序隔离计算

机密计算应用程序与机密计算应用程序之间的隔离计算流程如图 5 所示。

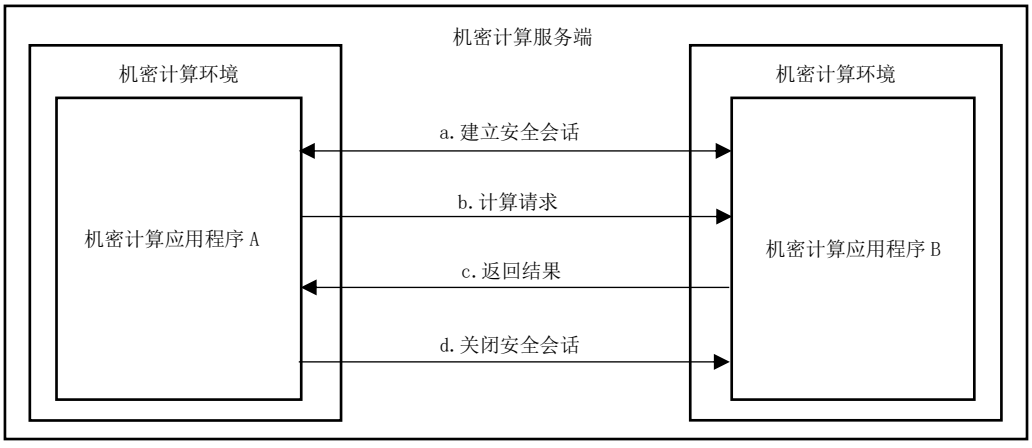


图5 机密计算应用程序与机密计算应用程序隔离通用流程图

机密计算应用程序与机密计算应用程序之间的隔离流程如下：

a） 机密计算应用程序 A 与机密计算应用程序 B 之间，先建立安全会话；

b） 机密计算应用程序 A 向机密计算应用程序 B 发起计算请求；

c） 机密计算应用程序 B 完成计算任务，并向机密计算应用程序 A 返回计算结果；

d） 完成所有计算任务后，机密计算应用程序 A 发出关闭会话的请求，会话结束。

7.2 安全启动

安全启动是保证机密计算环境的完整性和真实性的一种安全服务。在计算系统启动后，机密计算环境在建立前，应从物理信任根开始，建立自下而上的信任链，逐层验证机密计算环境中的关键组件。安全启动流程如图6所示。

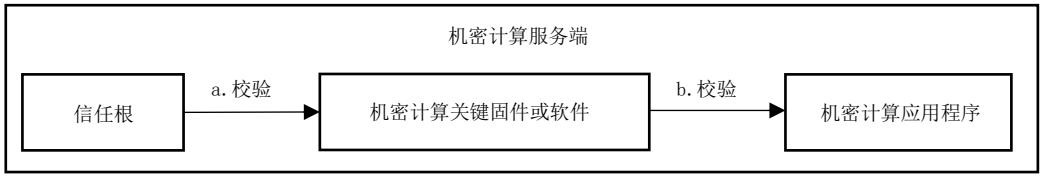


图6 安全启动通用流程图

安全启动流程如下：

a） 机密计算信任根在启动后对机密计算关键固件或软件的数字签名进行校验，确保未被篡改后，加载关键固件或软件；

b） 关键固件和软件对机密计算应用程序的数字签名进行校验，确保未被篡改后，机密计算应用程序可以正常运行。

7.3 远程证明

7.3.1 机密应用程序参与的远程证明

机密计算应用程序参与的远程证明通用流程如图7所示。在该流程中，远程证明发起端和机密计算服务端分别部署在独立的计算节点，远程证明服务端是可选的第三方可信实体。

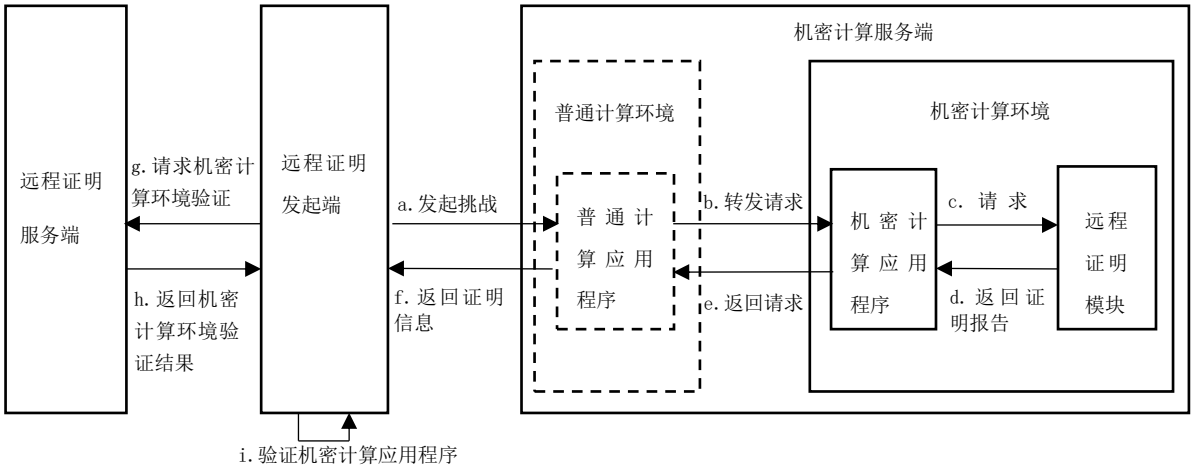


图7 机密计算应用程序参与的远程证明通用流程图

机密计算应用程序参与的远程证明通用流程如下：

a） 远程证明发起端通过远程证明接口，向机密计算服务端的普通计算应用程序发起证明挑战，通过发送随机值来防止重放攻击；

注：在虚拟化部署模式下，远程证明发起端可以直接向机密计算应用程序发起挑战，无需普通计算应用程序转发。

b） 机密计算服务端的普通计算应用程序将挑战转发至对应的机密计算应用程序；

c） 机密计算应用程序接收到请求后，将挑战转发给远程证明模块；

d） 远程证明模块接收到请求后，将证明报告（至少包括机密计算环境的度量报告、机密计算应用程序启动时的度量报告和运行时的度量报告）返回至机密计算应用程序；

e） 机密计算应用程序将证明报告返回至普通计算应用程序；

f） 普通计算应用程序将证明报告返回至远程证明发起端；

g） 远程证明发起端将证明报告发送给远程证明服务端；

h） 远程证明服务端验证证明报告中机密计算环境的度量信息（远程证明服务端维护了有效的机密计算环境列表），生成机密计算环境的验证结果，返回至远程证明发起端；

i） 远程证明发起端在确定机密计算环境可信的前提下，对机密计算应用程序的度量报告进行验证（远程证明发起端维护了机密计算应用程序的基线值），判断机密计算应用程序的完整性是否被破坏。

7.3.2 机密应用程序不参与的远程证明

机密计算应用程序不直接参与的远程证明通用流程如图 8 所示。在该流程中，远程证明发起端和机密计算服务端分别部署在独立的计算节点，远程证明服务端是可选的第三方可信实体。

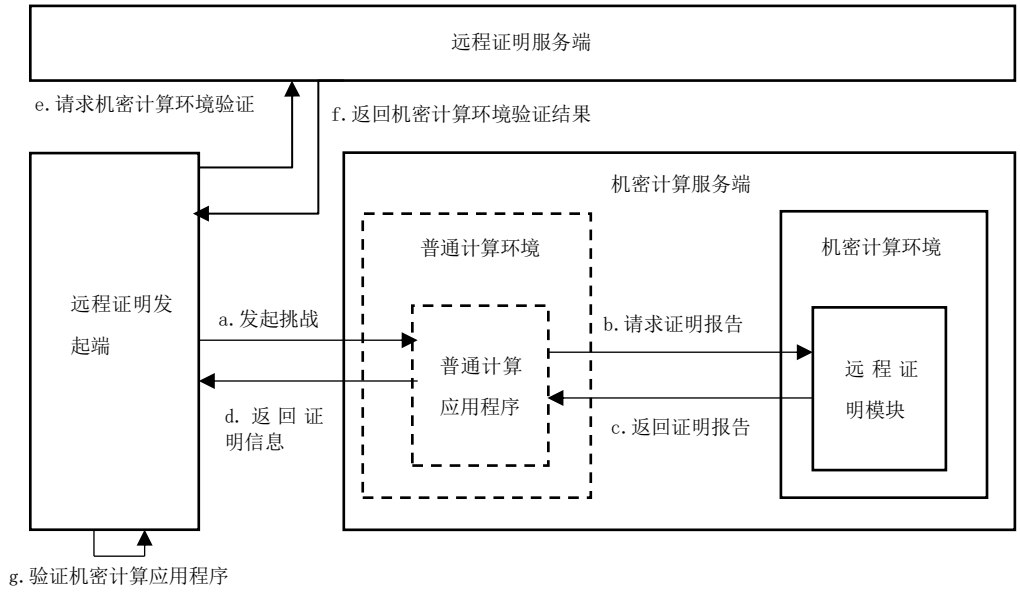


图8 机密计算应用程序不参与的远程证明通用流程图

机密计算应用程序不直接参与的远程证明通用流程如下：

a） 远程证明发起端通过机密计算统一服务平台提供的远程证明接口，向机密计算服务端的机密计算环境服务发起证明挑战，通过发送随机值来防止重放攻击；

b） 机密计算服务端普通计算应用程序将挑战转发至机密计算环境中的远程证明模块；

注：在虚拟化部署模式下，远程证明发起端可以向机密计算应用程序直接发起挑战，无需普通计算应用程序转发。

c） 远程证明模块接受到请求后，将证明报告（至少包括机密计算环境的度量报告、机密计算应用程序启动时的度量报告和运行时的度量报告）返回至普通计算应用程序；

d） 普通计算应用程序将证明报告返回至远程证明发起端；

e） 远程证明发起端将证明报告发送给远程证明服务端；

f） 远程证明服务端验证证明报告中机密计算环境的度量信息（远程证明服务端维护了有效的机密

计算环境列表），生成机密计算环境的验证结果，返回至远程证明发起端；

g） 远程证明发起端在确定机密计算环境可信的前提下，对机密计算应用程序的度量报告进行验证（远程证明发起端维护了机密计算应用程序的基线值），判断机密计算应用程序的完整性是否被篡改。

7.4 安全信道建立

安全信道建立是保护机密计算环境内外部通信安全的一种安全服务，通用流程如图9所示。其中，客户端和机密计算服务端分别部署在独立的计算节点。

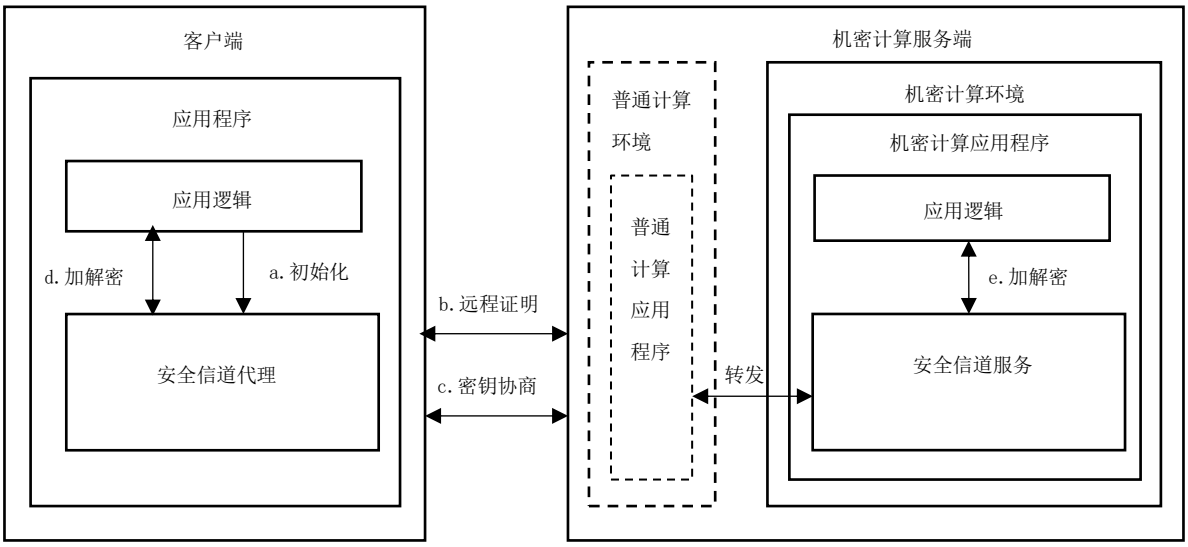


图9 安全信道建立通用流程图

安全信道建立流程如下：

a） 客户端应用程序通过安全信道初始化接口，向机密计算服务端发起构建安全信道请求；

b） 安全信道构建请求触发客户端应用程序向机密计算服务端发起远程证明请求，获取到携带公钥信息的远程证明报告，验证远程证明报告，证明机密计算应用程序完整性没有被破坏；

注：机密计算应用程序随机生成一对公私钥，将公钥信息作为远程证明报告的附加信息一起发送给客户端应用程序的安全信道代理，私钥缓存在内存中。

c） 客户端应用程序的安全信道代理基于公钥与机密计算服务端的机密计算应用程序的安全信道服务完成密钥协商，双方获得会话密钥，来执行加解密操作；

d） 其中步骤 c)为可选项，客户端应用程序的安全信道代理也可以根据业务场景直接选择使用公钥加密数据，机密计算服务端的机密计算应用程序的安全信道代理服务使用私钥进行解密；

e） 完成安全信道构建后，客户端应用程序可通过安全信道与机密计算服务端的机密计算应用程序进行安全通信。

注：普通计算应用程序作为可选组件。

7.5 密钥派生

密钥派生是保障机密计算环境中不同密码运算场景专属密钥需求的一种安全服务，通用流程如图10所示。基于硬件密码引擎，以设备唯一密钥为根密钥，派生得到的密钥与受信任的硬件绑定。

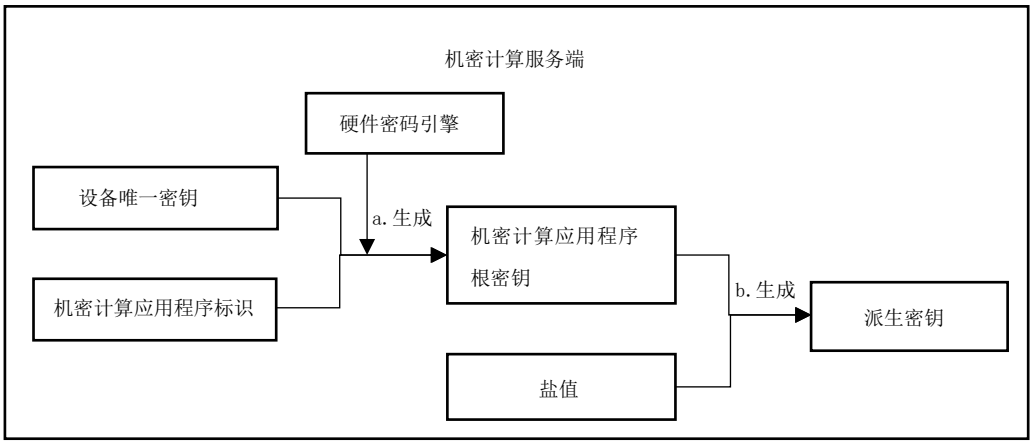


图10 密钥派生通用流程图

密钥派生流程如下：

a） 机密计算应用程序触发机密计算系统软件执行密钥派生功能，首先使用硬件密码引擎将设备唯一密钥和机密计算应用程序标识作为输入，派生出机密计算应用程序的根密钥；

b） 采用密码算法，将机密计算应用程序根密钥和盐值作为输入，计算出派生密钥，用来加密数据。

注：派生密钥使用完毕，可以通过释放内存来销毁密钥，再次使用时可重新派生，降低了密钥泄露的风险。

7.6 密码运算

密码运算是在机密计算环境中执行密码功能的一种安全服务，通用流程如图12所示。普通计算应用程序向机密计算应用程序发送密码功能请求，请求中可根据请求类型的不同，包含特定数目的参数，机密计算应用程序完成密码功能后返回密码功能响应给普通计算应用程序，响应中包含功能约定的处理结果。

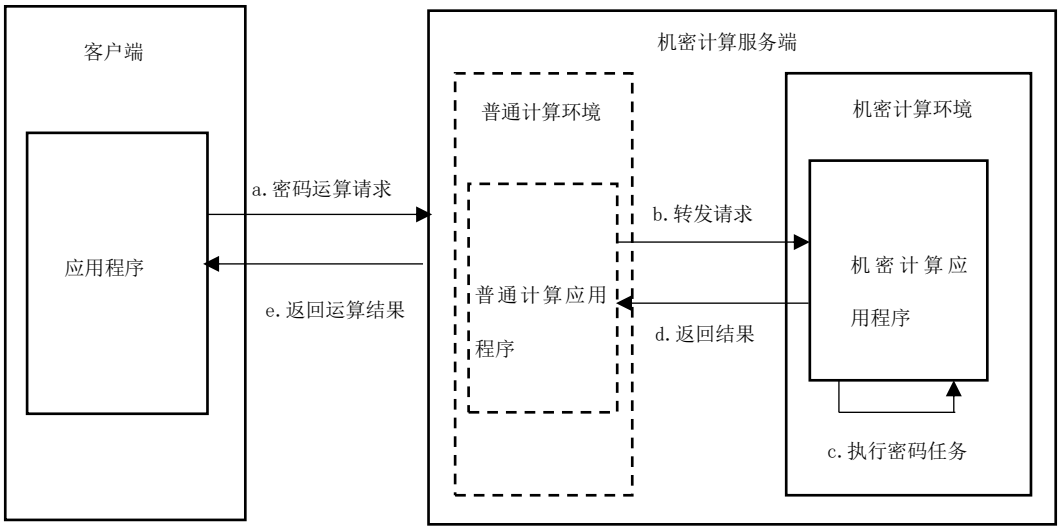


图12 密码运算通用流程图

密码运算包括但不限于以下类型：

a） 客户端应用程序通过密码运算接口，向机密计算服务端发起密码运算请求；

b） 机密计算服务端普通计算应用程序将请求转发至机密计算应用程序；

注：在虚拟化部署模式下，客户端可以向机密计算应用程序直接发起请求，无需普通计算应用程序转发。

c） 机密计算应用程序接受到请求后，执行密码运算任务，包括密钥生成、数据加解密、数字签名、

验证签名等操作，并将计算结果返回至普通计算应用程序；

d） 普通计算应用程序将计算结果返回至客户端。

7.7 存储保护

存储保护是一种保证结果需求方实现敏感数据加密存储，且只能由授权的机密计算应用程序访问或修改的安全服务，通用流程如图11所示。其中，客户端和机密计算服务端分别部署在独立的计算节点。

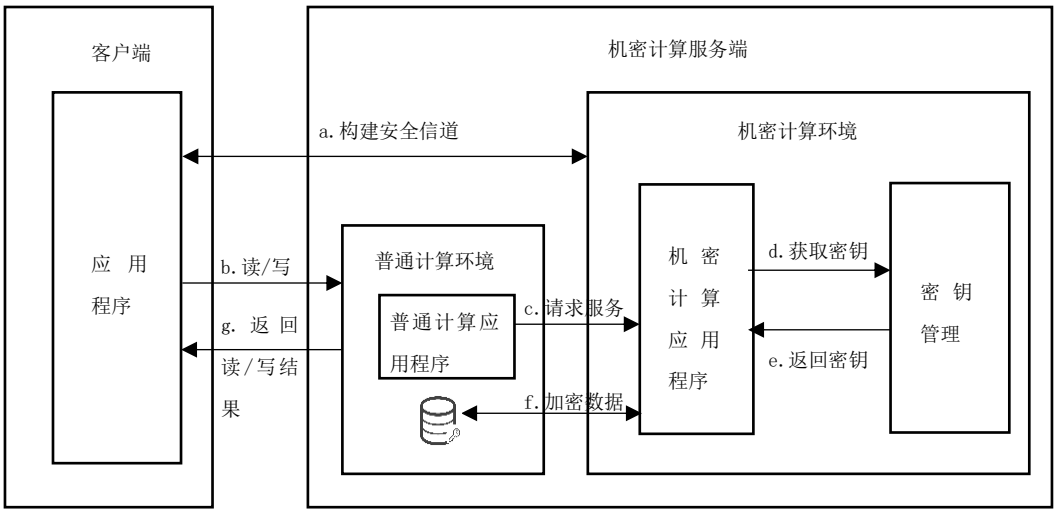


图11 存储保护通用流程图

写数据块流程如下：

a） 客户端在传输数据之前先和机密计算服务端构建安全信道（参见 7.4 流程）；

b） 客户端应用程序通过调用的存储保护接口，向机密计算服务端请求数据块写服务，并将数据块通过安全信道传输给机密计算服务端；

c） 机密计算服务端的普通计算应用程序将请求服务转发给机密计算应用程序接收任务；

注：在某些场景下，客户端可直接触发机密计算应用程序接收任务，无需普通计算应用程序转发。

d） 机密计算应用程序使用会话密钥或者私钥解密出数据块，并向密钥管理模块请求数据块加密密钥；

e） 密钥管理模块生成数据块加密密钥，返回给机密计算应用程序；

f） 机密计算应用程序使用数据块加密密钥对数据提供方上传的数据内容进行加密，将加密后的数据块存储在普通计算环境的磁盘中；

注：也可存储在机密计算服务端外部的存储系统中。

g） 完成存储后，机密计算应用程序返回结果至客户端应用程序。

读数据块流程如下：

h） 客户端应用程序通过调用存储保护接口，向机密计算服务端请求获取原始数据块；

i） 机密计算应用程序根据请求信息解析出需要获得的数据块名，并将数据块名发送至服务端的普通计算应用程序；

j） 普通计算应用程序根据数据块名，读取对应的密文数据块，并将密文数据块返回至机密计算应用程序；

k） 机密计算应用程序向密钥管理模块请求数据块加密密钥，并解密密文数据块，获取明文数据块；

l） 机密计算应用程序通过安全信道将数据块发送至客户端应用程序，流程结束。

7.8 数据封装

数据封装是一种使高敏感、高价值的数据与机密计算应用程序的完整性相绑定，在数据解封时，只有当机密计算应用程序的完整性未被篡改时，数据才可解封成功的安全服务，通用流程如图13所示。

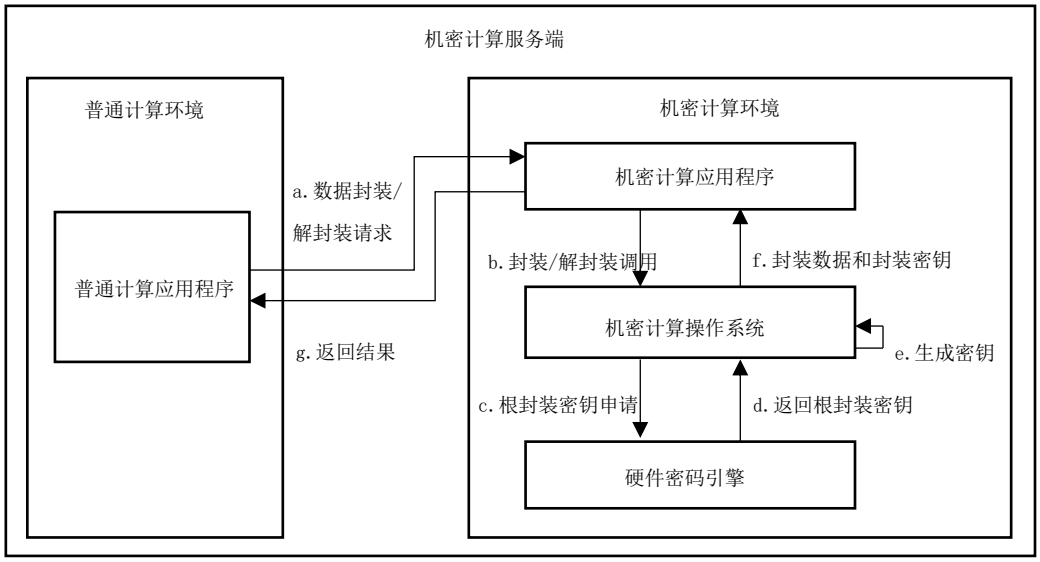


图13 数据封装通用流程图

数据封装流程如下：

a) 普通计算应用程序向机密计算应用程序发送数据封装请求；
b) 机密计算应用程序调用机密计算统一服务平台提供的数据封装接口触发机密计算操作系统；
c) 机密计算操作系统向硬件密码引擎发起根封装密钥申请；
d) 硬件密码引擎，将设备唯一密钥、机密计算应用程序标识和完整性度量值作为输入，生成根封装密钥并返回给机密计算操作系统；
e) 机密计算操作系统将生成的随机数和机密计算应用程序标识作为输入，生成封装密钥；
f) 机密计算操作系统使用封装密钥对数据进行加密，使用根封装密钥对封装密钥进行加密；
g) 机密计算操作系统将封装后的数据和封装后的密钥组合发给机密计算应用程序，同时释放内存，销毁根封装密钥和密钥明文，机密计算应用程序将密封数据和封装的密钥返回至普通计算应用程序，普通计算应用程序将其存储在本地的磁盘中。

数据解封装流程如下：

h) 普通计算应用程序向机密计算应用程序发送数据解封请求，并将封装数据和封装密钥发给机密计算应用程序；
i) 机密计算应用程序调用机密计算统一服务平台提供的数据解封装接口，触发机密计算操作系统使用硬件密码引擎，将该机密计算应用程序标识和完整性度量值作为输入，重新生成根封装密钥；
j) 机密计算操作系统使用根封装密钥对封装密钥进行解密，获得密钥明文，使用密钥对密封数据进行解密，获得明文数据；
k) 机密计算操作系统将解封的数据发给机密计算应用程序，同时释放内存，销毁根封装密钥和封装密钥明文；
l) 机密计算应用程序解封后的数据发送至普通计算应用程序，流程结束。

8 服务接口类型

本文件给出机密计算服务提供方或计算结果需求方开发应用程序所需的安全服务接口，见表1。

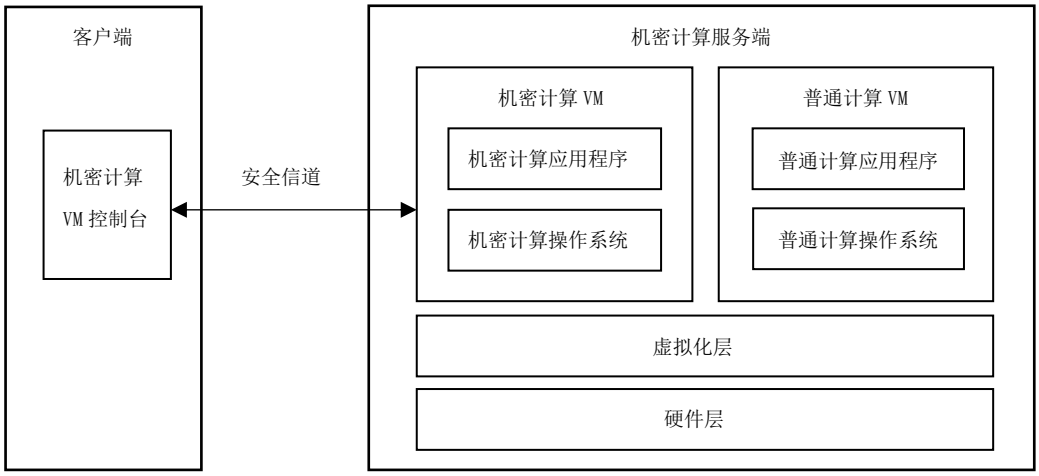
表1 机密计算服务接口类型

序号	接口名称	对应的安全服务	接口功能描述
1	创建机密计算应用程序	隔离计算	根据不同类型的可信硬件架构，调用不同的创建函数，完成不同类型的机密计算应用程序上下文初始化
2	销毁机密计算应用程序		根据不同类型的可信硬件架构，调用不同的退出函数，释放已经创建的机密计算应用程序实体
3	请求证明报告	远程证明	请求获取指定机密计算应用程序或机密计算环境的证明报告
4	验证证明报告		对指定机密计算应用程序或机密计算环境的证明报告进行验证，获得对其完整性状态的判定
5	安全信道初始化	安全信道	建立通信双方安全可信的传输通道，数据以密文形式传输到机密计算环境中
6	存储数据块	存储保护	请求写数据，以密文形式进行存储
7	读取数据块		请求读数据，对存储的数据进行解密
8	随机数生成	密码运算	调用随机数生成函数产生随机数，用于后面的密钥生成
9	密钥生成		通过密钥生成函数产生密钥
10	加密		对约定的数据进行加密
11	解密		对加密的数据进行解密
12	签名		对消息进行签名，生成数字签名
13	验签		对消息进行验签，以确认消息的完整性以及签名者的身份
14	封装数据	数据封装	使用和机密计算应用程序特征值绑定密钥加密数据
15	解封装数据		使用和机密计算应用程序特征值绑定的密钥解密数据

附 录 A
（资料性）
机密计算虚拟化部署模式

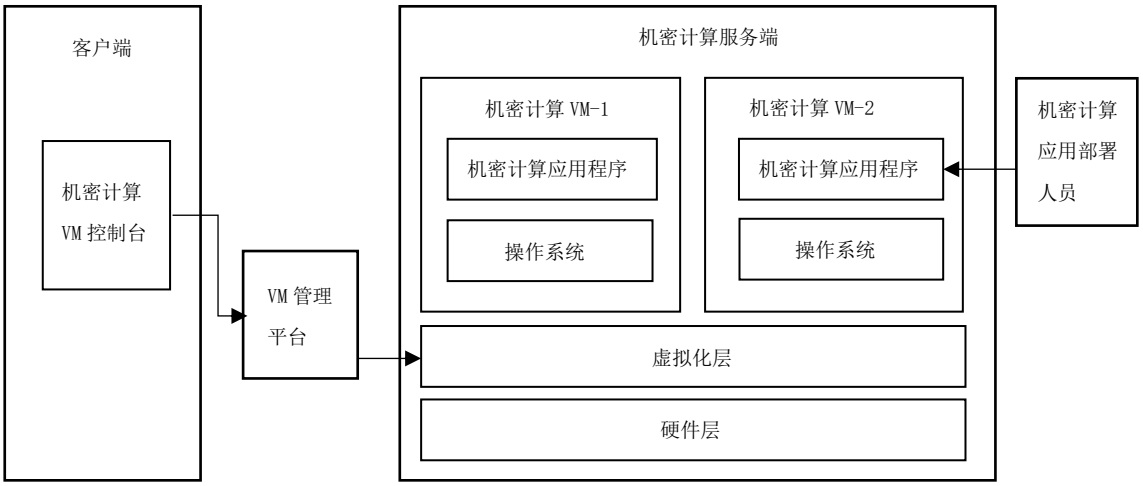
A.1 机密计算虚拟机

机密计算虚拟机（VM）是一个包含完整的机密计算操作系统和机密计算应用程序的的运行环境。机密计算操作系统可以支持完整的应用程序，也可以是应用程序拆分后的敏感部分。机密计算VM的部署模式有两种模式，分别如图A.1和A.2所示。



图A.1 机密计算VM部署模式一

在机密计算VM的部署模式一中，用户在客户端向机密计算服务端请求创建一个机密计算VM并建立客户端机密计算VM控制台和机密计算VM之间的安全信道，通过机密计算VM控制台发送请求，运行机密计算VM中的机密计算应用程序。机密计算应用程序的安装模式包含机密计算操作系统内置、非机密环境导入和运行时下载安装等。机密计算服务端可以根据硬件层的特征，选择部署机密计算虚拟化软件，或者部署通用的虚拟化软件，以支撑机密计算VM的创建、加载和运行。在运行时，机密计算应用程序的形态有两种模式，一种是完整的应用程序运行在机密计算VM中，另一种是将应用程序拆分敏感和非敏感两部分，非敏感部分作为普通计算应用程序运行在普通计算VM中，敏感部分作为机密计算应用程序运行在机密计算VM中。机密计算应用程序执行的中间结果或者最终结果，可通过安全信道直接返回给客户端或者先返回普通计算VM中的普通计算应用程序，再返回给客户端。



图A.2 机密计算VM部署模式二

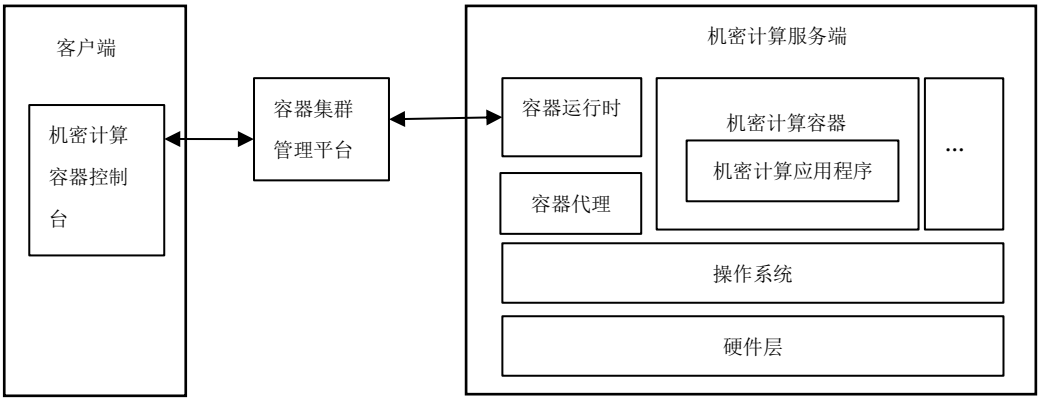
在机密计算 VM 部署模式二中，机密计算 VM 与普通计算 VM 在应用部署模式上并没有本质区别，只是机密计算 VM 对运行虚拟机的内存提供了硬件加密保护，可阻止主机和硬件所有者访问虚拟机中的数据。在该模式下，机密计算 VM 有两种运行方式：

登录部署：机密计算 VM 控制台通过机密计算 VM 控制台向虚拟机管理平台（例如云厂商提供）创建机密计算 VM，创建完毕后，机密计算应用部署人员即可登录到虚拟机中部署运行对应的机密计算应用程序。

直接运行：机密计算应用部署人员定制启动虚拟机的镜像文件，机密计算VM控制台直接通过虚拟机管理平台使用定制镜像创建启动虚拟机，机密计算应用程序自动在虚拟机中运行。

A.2 机密计算容器

机密计算应用程序可以以容器的方式部署与运行。机密计算容器的部署应支持对容器集群管理平台和容器运行时的兼容，用户的普通容器可以更加方便地切换为机密计算容器。机密计算容器部署模式如图A.3所示。其中，客户端具有机密计算容器控制台，用户使用机密计算容器控制台完成对其容器的具体操作；容器集群管理平台为对多节点容器部署调度的管理平台；服务端为运行机密计算容器的平台。



图A.3 机密计算容器部署模式

在机密计算容器部署模式中，用户在其客户端通过机密计算容器控制台向容器集群管理平台申请创建容器，容器集群管理平台采取相关的调度算法挑选一个服务器来承载用户机密计算容器。机密计算服务端可以根据硬件层的特征，选择部署机密计算操作系统，或者部署普通计算操作系统，以支撑机密容器的创建、加载和运行。机密计算服务端可以包含证明代理模块，完成对机密容器的完整性验证，在容器镜像加密的情况下，可以通过此代理在完整性验证成功后、完成对容器镜像的解密。当机密计算容器创建成功后，用户可通过机密计算容器控制台对机密计算应用程序进行创建、加载、销毁等具体操作。

附 录 B
（资料性）
机密计算任务执行过程中的信任模型

在机密计算环境中，需要建立各参与角色之间的相互信任，如果各角色间不能建立所需的信任关系，则存在计算结果不可信、算力被错误使用、数据权益被侵害等风险。安全威胁如表 1 所示。

表B.1 机密计算任务执行过程中的安全威胁

序号	关联角色	安全威胁
1	数据提供方对算力提供方*	若算力提供方的身份不可信，对数据提供方的数据权益造成侵害。
		若算力提供方的算力安全性不可信，数据可能在计算过程中被泄漏或被破坏，从而侵害数据提供方的权益。
2	算法提供方对算力提供方	若算力提供方的身份不可信，会造成算法滥用，对算法提供方的权益造成侵害。
		若算力提供方的算力安全性不可信，算法可能在计算过程中被泄漏或被破坏，从而侵害算法提供方的权益。
3	算力提供方对数据提供方	若数据提供方的身份不可信，会造成参与计算的数据不可信，从而破坏机密计算活动。
4	算力提供方对算法提供方	若数据提供方的身份不可信，会造成参与计算的数据不可信，从而破坏机密计算活动。
5	结果需求方对算力提供方、对数据提供方、对算法提供方	如果算力提供方身份以及安全能力不可信，或会造成结果需求方无法相信所获得的计算结果，从而破坏机密计算活动。
		如果数据提供方身份不可信，则意味着参与计算的数据来源不可信，会造成结果需求方无法相信所获得的计算结果，从而破坏机密计算活动。
		如果算法提供方身份不可信，则意味着参与计算的算法来源不可信甚至包含错误，会造成结果需求方无法相信所获得的计算结果，从而破坏机密计算活动。
6	算力提供者对结果需求方	若结果需求方身份不可信，则计算结果可能交给错误的接收者，损害结果需求方的权益。

注：为简洁起见，本文将机密计算平台提供方和机密计算服务提供方统称为算力提供方。

由上述威胁模型可推到得出典型的信任模型如图 B.1 所示。

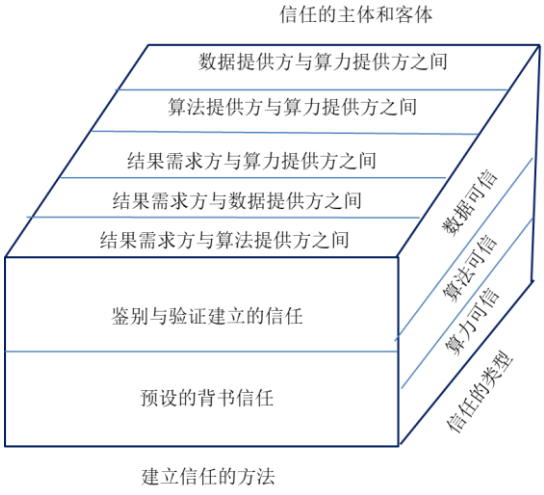


图 B.1 典型机密计算过程中的信任模型

典型机密计算业务执行过程中，信任模型包括三个维度，其一是信任的主体和客体维度，包括数据提供方、算法提供方、算力提供方以及结果需求方之间的信任；其二是信任的类型，包括数据、算法和算力的可信；其三是建立信任的方法，包括预设的背书信任、通过鉴别与验证建立的信任。其中信任背书提供者基于外部管理环节选择的设定内置在各实体机密计算相关系统中，为系统中的其他实体提供背书，同时为其它信任关系提供锚点和基础。

在此模型下，各角色的信任关系包括：

a） 数据提供方预设对算法提供方的信任背书提供者，包括算力安全性背书者以及业务身份背书者，从而能够信任数据计算方身份真实且能够在可信的封闭环境中完成数据处理，不造成数据泄漏，不侵害数据提供者的权益；

b） 算法提供方预设对算力提供方的信任背书提供者，算力安全性背书者以及业务身份背书者，从而能够信任算力提供者身份真实且能够在可信的封闭环境中完成数据处理，不造成算法内容泄漏，不侵害算法提供者的权益；

c） 算力提供方预设对数据提供方的信任背书提供者，从而能够信任所处理数据的来源真实可靠，进而保证数据可信；

d） 算力提供方预设对算法提供方的信任背书提供者，从而能够信任所运行算法来源真实可靠，进而保证算法内容可信。

e） 结果需求方预设对算力提供方、数据提供方、算法提供方的信任背书提供者，从而能够确认上述数据、算法和算力可信且安全，进而信任所获得的数据处理结果真实可信；

f） 算力提供方预设对结果需求方的信任背书提供者，从而能够信任接收数据处理结果的实体身份可信，确认计算结果交付的正确性。

附 录 C
（资料性）
机密计算典型应用场景

C.1 金融数据融合应用场景

金融机构在保证其资金正常运转，会利用大数据构建风控模型，通过技术手段减少风险事件发生的可能性，银行信贷风控与营销过程中往往需要政府、企业、个人数据提供支撑，然而在传统模式下，由于数据安全问题，银行难以高效且合规地获得企业与个人数据。机密计算技术可以在不泄露各方原始数据的前提下进行分布式模型推断和训练，政府部门可以将政务数据共享给金融机构，通过机密计算进行合规数据分析，实现精准风控。

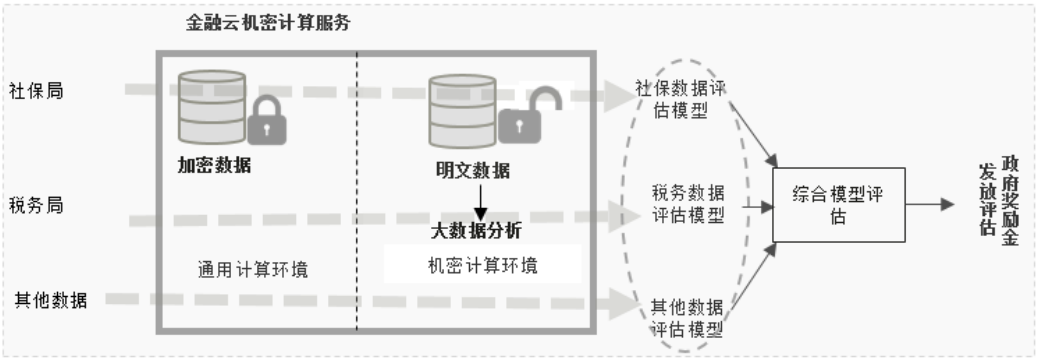


图 C.1 金融数据融合场景图

C.2 区块链智能合约应用场景

区块链场景下的典型安全解决方案利用机密计算、区块链等技术解决数据隐私问题，针对密钥以及当前物理加密机性能不足，基于硬件构建隐私保护的密钥管理系统，提高性能，能够提供一站式企业级可信数据协作解决方案，力图解决目前金融机构在数据协作过程中遇到的难题。在该方案中，智能云区块链平台提供了基于区块链的数据和计算过程的全流程监测、溯源和智能合约能力，同时结合机密计算安全硬件设备和技术，提供了区块链链外的可信计算能力，保障了数据在链外存储和链外运算过程中的安全、隐私、可信和公平。

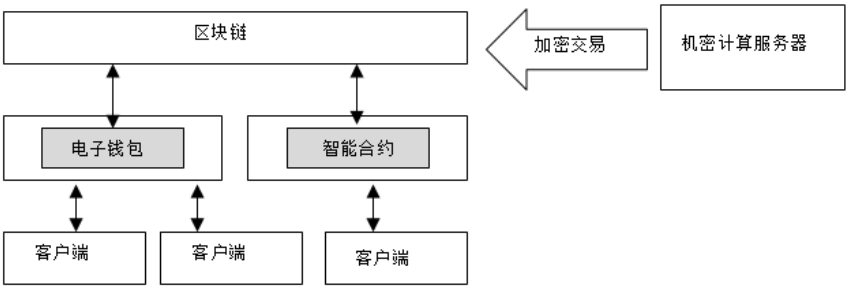


图 C.2 区块链智能合约场景图

C.3 保险机构核保查询应用场景

保险机构对自然人进行核保查询时，需要对被保人的健康情况和医疗记录进行核实比对。在传统的模式下保险机构可以直接读取到高度敏感的个人医疗数据，传统技术手段没有办法规约保险机构对

于隐私数据的使用范围。机密计算服务可以解决以上数据安全的问题，核保机密计算服务将核保模型置于可信执行环境运行，在核保过程中仅允许保险机构获取被核保算法运算过的核保结论，核保计算结束后即销毁计算环境和计算数据，真正确保了“只限核保”的使用约束。核保机密计算服务既可以保证核保算法的正确执行，又可以保证保险机构无法沉淀二次使用医疗数据。在整个核保数据流通过程中保证了数据的机密性、核保过程的准确性。

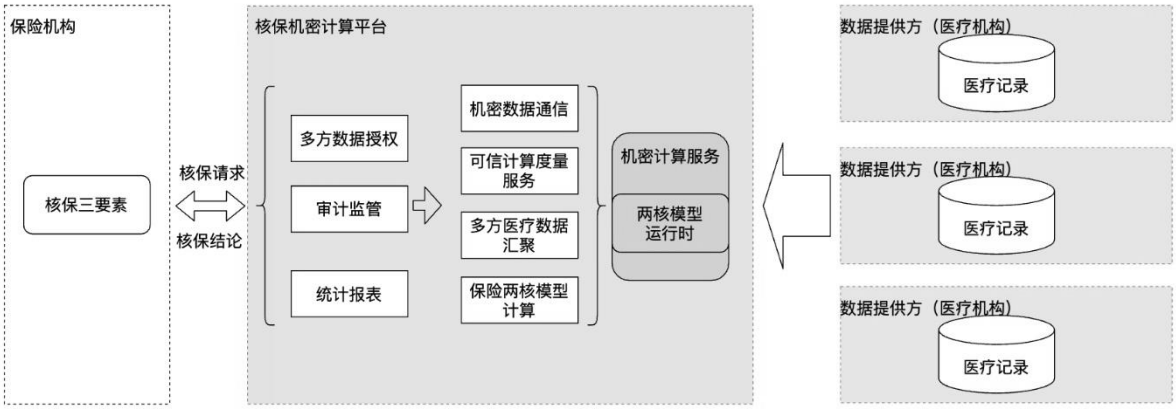


图 C.3 核保查询场景图

C.4 基因分析应用场景

在基因分析的场景中，专注于基因数据采集和基因数据分析的企业在医疗产业中紧密合作。由于基因分析需要传输和使用数量庞大且信息敏感的个人基因数据，数据提供方（基因数据采集机构）和数据使用方（基因数据分析机构）需要通过分布在产业云平台基础设施中完成数据的汇聚和计算。为了确保基因数据不泄露，基因数据分析算法全部运行在机密计算服务中，基因数据采集机构提供基因样本数据时需要验证机密计算服务的一致性和安全性。机密计算可保证在基因数据分析过程中基因数据被密态输入，基因数据的明文信息不落盘，且基因数据在分析后即销毁，基因分析需求方仅能获得最终的分析结果。用机密计算技术进一步加强了基因数据在使用时的安全性。

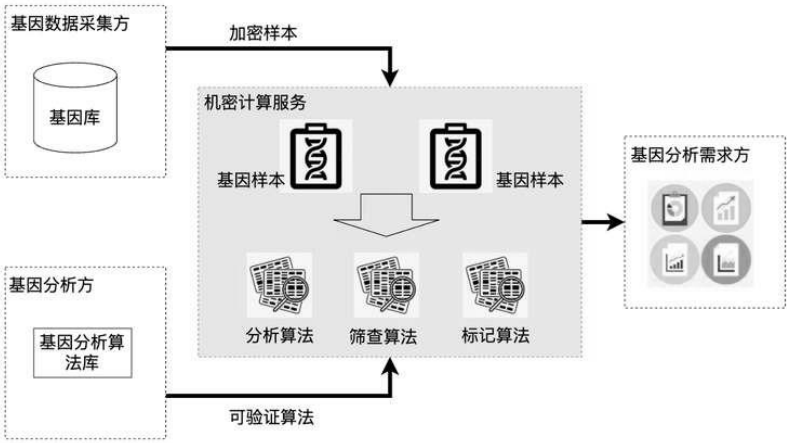


图 C.4 基因分析场景图

C.5 医疗数据共享应用场景

医疗数据包含患者信息、用户资料、基因数据等大量个人隐私数据，导致医疗机构、保险、药企、医药设备厂商之间数据流通共享难以高效协同，医疗数据价值难以有效发挥。机密计算可以为医疗数据参与方建立安全数据流通基础设施，推动医疗数据价值最大化利用。

目前各地卫健委响应国家健康医疗大数据战略纷纷建设医疗大数据平台，其医疗数据成为一座亟待挖掘的金矿。但碍于数据安全性考虑，医疗机构等多保持审慎的态度，对于与第三方企业共享数据积极性不足。医疗机构可基于机密计算数据安全开放平台实现健康医疗大数据的安全共享，在保证数据可用不可见，原始数据不流出的情况下，提供给医院或第三方企业对医疗数据进行充分挖掘。

基于机密计算平台，可以建立医疗数据安全共享科研平台，合法合规安全可控地向医院医生、科研机构、药企等单位开放医疗数据，提供丰富的算法与建模工具降低医生数据分析门槛，充分挖掘医疗数据价值。

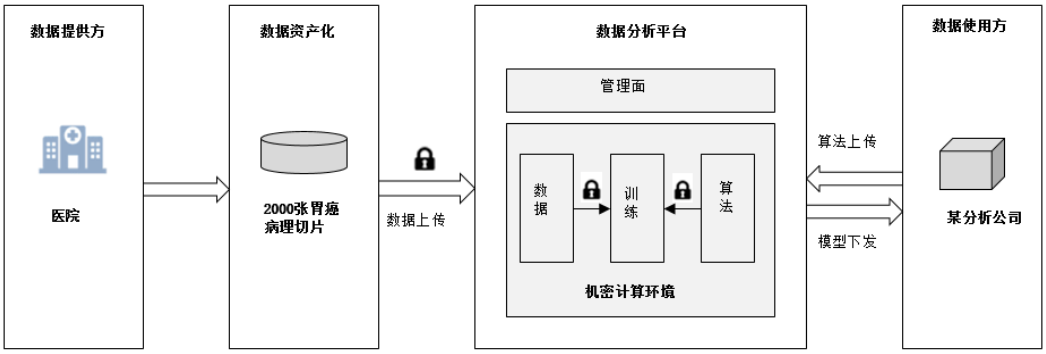
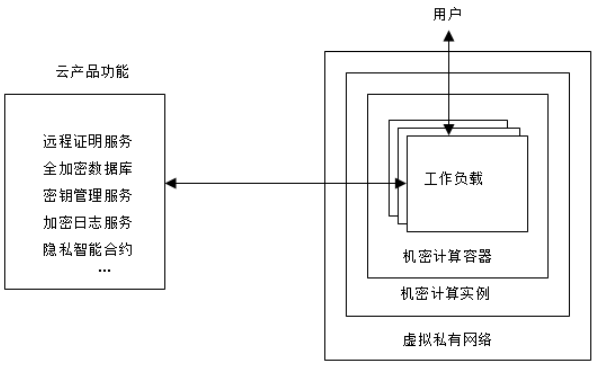


图 C.5 医疗数据共享场景图

C.6 公有云应用场景

在大数据时代，数据安全和隐私保护面临的挑战日益严峻，数据的安全处理和流通也受到国内外监管部门的广泛重视，公有云用户开始要求降低对云厂商的信任需求。这种变化趋势一方面与日趋严苛的隐私保护相关法律法规相关，另一方面考虑到云厂商可能不只是纯粹的云服务提供商，其业务与需求在不同领域可能与云租户或企业存在直接交叉，因此商业保密的风险问题对于公有云用户也必须充分考虑。

为了解决公有云上使用中数据的计算信任和安全性问题，同时推动数据要素的可信流通和开发利用，国内外主流云厂商正在通过开放协作的方式积极推动机密计算相关的技术和法规标准建设，并持续发布基于机密计算技术的云产品，旨在利用机密计算相关的理论框架和技术体系，对已有云产品的隐私安全能力进行增强，为用户的数据处理和模型合作提供全流程的安全和隐私保护，使用户更专注于业务上的创新。机密计算在公有云中的典型应用场景是为复杂多变的上层业务提供通用的“数据可用不可见”的安全体验，并实现机密计算资源的开箱即用和弹性伸缩。



图C.6 机密计算在公有云的典型场景图

C.7 云上全密态计算场景

云环境中，数据的所有权属于租户、但数据的计算需要在云环境中完成，如何防止数据在使用过程中不被攻击者（包括云服务提供方）获取始终是租户最为关心的问题，现阶段常用的解决方案是在云环境中部署专用的硬件密码机，租户的所有敏感内容均在指定的硬件密码机中完成。这种方式一定程度上解决了数据机密性问题，但硬件密码机的计算逻辑在出厂时就已固化，难以随业务需求快速调整；另外专用设备的计算能力受硬件限制，难以随业务需求动态伸缩，对于计算性能经常调整的场景，很难在性能和成本之间进行平衡。

利用机密计算环境可以提供全密态计算方案，较好解决上述问题。全密态计算方案包括管理节点、计算节点两种节点类型。管理节点负责对用户密钥进行统一管理，密钥与用户身份严格绑定，密钥不用时加密存储，密钥只能在用户参与下才能被解密并加载到机密计算环境中使用，单个管理节点可以管理大量的计算节点；计算节点基于机密计算环境构建，机密计算服务可以通过软件实现，按需加载，涉及敏感数据计算时，在租户参与下将所需密钥加载到机密计算环境中，然后由机密计算服务使用已加载的密钥，按照预先约定的接口对外提供服务即可。

该方案中所有涉密计算逻辑可由软件实现，可以随业务需求快速迭代；涉密计算均利用节点自身算力完成，避免了调用远程密码机的数据泄露风险、不再占用网络带宽、密码算力也可以随业务节点增减弹性伸缩。该方案较好的解决了数据机密性与流动性的矛盾，可以广泛用于全密态数据库、云上机密计算资源池、多方参与的隐私增强计算等场景，为“数据可用不可见、数据不动价值动”提供了一种较为理想的实现方式。

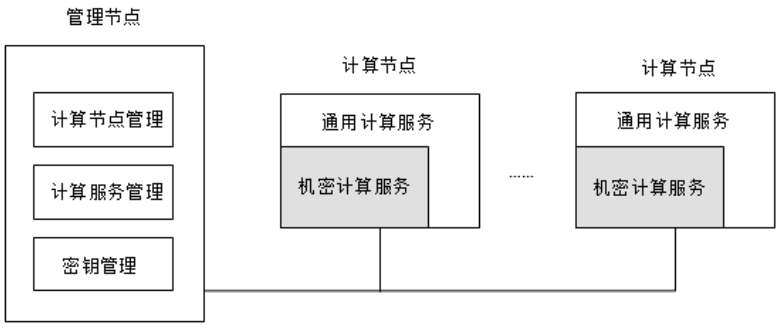
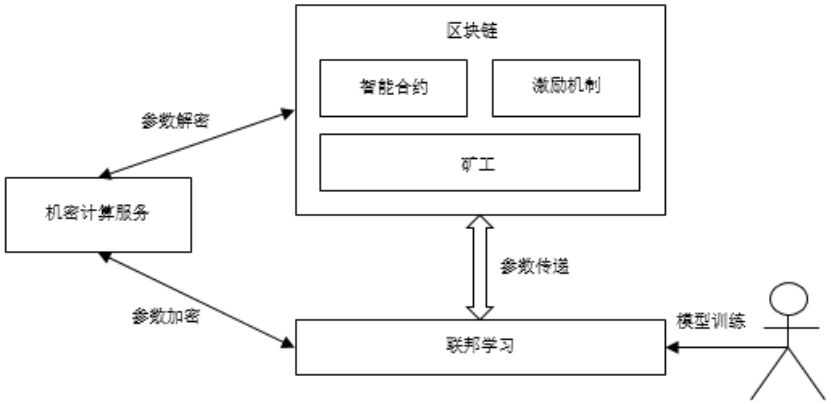


图 C.7 云上全密态计算场景

C.8 区块链联邦学习应用场景

传统联邦学习中每个用户在本地进行模型训练，将参数上传至一个可信中央服务器中，结合多方完成模型更新，保证用户的数据隐私。其局限性在于该场景依赖于一个单一的中央服务器，容易受到服务器故障的影响，同时不存在适当的激励奖赏来激励用户提供数据训练和上传模型参数，数据安全性也难以保障。面对以上问题，基于机密计算的区块链联邦学习,使用区块链网络替代中央服务器，区块链网络允许本地模型更新，用户将自身训练模型的梯度通过机密计算单独加密后进行上传；同时提供激励机制，矿工使用所有梯度来更新所有参与者协同加密的协作模型的参数，将包含该参数的新区块添加到区块链中，并对诚实参与者进行激励；多个用户需要提供他们的私密密钥，借助区块链访问机密计算服务来协同解密获得已更新的模型参数。通过区块链与机密计算的结合，使得联邦学习拥有更佳的保密性、可审计性和公平性，并进一步提高了联邦学习的安全性和实际使用性。



图C.8 区块链联邦学习应用场景图

参 考 文 献

[1] GB/T 41388-2022 信息安全技术 可信执行环境 基本安全规范

[2] 机密计算产业联盟（Confidential Computing Consortium，CCC）白皮书：Confidential Computing: Hardware-Based Trusted Execution for Applications and Data

[3] 机密计算产业联盟(Confidential Computing Consortium,CCC)白皮书:A Technical Analysis of Confidential Computing v1.2

[4] IETF RATS Working Group：Remote Attestation Procedures Architecture