专栏：算力网络

基于国密算法的算力网络安全研究

潘洁[1]，叶兰[2]，张鹏飞[2]，卜忠贵[1]
（1. 中国移动通信集团设计院有限公司，北京 100080；
2. 中国移动通信集团有限公司，北京 100032）

摘　要：随着国密算法的推广，对算力网络进行了深入的研究，提出了更高效合理的算力网络安全方案，方案借助国密算法保证算力网络的数据安全及隐私。设计方案内容主要包括：通过底层资源支撑算力需求及密码调用，算力编排层提供数据算力的编排能力；同时，算力调度层智能判别算力资源调度分配的最优节点；密码加固层使用基于硬件支撑下的国密算法，借助公钥密码体制、哈希函数、数字信封、同态加密、区块链等技术，重点研究了算力网络接入安全、传输安全、数据安全及隐私保护方面的安全实现。研究方案创新性地提出了一种保障算力网络数据安全的架构及应用形式，能够满足应用层算力在大数据、智能技术等场景的需求。通过国密算法赋能算力网络，提升算力网络的安全性。

关键词：算力网络；国密算法；隐私保护；同态加密；区块链
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2023160

Research on the security of national secret algorithm based compute first networking

PAN Jie[1], YE Lan [2] , ZHANG Pengfei[2], BU Zhonggui[1]
1. China Mobile Group Design Institute Co., Ltd., Beijing 100080, China
2. China Mobile Group, Beijing 100032, China

Abstract: With the promotion of national secret algorithm, in-depth research on the arithmetic network was carried out, a more efficient and reasonable security scheme for the arithmetic network was proposed, ensuring the data security and privacy of the arithmetic network with the help of the state secret algorithm. The main elements of the design program included: Supporting arithmetic demand and cryptographic invocation through the underlying resources, the arithmetic orchestration layer provided the ability to orchestrate data arithmetic, meanwhile, the arithmetic scheduling layer intelligently discerned the optimal nodes for arithmetic resource scheduling and allocation; the cryptographic reinforcement layer used the national secret algorithm based on hardware support with the help of public key cryptosystem, hash function, digital envelope, homomorphic encryption, blockchain and other technologies. Focusing on arithmetic network access security, transmission security, data security and privacy protection aspects of security implementation. An architecture and application form was innovatively proposed to guarantee the data security of the arithmetic network, which could meet the needs of the application layer arithmetic in the scenarios of big data, intelligent technology, etc.. The security of the arithmetic network is enhanced by empowering the arithmetic network through the state-secret algorithm.

Key words: compute first networking, national secret algorithm, privacy protection, fully homomorphic encryption, blockchain

收稿日期：2023−06−13；修回日期：2023−08−06

0 引言

随着全球 5G 及 AI 等技术的快速发展，各种人工智能、大数据分析等应用场景越来越多；同时，智算、超算、图像处理等异构算力不断兴起，数据使用呈指数型增长，算力面临着更强大的使用需求。此外，云计算等技术的广泛使用也使得算力应用更加便捷，可供应用的算力节点广泛分布。但目前这些计算节点散落分布，没有行之有效的协同机制，在此大环境下，算力网络由此诞生，用以实现“计算+网络”的高效协同发展，实现算力的统一调度编排。

在数字信息时代，算力无疑是具有强核心竞争力的，甚至在未来，算力也将发挥更大的作用及价值。而把所有算力连接成网络，即算力网络，也是一种新型信息基础设施，是通信、计算、存储及智能化调度的深度融合，用以实现算力资源高效协同与融合发展。与此同时，算力网络资源作为新型基础设施，资源布局需落实国家政策要求、预判产业趋势，并满足未来业务对大规模、广覆盖、高性能、高可靠算力的迫切需要，这也是算力网络的研究现状。

算力网络（compute first networking）提供算力和网络的深度融合，已成为“网络强国”“数字中国”等相关工程的重要支撑。当前算力网络的建设已步入关键时期，保证算力网络安全、构建属于算力网络的安全体制，成为推动算力网络高质量发展的关键。但进入算力时代以来，伴随泛在接入、万物互联，全社会数据量迎来爆发式增长，需要通过算力网络解决大数据计算资源不足、异构算力不足等问题，同时安全攻击手段层出不穷，算力网络也面临着各种安全隐患。

算力网络的发展经历了很多过程。“东数西算”的提出标志着国家对全国和区域算力的统筹规划，是实现算力资源优化配置的一个国家工程，同时东数西算工程也是算力网络的宏观背景。当前算力网络安全研究还在探索中，大量研究工作在不断推进。我国三大运营商高度重视算力网络发展，并积极推动相关标准的制定；2021 年 4 月，中国通信标准化协会（CCSA）通过了算力网络、泛在计算总体技术要求等相关行业标准立项。IMT-2030（6G）网络工作组成立算力网络研究组，研究网络中计算、网络融合对于网络架构的影响。2022 年 1 月，中国移动发布了《算力网络安全白皮书》，提出了融合接入安全、隔离安全等一体化安全防护技术架构及一体化全程可信的安全机制。此外，三大运营商积极在国际电信联盟电信标准部（ITU-T）、CCSA 等主要标准组织立项算力网络相关标准。

算力网络的新架构、新技术和新服务可能带来新的安全风险，需要与之适配的新的安全机制来保障。例如，在算力节点的网络接入、身份鉴别等过程，在算力数据的跨节点网络传输过程，在算力数据的机密性完整性保护过程等。此外，算力网络中还面临用户隐私保护的问题，可能存在用户隐私泄露、数据流转不可控等安全风险。因此，对算力网络展开安全风险研究，并结合密码学技术实现算力网络安全是非常必要的。

1 关键技术

算力信息的机密性、完整性等安全特性在算力网络的平稳运行中起着关键性影响。但算力节点分布广泛且安全防护能力各异，若某一节点被伪装攻击，非法节点获取算力信息或者伪冒篡改算力信息，将对算力网络安全产生重大危害。大量重要信息集中存储，数据被窃取的风险也在无形增加，一旦数据泄露，可能会导致黑客对算力网络的非法利用，若数据被篡改，还会造成用户数据的泄露。此外，在算力网络中数据所有权与使用权分离，计算主客体信任关系被割裂，使得计算数据的保密性、完

整性和可用性面临威胁。数据在流转过程中可能被窃取、篡改，数据流转信息及计算状态信息可能被伪造。

因此，在算力网络中，数据在各节点的使用、传输、存储等过程的安全性也是不容忽视的。为保证算力服务的正常开展，本文方案提出了基于国密算法的算力网络安全加固思想。

国密算法，即国家商用密码算法，是由国家密码管理局认定和公布的密码算法标准及应用规范，其中部分密码算法已经成为国际标准。将明文数据通过加密变成密文，可以确保数据的机密性、完整性、不可否认性，同时也能起到身份认证的作用。目前，常用的国密算法见表 1。

表 1　常用的国密算法

密码算法类别		国产商用密码算法
对称密码算法	分组密码/块加密	SM1、SM4、SM7
	序列密码/流密码	祖冲之（ZUC）
非对称密码算法/公钥	基于离散对数问题	SM2、SM9
哈希函数/杂凑算法	—	SM3

SM2 算法是基于椭圆曲线公钥算法，也是国密标准中的非对称算法，具有公钥加/解密、密钥交换以及数字签名功能。SM3 算法是国密标准中的杂凑算法，用于数字签名验签、消息认证码及伪随机数生成等。SM4 算法是国密标准中的分组对称算法，加密和解密所用密钥相同，可用于数据的快速加/解密。

此外，隐私保护在算力网络中也是至关重要的，因此本文在国密算法的基础上，借助区块链、多方安全计算、同态加密等技术完善安全算力网络的隐私性。

（1）同态加密：在不解密密文的情况下，对密文进行特定的运算，使得解密该运算结果与直接使用对应明文进行运算操作效果一致，确保数据机密。

设 $E(K,x)$ 表示用加密算法 E 和密钥 K 对 x 进行加密，F 表示运算，如果对于加密算法 E 和运算 F，存在有效算法 G 使得：

$$E(K,F(x_1,\cdots,x_n))=G(K,F(E(x_1),\cdots,E(x_n))) \quad (1)$$

因此，就称加密运算 E 对于运算 F 具有同态性。设加密函数为 E_k，解密函数为 D_k，明文数据为 $(m_1,m_2,\cdots,m_n)$，则加法同态和乘法同态可分别表示为：

$$\sum_{i=1}^{n} m_i = m_1+m_2+\cdots+m_n = D_k(E_k(m_1)+E_k(m_2)+\cdots+E_k(m_n)) \quad (2)$$

$$\prod_{i=1}^{n} m_i = m_1\cdot m_2\cdots m_n = D_k(E_k(m_1)\cdot E_k(m_2)\cdots E_k(m_n)) \quad (3)$$

（2）安全多方计算：为数据需求方提供不泄露原始数据前提下的多方协同计算能力，能够在数据机密性的前提下对数据进行处理。此外多方计算也能实现数据的访问控制权，即计算方只能获得特定数据结果。简单阐述即，设 $n(n\geqslant 2)$ 个参与方 $D_1,D_2,\cdots,D_n$，然后参与方使用各自的秘密输入 $x_1,x_2,\cdots,x_n$，共同计算一个 n 元函数 $f(x_1,\cdots x_n,)=(y_1,\cdots,y_n)$，其中 y_i 是参与方 D_i 完成计算后得到的秘密输出。最终每位参与方 D_i 仅可获取 y_i 和 x_i 及由这二者推出的信息，而得不到其他信息。

（3）区块链技术：区块链可以看成是一种按时间的先后顺序将数据区块相连的形式连接而成的链式数据结构，且用密码学保证其难以篡改、难以伪造、去中心化、去信任的分布式账本。区块链是由无数区块前后相连形成的链，而区块又由两部分组成：区块头、区块体。区块头代表了该区块的基本信息，里面包含版本信息、时间戳、前一个区块的哈希值、当前区块目标哈希值、默克尔（Merkle）树根、随机数。在区块头中，通过前后区块哈希值保证区块以时间序列相互连接且难以篡改，并且是可溯源的。区块体则包含了某段时间内的账本即交易记录。

2 算力网络国密算法安全应用架构

考虑算力网络安全，安全应用架构设计方案引入国密算法。整体架构由算力资源层、算力编排层、算力调度层、密码安全层和算力应用层组成。底层是算力基础设施，包括计算资源、网络资源等，同时本文方案加入密码资源池，创建不同密码资源以保证数据安全。算力编排层负责算力的编排、管理，主要进行算力的多维度划分，如时效要求、算力要求、智能计算要求、安全性要求等，将算力资源和算力信息进行统一服务编排。在算力调度层使用蚁群优化算法、多级反馈队列调度算法等进行算力的调度，将不同算力需求分配到各算力枢纽或算力集群及边缘算力节点等，进而为更上层的大数据、超算服务、虚拟现实（VR）视频等业务提供直接调度应用。在整个算力网络构架构中，本文主要工作在于加入密码安全层，一方面借助国密算法实现整个算力网络中接入安全、传输安全、数据安全的机密性、完整性、不可否认性等要求；另一方面，通过同态加密、区块链等技术实现算力网络的隐私保护。基于国密算法的算力网络安全架构如图 1 所示。

本文安全架构主要在算力网络架构中引入密码安全层，构建公钥密码体制、数字信封、同态加密、零知识证明等的安全使用，保证数据机密性、完整性、可溯源及不可否认性。在接入安全方面，借助公钥密钥体系的数字证书认证机构（CA）及数字签名（Sig）实现身份鉴别；在传输安全方面借助安全套接层（SSL）握手协议实现会话密钥协商，从而保证传输通道安全；在数据安全方面，使用 SM4 算法对称加密实现数据机密性，使用 SM3 哈希运算实现数据完整性保护，使用 SM2 算法实现非对称加密及签名验证的身份验证、数字信封的密钥传递等。同时，密码安全层还可进行隐私保护技术应用，通过同态加密实现机密数据的安全传输及密文可计算，以及通过区块链技术数据上链，多节点使用，并保证数据安全的可验证性等。

图 1 基于国密算法的算力网络安全架构

3　算力网络国密安全应用方案设计实现

3.1　密码技术框架

在算力网络中，算力网络的安全性是必不可少的。安全算力网络建设则离不开密码体系的建设，本文主要通过国产商用密码算法，结合对应的软硬件实现算力网络中的机密性、完整性、不可否认性等安全特性。商用密码应用技术框架如图 2 所示。

该框架分为密码资源层、密码支撑层、密码服务层和密码应用层 4 个层次，同时，密码管理基础设施保障整体的系统运行。

密码资源层提供对称、非对称、杂凑等基础密码算法；其上层以算法软件、算法 IP 核、算法芯片等形态对密码算法封装。密码支撑层提供密码资源调用，由安全芯片类、密码模块类、密码整机类等密码产品，如算法芯片、软件算法引擎、数据库加密机、密钥管理系统等组成。密码服务层提供密码应用程序接口，其中，对称密码服务为上层应用提供数据的机密性保护功能；公钥密码服务为上层应用提供身份认证、数据完整性和抗抵赖等功能。密码应用层调用密码服务层提供的密码应用程序接口，实现数据在传输、存储和处理时的机密性和完整性。密码管理基础设施作为一个相对独立的组件，为上述 4 个层次提供运维管理、信任管理、设备管理和密钥管理等功能。

国密算法在安全性、性能等方面都优于国际通用算法，使用 SM2、SM3、SM4 等国密算法进行数据安全保护是行之有效且自主可控的。针对数据机密性要求，可根据使用场景采用不同的国密算法及密码技术进行安全加固，例如，普通数据通过数字信封下发对称密钥，各节点通过对称密码 SM4 对处理数据进行加解密；针对需要身份鉴别的节点认证过程，通过公钥密码算法的 SM2 签名验签进行身份鉴别，SM2 加解密保证目标节点可解密；针对数据完整性需求的过程，通过 SM3 消息摘要及 SM3-HMAC 消息认证码实现完整性校验；同时，借助身份认证方案及密钥协商协议可在通信过程中实现身份认证，并确保数据安全性，做到会话密钥协商。

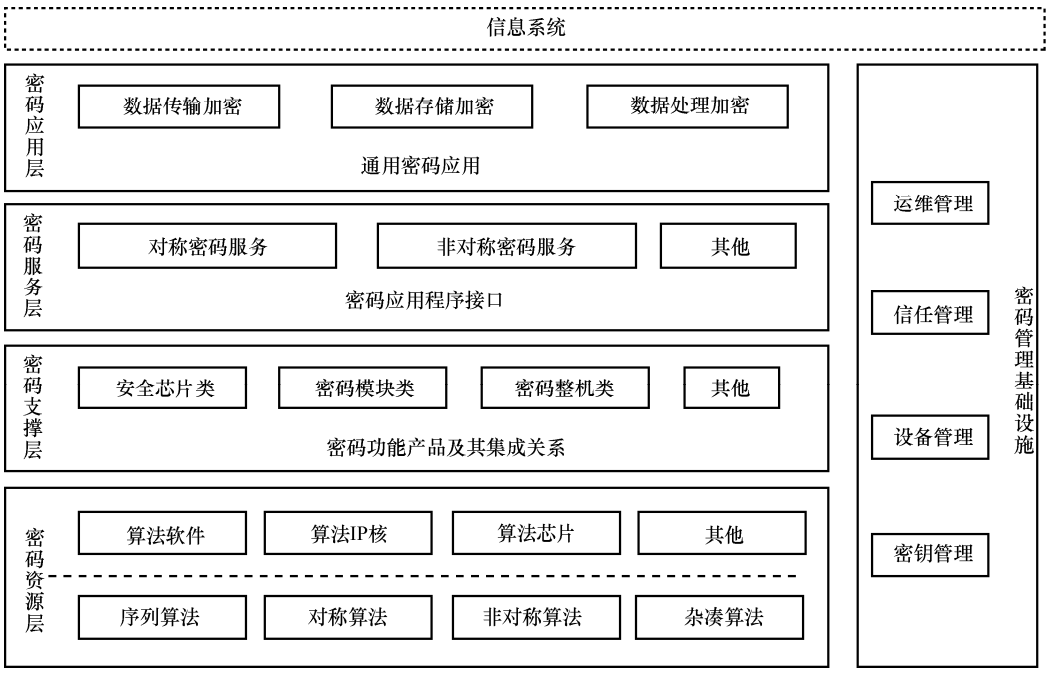


图 2　商用密码应用技术框架

除此之外，在算力网络中，可以将各枢纽、集群、边缘算力等节点联合，组建区块链网络，保证上链数据多节点可见可验证，做到数据可溯源；在算力调度到各不同节点运算的过程中，对于机密性、秘密性数据的隐私保护，可利用同态加密等技术进行密文传输和密文计算；对于数据的安全可验证性可联系零知识证明保证数据计算结果的安全牢固等。

3.2 基于国密算法的算力网络安全实现

本安全架构将算力网络与密码紧密结合，最终实现基于国密算法的安全算力网络。在确定算力的节点调度后，根据算力网络安全需求确定密码算法及密码资源调用。首先需要对算力需求数据的安全性要求及应用场景分析，判断算力网络数据传输的密码需求，然后根据算力需求节点与算力调度节点之间的实际情况，选择合适的密码资源及密码算法。最终，借助相应国密算法进行算力网络安全建设，形成算力网络的算力调用分发及算力结果反馈，完成算力网络的应用服务。

在算力网络的安全架构及安全体系下，本方案重点关注接入安全、传输安全、数据安全 3 个层面的国密算法安全实现以及其他隐私计算安全要求下的密码技术应用实现。

3.2.1 接入安全

安全接入是算力网络安全的第一道防线，主要手段通过身份鉴别、身份认证实现，即保证算力网络节点的身份合法性，防止非授权用户访问系统。

安全接入技术思路是对节点进行身份认证，只允许通过安全认证的节点接入系统。身份认证的主要功能是验证用户的身份，现在常用的是公私钥和数字证书机制。X.509 证书是必需的，并使用公钥技术和数字证书验证数字证书所有者的身份；同时，为了防止重放攻击，也会加入时间戳。时间戳和数字证书由可信第三方信任背书身份。验证步骤如下。

步骤 1 各节点向 CA 申请证书，随后 CA 为各个算力节点颁发数字证书。

步骤 2 在需要接入算力网络与其他节点发起会话请求时，节点 A 使用自己的节点私钥 sk_A 进行签名得到 $Sig_{sk_A}(M)$，同时选取当前时间戳 T，以及 CA 颁发给自己的数字证书，将这 3 部分内容发送给其他算力网络节点。

步骤 3 算力网络节点收到节点 A 的会话请求时，首先计算 $\Delta T = T' - T$,检查是否在可信时间内，然后借助 CA 机构颁发的数字证书获取节点 A 的公钥 PK_A，使用 PK_A 验证签名 $Sig_{sk_A}(M)$。验证通过则该节点合法。

3.2.2 传输安全

数据传输安全需要基于国密安全算法的通信防护技术支撑，主要通过对称加密、非对称加密、消息摘要等数据加密技术、密钥交换技术、通信终端在链路层、网络层及传输层的数据机密性和完整性保护技术。

在各算力枢纽算力集群等节点间建立安全通道，实现算力节点的身份认证，确保通信的保密性和传输数据的完整性，主要通过以下几种方式。

（1）以数字令牌为媒介，在传输过程中，配置安全接入网关，通过 VPN 技术，使用国密 SM2_SM3_SM4 算法套件的 SSL 协议实现双向握手，建立安全传输通道。

（2）通过国密 SM2 和 SM4 混合加密算法，同时使用 SM3 算法进行数据摘要并完成完整性认证，SM2 签名算法进行身份认证，防止伪装、篡改、重放、抵赖等攻击。

（3）安全传输系统采用 HTTPS 协议进行随机数交换，并通过约定协议计算会话密钥，随后通过会话密钥进行传输数据的 SM4 加密。

算力网络传输安全步骤如下。

步骤 1 各节点通过 SSL 协议或基于数字证书的身份签名 Sig 实现身份认证，并协商会话密钥 sk，建立安全通道，或者通过 SSL VPN 握手建立。

步骤 2 完成通道建立后，数据传输时，发

送方使用接收方公钥 PK 进行公钥加密 $E_{\mathrm{PK}}(M)$，此时算法使用 SM2 算法进行数据加密，或者使用会话密钥进行对称加密 $E_{\mathrm{sk}}(M)$保证机密性，此时算法使用 SM4 加密，同时在消息 M 后接连该数据杂凑值 $\mathrm{Hash}(M)$ 以保证完整性，此时算法使用 SM3 加密。

步骤 3　接收方拿到发送方数据后，进行对应的算法解密 $D_{\mathrm{sk}}(M)$，从而实现数据传输安全；此外，接收方对获取的消息 M 进行 SM3 哈希运算，并对比收到的哈希值 $\mathrm{Hash}'(M)?=\mathrm{Hash}(M)$，从而实现数据传输的完整性校验。

3.2.3　数据安全

（1）在数据安全方面，主要对重要鉴别数据、身份数据、应用数据做机密性完整性保护，同时在数据落盘存储时进行数据安全保护。下面对机密性完整性如何通过国密算法实现分别进行描述。

步骤 1　资源调度节点发起算力请求，并根据调度节点公钥 PK 进行 SM2 公钥加密算法对会话密钥 sk 加密 $E_{\mathrm{PK}}(\mathrm{sk})$，使用会话密钥 sk 通过 SM4 对称加密算法加密算力调度请求数据 $E_{\mathrm{sk}}(M)$。

步骤 2　调度节点收到相应的算力请求，使用自身私钥 sk 借助 SM2 公钥算法解密会话密钥 $D_{\mathrm{sk}}(\mathrm{sk})$，然后使用会话密钥 sk 对称解密算力数据进行数据处理 $D_{\mathrm{sk}}(M)$。

步骤 3　数据处理完成后，使用会话密钥加密数据处理结果 $E_{\mathrm{sk}}(M')$，并响应给算力需求节点。

（2）当算力需求节点与调度节点算力网络涉及算力的身份认证及完整性要求时，步骤如下。

步骤 1　算力需求节点向调度节点发起算力请求，并使用自身私钥 sk 进行 SM2 算法数字签名 $\mathrm{Sig}_{\mathrm{sk}}(M)$，同时将数据进行 SM3 哈希运算 $\mathrm{Hash}(M)$。

步骤 2　调度节点收到相应的算力请求，使用算力需求节点公钥 PK 借助 SM2 算法验证签名 $\mathrm{Ver}_{\mathrm{PK}}(M)$，并对数据进行 SM3 哈希运算 $\mathrm{Sig}_{\mathrm{sk}}(M)$，从而对比哈希值是否一致。

步骤 3　通过后，该集群进行数据处理，并将处理结果使用算力需求节点公钥 PK 加密后发送给该节点 $E_{\mathrm{PK}}(M')$。

3.2.4　其他安全要求实现

除此之外，其他算力调度需求根据不同的场景及安全性进行了不同的安全加固，包括数据采集安全、数据隐私保护等方面。

（1）算力网络涉及多源、泛在算力节点，无法保证每个算力节点都是安全可靠的，将数据分配到算力节点进行计算的模式使数据面临隐私泄露的风险，需要借助隐私计算技术来实现数据的“可用不可见”。隐私计算包括安全多方计算、可信执行环境、联邦学习等多种技术路线，分别适合不同的应用和场景。在算力网络中，算力节点采用隐私计算的应用场景包括以下几点。

- 数据计算场景：用户将数据上传到算力网络中，算力网络运营者会访问到机密数据，暴露相关数据隐私；在这种情况下，可使用多方计算、同态、私密计算等隐私计算技术来实现数据的“可用不可见”。
- 端云协作场景：toC 应用中需要收集用户数据进行画像、服务推荐、统计分析、AI 训练及服务等，需要在端侧收集个人相关数据，可使用差分隐私、联邦学习、多方计算技术在不收集用户数据或不明文使用数据的前提下，满足业务需求，保证数据最小化隐私保护要求。

在算力网络中，借助多方安全计算及同态加密实现隐私保护步骤如下。

步骤 1　算力需求节点将消息 M 处理得到 $m_1,m_2,\cdots,m_n$，并在调度中将不同的需求算力数据分配到不同的调度节点。当需求节点发起算力请求时，使用自身节点私钥 sk 进行 SM2 算法加密 $E_{\mathrm{sk}}(m)$，同时发送 Diffie-Hellman（DH）协商请求信息，如随机数 R；对不同调度节点发送不同的

密文信息及随机数 $E_{sk}(m_i),R_j$。

步骤 2 调度节点收到相应的算力请求，直接对密文数据进行密文同态处理 $G(K,F(E(m_1),\cdots,E(m_n)))$，并选取随机数 r 进行 DH 会话密钥协商。

步骤 3 调度节点完成算力数据处理后，将处理结果进行会话密钥协商，其中协商过程使用算力需求节点发送的随机数 R 及自身选取随机数 r。将最终结果通过会话密钥反馈给需求节点 $E_{sk}(m)$。

步骤 4 需求节点使用调度节点发送的随机数 r 及自身选取的随机数 R 进行会话密钥计算，得到后解密收到的结果 $D_{sk}(m)$，然后对该同态处理密文进行解密 $D(K,F(m_1,\cdots,m_n))$。若为加法同态，则为 $D_k(E_k(m_1)+E_k(m_2)+\cdots+E_k(m_n))=m_1+m_2+\cdots+m_n=m$。

在算力网络中，借助区块链实现隐私保护及可溯源的步骤如下。

步骤 1 算力需求节点将消息 M 进行处理得到该时间段区块交易信息。当需求节点发起算力请求时，使用自身节点私钥 sk 进行数字签名 $\mathrm{Sig}_{sk}(M)$，同时通过链上的假名将该交易信息广播到区块链系统。

步骤 2 区块链节点共识，区块上链。当需求节点将对应的信息广播到整个链上之后，其余节点使用该假名节点公钥 PK 进行数字签名 $\mathrm{Sig}_{sk}(M)$ 的验证，并借助系统的激励机制与共识机制获取记账权，该交易信息得以成功上链，所有节点同步账本信息。

步骤 3 数据账本溯源。当算力网络中的节点交易数据出现问题时，根据该数据信息的节点名称、区块记录时间、节点公钥等信息查找账本记账数据，由于账本信息全系统节点同步，无法同时篡改所有节点账本信息，保证防篡改。同时区块链式存储，查链后查询当时区块信息，实现了可追踪溯源。

3.2.5 基于国密算法的算力网络安全架构

最终，构建了更安全合理的算力网络，基于国密算法的算力网络安全架构实现如图 3 所示。

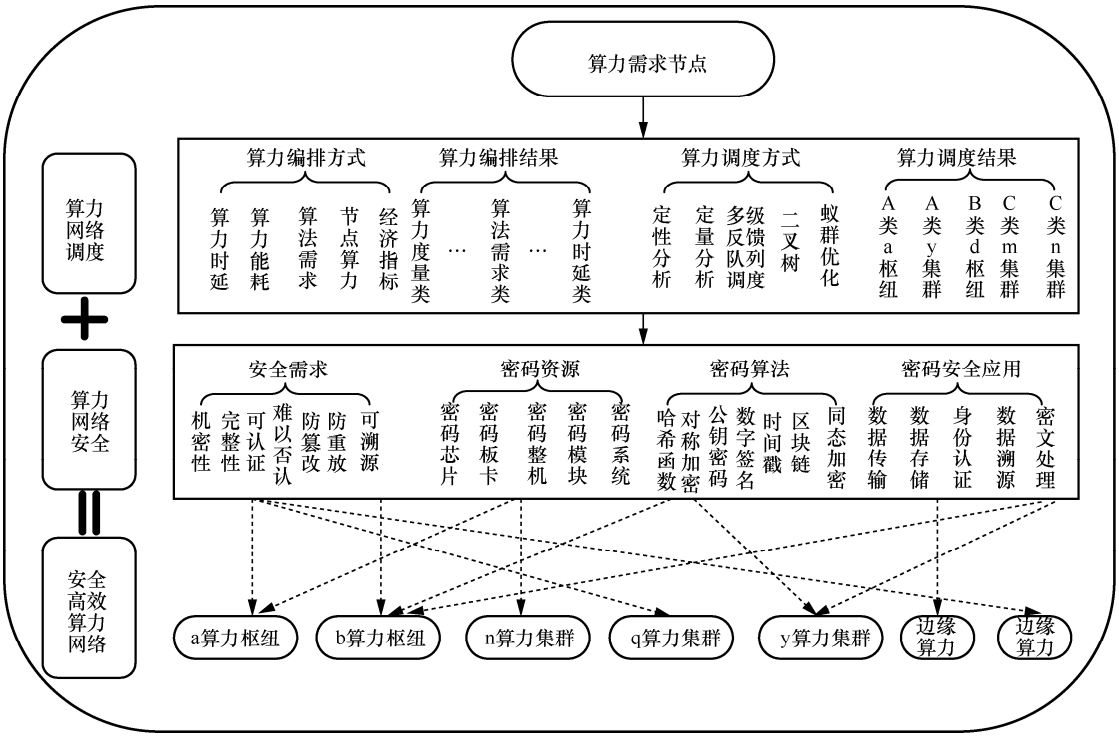


图 3 基于国密算法的算力网络安全架构实现

综上，本文研究的算力网络安全方案，其调度过程借助国密算法，根据算力网络的安全性需求，结合应用场景，进行算力网络密码安全建设，最终实现算力应用，保证业务的用户体验。

本文借助国密算法保证算力网络的安全，赋能算力网络在应用中发挥更大的价值，同时减弱算力网络使用中因信息安全给社会和个人带来的危害，提供既切合业务需求又安全可靠的算力网络服务。本文探究了在国密算法的安全加固下，推动算力网络的可信构建，保证数据生命周期安全，实现算力网络安全可信。

4　结束语

本文提出了基于国密算法的算力网络安全研究建设方案。在安全性保证方面，本文引入国密算法及密码应用技术框架，针对不同需求进行不同密码安全建设，重点针对接入安全、传输安全、数据安全三大方面进行方案实现的阐述，并提出其他隐私计算场景及技术实现，保证算力网络隐私安全。在国密 SM2、SM3、SM4 等算法及对称加密、非对称加密、数字签名、多方安全计算、同态加密、区块链等技术的支撑下，本文方案可以有效地实现算力网络安全，此外，配合产业发展制造，在基于软硬件支撑下的国密算法加固下增强算力网络稳健性。

展望算力网络的发展过程，未来的路还很长，主要体现在：构建算力网络安全技术联合创新，强化顶层设计，攻关隐私计算、全程可信等安全领域安全技术，统一算力网络安全技术路线；除了安全建设之外，仍需要加快算力网络安全产业成熟发展，强化算网安全产业链协同。最后，需要全社会共同推进算力网络安全生态繁荣。

参考文献：

[1] 雷波, 刘增义, 王旭亮, 等. 基于云、网、边融合的边缘计算新方案: 算力网络[J]. 电信科学, 2019, 35(9): 44−51.
LEI B, LIU Z Y, WANG X L, et al. Computing network: a new multi-access edge computing[J]. Telecommunications Science, 2019, 35(9): 44−51.

[2] 唐雄燕，曹畅，李建飞, 等. 算力网络前沿报告[R]. 北京: 中国通信学会, 2020.
TANG X Y, CAO C, LI J F, et al. Frontiers of algorithmic networks report[R]. Beijing: China Institute of Communications, 2020.

[3] 国家发展和改革委员会. 全国一体化大数据中心协同创新体系算力枢纽实施方案[R]. 2021.
National Development and Reform Commission. Implementation plan for the arithmetic hub of the national integrated big data center collaborative innovation system[R]. 2021.

[4] 工业和信息化部. 新型数据中心发展三年行动计划[R]. 2021.
Ministry of Industry and Information Technology. Three-year action plan for new data center development[R]. 2021.

[5] 中国信息通信研究院. 中国数字经济发展白皮书[R]. 2021.
China Academy of Information and Communications Technology. White paper on the development of China's digital economy[R]. 2021.

[6] 中国信息通信研究院. 2022 中国综合算力指数[R]. 2022.
China Academy of Information and Communications Technology. 2022 China integrated computing power index[R]. 2022.

[7] 中国移动通信集团有限公司. 算力网络白皮书[R]. 2021.
China Mobile Communications Group Co., Ltd. Computing force network white paper[R]. 2021.

[8] 中国移动通信集团有限公司. 算力网络安全白皮书[R]. 2022.
China Mobile Communications Group Co., Ltd. Computing force network security white paper[R]. 2022.

[9] 叶沁丹, 范贵生, 黄衡阳. 算力网络一体化支撑方案及应用场景探索[J]. 数据与计算发展前沿, 2022, 4(6): 55-66.
YE Q D, FAN G S, HUANG H Y. Study on integrated support solution and application scenarios of computing power network[J]. Frontiers of Data & Computing, 2022, 4(6): 55-66.

[10] 张旭光, 陈鸣锴, 魏昕. 算力网络支撑下的泛在化视频传输调度[J]. 计算机研究与发展, 2023, 60(4): 786-796.
ZHANG X G, CHEN M K, WEI X. Ubiquitous video transmission scheduling supported by computing power network[J]. Journal of Computer Research and Development, 2023, 60(4): 786-796.

[11] 段晓东, 姚惠娟, 付月霞, 等. 面向算网一体化演进的算力网络技术[J]. 电信科学, 2021, 37(10): 76-85.
DUAN X D, YAO H J, FU Y X, et al. Computing power network technologies for computing and network integration evolution[J]. Telecommunications Science, 2021, 37(10): 76-85.

[12] 姚惠娟, 耿亮. 面向计算网络融合的下一代网络架构[J]. 电信科学, 2019, 35(9): 38-43.
YAO H J, GENG L. Trend of next generation network architec-

ture: computing and networking convergence evolution[J]. Telecommunications Science, 2019, 35(9): 38-43.

[13] DONG Y, SONG L, XIE R, et al. Ultra-low latency, stable and scalable video transmission for free-viewpoint video services[J]. IEEE Transactions on Broadcasting, 2022, 68(3): 636−650.

[14] MINOPOULOS G, PSANNIS K E, KOKKONIS G, et al. QoE assessment of video codecs for video streaming over 5G networks[C]//Proceedings of 2020 3rd World Symposium on Communication Engineering (WSCE). Piscataway: IEEE Press, 2020: 34-38.

[15] 陈波, 邓清唐. 基于云计算的电力终端安全接入体系架构研究[J]. 电子产品可靠性与环境试验, 2022, 40(4): 89-93.
CHEN B, DENG Q T. Research on the security access architecture of power terminal based on cloud computing[J]. Electronic Product Reliability and Environmental Testing, 2022, 40(4): 89-93.

[16] 贾庆民, 郭凯, 周晓茂, 等. 新型算力网络架构设计与探讨[J]. 信息通信技术与政策, 2022, 48(11): 18-23.
JIA Q M, GUO K, ZHOU X M, et al. Design and discussion for new computing power network architecture[J]. Information and Communications Technology and Policy, 2022, 48(11): 18-23.

[17] ZHANG Y R, GENG H Z, SU L, et al. Research on security technology of computing force network service[J]. Mobile Communications, 2022, 46(11): 90-96.

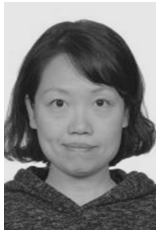
[18] ZHOU G F, LEI B. Computing service demand matching based on computing power identification in computing power network [J]. Frontiers of Data & Computing, 2022, 4(6):20-28.

[19] SHI J D, ZHU X R. Performance analysis of video-flow in mobile edge computing networks based on stochastic network calculus[C]//Proceedings of International Conference on Wireless and Satellite Systems. Cham: Springer, 2021: 599-610.

[20] JIN T J, LI W. An Intelligent scheduling and allocation method of big data computing resources based on computing power network [J]. Frontiers of Data & Computing, 2022, 4(6):29-37.

[作者简介]

潘洁（1978− ），女，中国移动通信集团设计院有限公司高级工程师、高级咨询设计师，主要研究方向为数据业务网、网络安全和信息安全。



叶兰（1979− ），女，中国移动通信集团有限公司工程师，主要研究方向计算机科学技术网络及数据安全。

张鹏飞（1977− ），男，中国移动通信集团有限公司高级工程师，主要研究方向为算力网络、云计算、网络及信息安全。

卜忠贵（1976− ），男，中国移动通信集团设计院有限公司正高级工程师，主要研究方向为移动通信核心网、算网安全等。