新型智算中心密钥分发设计方案

马爱良，张艳，张杨，彭华熹，张媞，李邦灵，杨凯，粟栗，何申
（中国移动通信有限公司研究院，北京 100053）

摘　要：新型智算中心作为融合算力和网络的新型基础设施，在提供灵活的算力服务的同时，其网络安全变得至关重要。在研究算力网络服务部署的基础上，分析了智算中心面向入算、算内、算间的不同安全诉求，构建密码应用工作流程，提出了基于国产密码算法的密钥分发机制，解决了智算中心不同环节、不同诉求的安全问题，为智算中心的规划建设提供参考。

关键词：智算中心；国产密码；密钥分发；密码应用
中图分类号：TP393，TN92
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2025158

Design scheme of key distribution for new intelligent computing center

MA Ailiang, ZHANG Yan, ZHANG Yang, PENG Huaxi, ZHANG Ti,
LI Bangling, YANG Kai, SU Li, HE Shen
Research Institute of China Mobile Communications Co., Ltd., Beijing 100053, China

Abstract: As a new infrastructure that integrated computing power and network, the new intelligent computing center not only provided flexible computing services, but also its network security had become crucial. Based on the study of the deployment of computing power network services, the different security requirements of the intelligent computing center for incoming, inside, and between computing networks were analyzed, a cryptographic application workflow was constructed, and a key distribution mechanism based on domestic cryptographic algorithms was proposed to solve the security problems of different links and demands of the intelligent computing center, it provids reference for the planning and construction of the intelligent computing center.

Key words: intelligent computing center, domestic cryptographic, key distribution, cryptographic application

收稿日期：2025−04−10；修回日期：2025−06−18
通信作者：马爱良，maailiang@chinamobile.com

0 引言

新型智算中心作为一种新型算力基础设施，不同于传统的云数据中心和超算中心，是以图形处理器（graphics processing unit，GPU）、人工智能（artificial intelligence，AI）加速卡等智能算力为核心、集约化建设的新型数据中心，为AI应用提供所需的算力服务、数据服务和算法服务。中国移动提出了新型智算中心技术体系架构[1]，指出新型智算中心具备从硬件设施到软件服务的端到端AI全栈环境，支撑超大规模、超高复杂度的模型训练和推理业务，最终赋能行业数智化转型升级。计算架构是智算中心的基础，决定了数据处理的方式和流程。在智算中心中，可采用分布式计算的方式将大量的计算任务分解成小的任务，再分配给多台计算机进行处理，以有效提高计算效率，并保证计算的稳定性和可靠性[2]；智算集群的无损网络[3]可以通过先进的技术和智能算法实现数据传输的高效率和无损，同时支持异构计算资源的整合和管理。而在设计智算中心这一算力基础设施的过程中，安全至关重要。经研究，安全加密与以太网物理层特性相融合来构建全新的以太网安全机制，可实现低时延、低开销、高吞吐、高安全的数据加密[4]；新型智算中心还需要实施严格的数据保护措施，包括采用加密技术，保护数据在传输和存储过程中的安全，以及实施访问控制策略，防止未授权访问[5]。

密码机制能够实现算力的身份鉴别、来源鉴别、信息存储与安全传输等多方面的应用需求。如何正确、有效地使用密码技术，充分发挥其在基础设施安全中的核心技术和基础支撑作用，关乎智算能力的安全以及智算中心的整体布局。本文根据智算中心的基本架构，分析其密码应用需求，提出了智算中心密钥分发设计方案。

1 智算中心技术体系

1.1 智算技术

当前，新型智算中心技术研究正处于快速发展阶段，呈现出异构融合、绿色低碳、服务智能化和安全可信等显著特征。

在硬件方面，国产算力芯片如华为昇腾910、寒武纪MLU370等通过架构创新实现了算力突破，其中昇腾910配合华为开源的MindSpore框架，代表昇腾系列的最强算力，显著提高了AI训练效率；在组网方面，由于算法模型巨量化发展，合适的并行方式是提升训练效率的关键，目前主要的3种并行方式为：数据并行、流水线并行、张量并行[6]；在算力互联方面，随着“东数西算”等国家重大工程的深入推进，智算中心与算力网络的网络互联对信息传输的时延、吞吐量和确定性有更高的要求，进而通过快速光交换技术可以实现高效、确定和安全的数据交换通道[7]。

然而，新型智算中心的研究仍面临若干挑战，如随着分布式训练任务规模的增加，GPU之间的通信时间可能成为瓶颈[8]、多元算力融合导致的编程复杂性[9]以及传统的通用算力、超级算力与智能算力兼容性问题[10]。未来应在芯片设计、编译优化、网络安全协议等基础领域持续突破。

1.2 密码安全

随着智算中心规模的扩大和计算场景的复杂化，密码安全面临前所未有的挑战与机遇。当前研究主要聚焦于隐私计算、抗量子密码迁移和动态信任管理三大方向，呈现算法创新与工程实践并重的发展态势。

（1）隐私计算：隐私计算是在保护隐私的前提下，实现数据的安全共享、互通、计算和建模。通过使用密码协议[11]、联邦学习[12]、差分隐私[13]、联邦学习[14]等技术手段有效降低数据泄露的风险，同时保证数据的可用性和分析价值，达

到对数据“可用而不可见”的目的。

（2）抗量子密码迁移：量子计算机基于量子叠加特性实现并行计算，计算能力较传统计算机有指数级提升，有可能高效率解决一些在经典计算模式下“指数”级困难的问题，从而对密码体系带来巨大威胁，抗量子密码算法部署研究已经迫在眉睫。

（3）动态信任管理：可信执行环境（trusted execution environment，TEE）通过硬件级隔离（如 Intel SGX、ARM TrustZone、AMD SEV）为动态信任管理提供安全可信的执行基础以及硬件级密钥存储，用于签名和加密信任评估结果，确保输入的设备行为数据来自可信传感器或签名模块。

1.3　基本架构

新型智算中心基本架构如图 1 所示。新型智算中心基本架构[1]由“三层两域”构成，分别是基础设施层、智算平台层、应用使能层、智算运维域和智算运营域。

其中，基础设施层提供计算、存储、网络等硬件资源；智算平台层作为资源管理的核心，提供裸金属、虚机和容器等多样化实例以及细粒度的资源池化能力，并在此之上搭建算力原生平台提供应用跨架构迁移能力；应用使能层集成行业主流 AI 开发框架以供应用开发调用。智算运维域主要负责对底层基础设施即服务（infrastructure as a service，IaaS）资源进行管理维护，确保系统的稳定运行；智算运营域对接外部客户，提供计量计费、访问、交易等界面，对内根据上层任务进行资源编排调度。

在实际应用中，智算中心布局可有效提升计算效率，保障数据安全以及推动智能技术的应用。

2　密码应用需求

智算中心网络场景的底层承载网络是以太网，为了应对日益严峻的数据安全挑战，须分析面向算内、入算和算间的不同安全诉求，研究适合的安全加密机制。新型智算中心部署场景如图 2 所示。

2.1　入算诉求

2.1.1　用户访问

算力用户接入智算中心时须进行身份鉴别，以避免用户非授权的访问和操作，保证只有授权的实体才能使用算力服务，抵抗算力非法调用。

2.1.2　关键数据

（1）鉴别信息：算力用户的身份鉴别口令传输和存储须进行机密性和完整性保护，以抵抗数

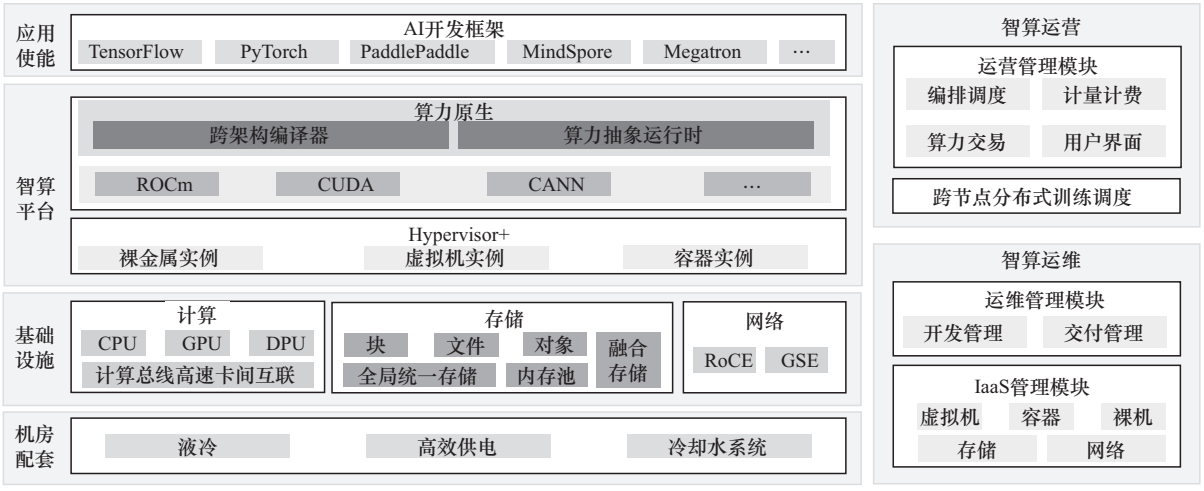


图 1　新型智算中心基本架构

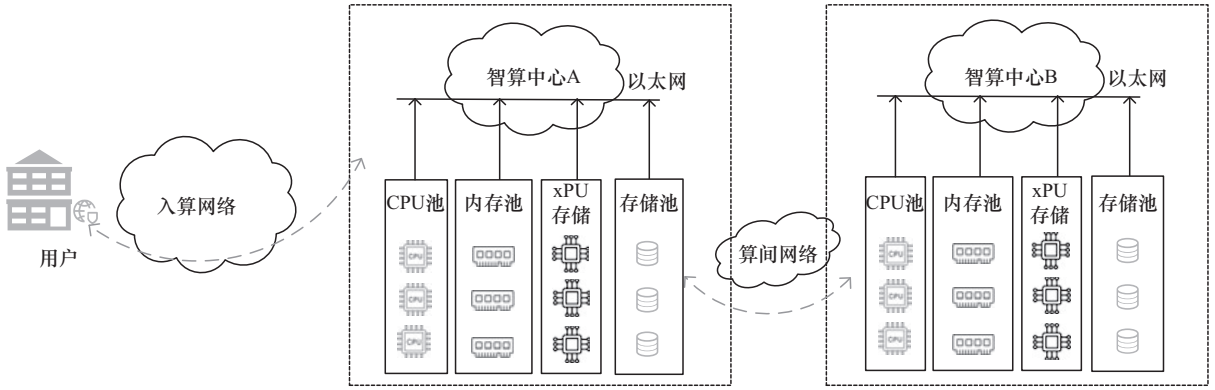


图2　新型智算中心部署场景

据在传输、存储、调度、计算过程中遭受泄露、篡改的风险。

（2）用户信息：算力用户的手机号、身份证号、企业编码等信息须进行机密性和完整性保护，以抵抗数据在传输、存储、调度、计算过程中遭受泄露、篡改的风险。

（3）AI模型训练：用户入算上载样本数据，算内及算间训练生成模型及参数、下载训练后的模型及参数，涉及敏感数据的频繁交互，存在泄露、窃听风险。

2.1.3　算力交易的抗抵赖

算力用户使用算力资源服务时，需要对算力交易进行原发和接收行为不可否认性的保护，以保证其可溯源性。

2.2　算内诉求

（1）关键数据：入算用户上传的样本数据、训练生成的模型和参数须进行加密存储，以抵抗计算过程中遭受泄露、篡改的风险。

（2）安全通信：搭建安全通信信道，保证算内各计算节点访问存储节点时网络通信的安全，以抵抗关键数据读取、写回、复制时泄露的风险。

2.3　算间诉求

搭建安全通信信道，保证算力网络之间通信的安全，以抵抗算间传输的模型和参数的泄露风险。

2.4　关键数据汇总

智算中心关键数据汇总见表1。

3　密钥分发设计方案

3.1　密码工作流程

智算中心可采用集团——大区的建设体系，由集团总部建立密钥管理中心（key management center，KMC）KMC/证书认证（certificate authentication，CA）双中心，每个大区建立一个智算中心，且每个智算中心建立配套的子密钥管理中心（sub-key management center，SKMC），由SKMC对智算中心的密钥进行直接管理。图3展示了新型智算中心密码工作流程，详细分析如下。

（1）用户的身份鉴别。入算用户通过用户名/口令和智能密码钥匙登录智算平台，智算平台身

表1　关键数据汇总

关键数据	描述	功能	需求
鉴别信息	算力用户口令	身份鉴别	机密性、完整性
用户信息	算力用户的手机号、身份证号、企业编码等	身份绑定	机密性、完整性
AI训练数据	算力用户样本数据	样本数据的上传、存储、读取、写入	机密性、完整性
	训练生成的模型	模型框架的下载、复制	机密性、完整性
	模型参数	算力网络之间的参数传递	机密性、完整性

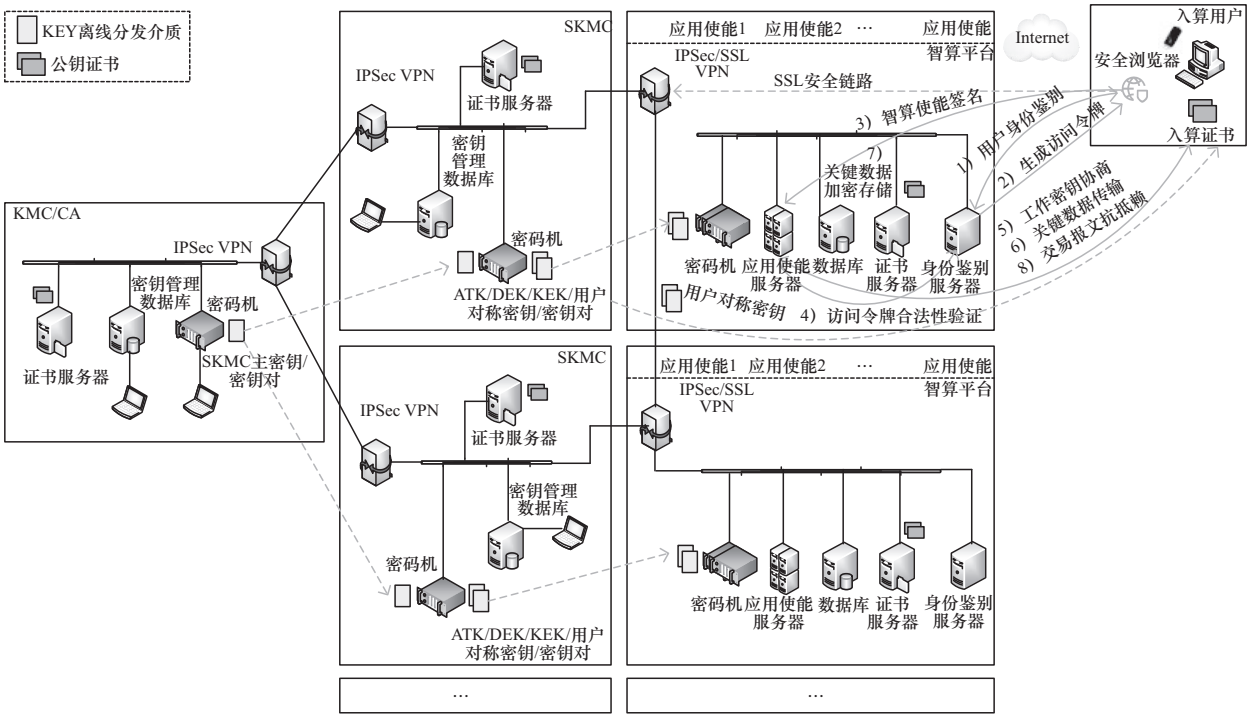


图3　新型智算中心密码工作流程

份鉴别服务器对用户的身份进行鉴别，以确保用户身份的真实性。

（2）生成访问令牌。智算平台的身份鉴别服务器根据智算使能（应用使能）的redirect_uri（回调地址）和用户信息生成访问令牌，并采用HMAC-SM3算法对其进行完整性保护。

（3）智算使能签名。智算使能使用自己的签名私钥对访问令牌进行签名。

（4）访问令牌合法性验证。首先，身份鉴别服务器使用智算使能的公钥证书对其签名进行验证，以鉴别为何种智能算力；然后，身份鉴别服务器对访问令牌进行HMAC-SM3验证，以确认访问令牌的合法性；最后，检查访问令牌与智能算力是否匹配。

（5）工作秘钥协商。生成工作密钥，以数字信封方式传递。当前的智能算力调用密码机生成会话密钥，通过入算用户的公钥证书进行加密后，传输给入算用户。

（6）关键数据传输。入算用户与智算能力之间采用工作密钥对传输的关键数据，如用户鉴别信息、用户信息、样本数据、参数、模型等进行加密保护，并实施签名。

（7）关键数据加密存储。智能算力数据库采用数据存储加密密钥对关键数据，如用户鉴别信息、用户信息、样本数据、参数、模型等进行加密存储或签名，确保重要数据不被泄露。

（8）交易报文的抗抵赖。入算用户申请或调用智能算力的报文采用私钥进行签名操作，确保使用智能算力服务行为的不可否认。

（9）通信信道安全：算内计算节点之间、计算节点与存储节点之间、智算中心之间等通信信道采用国密安全套接层协议（security socket layer，SSL）/互联网安全协议（Internet protocol security，IPSec）实现信道安全，确保算间、算内传输的关键数据不被泄露。

3.2　密钥层级结构

密钥体系包含对称密钥体系和非对称密钥体系两部分。智算中心涉及的对称密钥体系见表2，智算中心涉及的非对称密钥体系见表3。

表2 对称密钥体系

序号	密钥名称	功能
1	KMC主密钥	由密码机生成，用于分散SKMC主密钥
2	SKMC主密钥	由KMC主密钥和SKMC信息（包含智算中心信息）进行密钥分散生成，由KMC通过智能IC卡以离线方式分发给SKMC。用于智算能力ATK、智算平台DEK、智算平台KEK的分散
3	智算能力访问令牌完整性保护密钥（access token integrity protection key，ATK）	由SKMC与智算能力信息进行密钥分散生成，实现算力用户访问智算能力的二次认证，完整性保护算法是HMAC-SM3，通过智能IC卡以离线方式分发
4	智算能力数据加密密钥（data encryption key，DEK）	由SKMC与智算能力信息进行密钥分散生成，为两个对称密钥，用于智算中心对口令、用户信息等关键数据的加密存储和完整性保护，算法支持SM4、HMAC-SM3，通过智能IC卡以离线方式分发
5	智算能力密钥加密密钥（key encryption key，KEK）	由SKMC主密钥与智算能力信息进行密钥分散生成，用于智算平台DEK的加密保护，算法使用SM4，通过智能IC卡以离线方式分发
6	工作传输密钥（working transmission key，WTK）	即会话密钥，由每个智算能力（智算使能）与入算用户基于数字信封方式生成，用于保障智算中心与入算用户之间关键数据的传输安全，算法使用SM2、SM4、HMAC-SM3

表3 非对称密钥体系

序号	密钥名称	功能
1	KMC签名密钥对	对SKMC证书进行签发和验证
2	SKMC签名密钥对	对智算平台证书的签发和验证
3	智算平台的签名密钥对	对入算用户身份进行鉴别
4	智算使能签名密钥对	智算使能（应用使能）与入算用户之间算力交易报文的签名和验签
5	算力用户签名密钥对	智算使能（应用使能）与入算用户之间算力交易报文的签名和验签
6	算力用户加密密钥对	智算使能（应用使能）与入算用户之间工作密钥的生成

3.3 密钥分发体系

新型智算中心密钥分发体系如图4所示。算力网络智算中心的密钥分为对称密钥和非对称密钥。

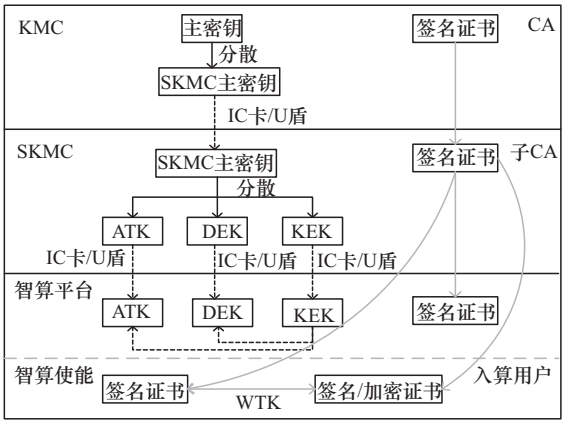


图4 新型智算中心密钥分发体系

密钥分发体系架构分析如下。

（1）KMC主密钥、CA签名密钥对

在集团层部署KMC、CA，产生KMC主密钥和CA签名密钥对及相应的签名证书。由KMC的服务器密码机保障其安全。

（2）SKMC主密钥、SKMC签名密钥对

在各大区部署SKMC和子CA，由KMC主密钥和SKMC信息进行密钥分散生成SKMC主密钥，并通过智能IC卡或U盾以离线方式分发给SKMC。同时生成SKMC签名密钥对，由CA签发SKMC的签名证书。由SKMC的服务器密码机保障其密钥的安全。

（3）智算能力ATK、智算平台签名密钥对

由SKMC与智算使能信息进行密钥分散生成，实现算力用户访问智算能力的二次认证，通过智能IC卡或U盾以离线方式分发。同时，在智算平台生成签名密钥对，并由子CA签发算力平台签名证书。由智能平台服务器密码机保障密钥安全。

（4）智算能力DEK、智算使能签名密钥对

由SKMC与智算使能信息进行密钥分散生成，为两个对称密钥，用于智算中心对口令、用户信息等关键数据的加密存储和完整性保护，通过智能IC卡或U盾以离线方式分发。同时在智算平台生成各个智算使能能力的签名密钥对，并由子CA签发签名证书。由智能平台服务器密码机保障密钥安全。

（5）智算能力KEK

由SKMC主密钥与智算使能信息进行密钥分散生成，用于智算平台DEK以及ATK的加密保护，通过智能IC卡或UKEY以离线方式分发。由智能平台服务器密码机保障密钥安全。

（6）WTK

WTK即会话密钥，由每个智算使能与入算用户基于数字信封方式生成，当前的智算使能调用密码机生成会话密钥，通过入算用户的公钥证书进行加密后，传输给入算用户，用于智算中心与入算用户之间关键数据的传输安全。工作密钥一次一密。

（7）入算用户的签名密钥对、加密密钥对

用户进行智算平台注册时，由大区子CA进行签名证书和加密证书的签发。签名密钥对用于算力交易报文的签名和验签；加密密钥对用于数字信封的生成。由入算用户保障密钥的安全。

3.4　方案分析

3.4.1　设计原则

本方案设计遵循多重原则。安全性原则是核心，通过采用国产密码算法、构建多层次密钥体系以及实施严格的身份鉴别机制，确保智算中心各环节数据的机密性、完整性和可用性。以对称密钥体系中的智算能力DEK为例，采用SM4和HMAC-SM3算法，分别保障数据加密存储的机密性和完整性，有效防止数据泄露和篡改。实用性原则体现在满足智算中心复杂业务场景需求上，无论是用户入算、算内数据处理还是算间交互，密钥分发机制都能无缝适配，确保业务流程顺畅。可扩展性原则为智算中心未来的规模扩张和功能升级奠定基础，集团–大区的建设体系以及灵活的密钥分散和管理方式，便于新增智算中心或扩展业务时，轻松进行密钥体系的调整和扩展。

3.4.2　区域划分

从架构层面来看，集团建立KMC/CA双中心，大区设立智算中心及配套SKMC的架构，实现了密钥管理的分层分级，既保障了集中管控，又赋予了本地管理的灵活性。这种架构在管理效率和安全性之间取得了平衡，避免了单一管理中心带来的管理负担过重和潜在安全风险。在密钥生成和分发方面，基于不同层级信息进行密钥分散的方式，使得每个密钥都与特定的环境和功能紧密关联，增强了密钥的针对性和安全性。例如，智算能力ATK由SKMC与智算能力信息生成，确保了对特定智算能力访问的有效验证和保护。

3.4.3　冗余设计

针对单点失效问题，方案通过多中心架构和冗余设计进行防范。KMC/CA双中心相互备份，当一个中心出现故障时，另一个中心可迅速接管工作，保障密钥管理的连续性。SKMC在各大区的分布式部署，也降低了某个节点故障导致整个智算中心密钥管理瘫痪的风险。对于主密钥存储，可引入安全硬件，例如，专业的加密芯片或可信计算模块。这些硬件具备强大的加密和防护能力，能够有效防止主密钥被非法获取和篡改。同时，门限密钥分享技术也可应用于主密钥管理，将主密钥分割成多个份额，只有在满足一定数量份额的情况下才能恢复主密钥，进一步提升了主密钥的安全性。

4　结束语

智算中心作为提供算力和网络深度融合、一体

化服务的新型基础设施，能够提供灵活、按需的AI算力服务体验。本文根据智算中心面向入算、算内、算间网络的不同安全诉求，分析了密码应用需求，梳理了智算中心密码工作机制，并设计了对称/非对称的双层密钥管理体系，为构建智算中心的整体安全架构提供参考。

参考文献：

[1] 中国移动通信集团有限公司.中国移动NICC新型智算中心技术体系白皮书[R]. 2023.
China Mobile Communications Group Corporation Limited. China Mobile newintelligent computing centertechnology framework white paper[R]. 2023.

[2] 钟歆. 新型智算中心核心技术布局分析[J]. 低碳世界, 2024, 14(11): 184-186.
ZHONG X. Analysis of core technology layout of new intelligent computing center[J]. Low Carbon World, 2024, 14(11): 184-186.

[3] 孙长秋, 杜长斌, 高肇明, 等. 无损网络技术在智算中心的应用研究[J]. 通信管理与技术, 2024(5): 30-33.
SUN C Q, DU C B, GAO Z M, et al. Research on the application of lossless network technology in intelligent computing center[J]. Communications Management and Technology, 2024(5): 30-33.

[4] 段晓东,李婕妤,程伟强,等.面向智算中心的新型以太网需求与关键技术[J].电信科学,2024,40(6):146-159.
DUAN X D, LI J Y, CHENG W Q.Challenges and key technologies of new Ethernet for intelligent computing center[J]. Telecommunications Science,2024,40(6):146-159.

[5] 段晓东, 程伟强, 王瑞雪, 等. 面向新型智能计算中心的全调度以太网技术[J]. 中兴通讯技术, 2023, 29(4): 57-63.
DUAN X D, CHENG W Q, WANG R X, et al. Global scheduling Ethernet for new intelligent computing center[J]. ZTE Technology Journal, 2023, 29(4): 57-63.

[6] 中国移动通信研究院.面向AI大模型的智算中心网络演讲白皮书[R].2023.
China Mobile Research Institute. White paper on intelligent computing center network evolution for AI large models[R]. 2023.

[7] 尹林, 王富, 王小龙, 等. 面向算力互联的快速光交换技术研究. 光通信研究[J]. 2024(5): 50-57.
YIN L, WANG F, WANG X L, et al. Fast switching for computing-gcwer interconnects[J]. Study on Optical Communications, 2024(5): 50-57.

[8] ZHANG Z,CHANG C K,LIN H B,et al."Is network the bottleeneck of distributed training?" [J]. arXiv preprint, 2020, arXiv: 2020:2006.10103.

[9] 王小宁, 卢莎莎, 吴璨, 等. 基于高性能计算环境的HPC算力编程模式[J]. 数据与计算发展前沿, 2022, 4(5): 33-41.
ZHAO X N, LU S S, WU C, et al. HPC computing power programming garadigm based on CNGrid[J]. Frontiers of Data & Computing, 2022，4(5): 33-41.

[10] 赵栖平, 丁飞, 王诗怡, 等. 算力中心云服务架构与关键技术研究[J]. 信息通信技术与政策, 2025, 51(2): 30-39.
ZHAO Q P, DING F, WANG S Y, et al. Research on cloud service architecture and key technologies of computing power centers[J]. Information and Communications Technology and Policy, 2025, 51(2): 30-39.

[11] FENG Q, HE D B, ZEADALLY S, et al. A survey on privacy protection in blockchain system[J]. Journal of Network and Computer Applications, 2019, 126: 45-58.

[12] 王鑫, 黄伟口, 孙凌云. 跨机构联邦学习的激励机制综述[J]. 计算机科学, 2024, 51(3): 20-29.
WANG X, HUANG W K, SUN L Y. A Survey of incentive mechanisms for cross-institutional federated learning[J]. Computer Science, 2024, 51(3): 20-29.

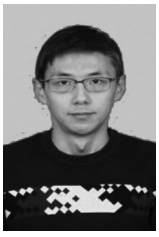
[13] 熊平, 朱天清, 王晓峰. 差分隐私保护及其应用[J]. 计算机学报, 2014, 37(1): 101-122.
XIONG P, ZHU T Q, WANG X F. A survey on differential privacy and applications[J]. Chinese Journal of Computers, 2014, 37(1): 101-122. .

[14] 肖雄, 唐卓, 肖斌, 等. 联邦学习的隐私保护与安全防御研究综述[J]. 计算机学报, 2023, 46(5): 1019-1044.
XIAO X, TANG Z, XIAO B, et al. A survey on privacy and security issues in federated learning[J]. Chinese Journal of Computers, 2023, 46(5):1019-1044.

[作者简介]

马爱良（1982– ），女，中国移动通信有限公司研究院工程师，主要研究方向为通信网商用密码应用、数据安全、算力网络安全等。

张艳（1984– ），女，中国移动通信有限公司研究院高级工程师，主要研究方向为网络与信息安全、数据安全、量子密码等。



张杨（1983– ），男，中国移动通信有限公司研究院高级工程师，主要研究方向为网络与通信安全、后量子密码等。

彭华熹（1978– ），男，博士，中国移动通信有限公司研究院高级工程师，主要研究方向为网络与通信安全、密码应用等。

张媞（1987– ），女，中国移动通信有限公司研究院高级工程师，主要研究方向为网络通信安全、可信计算等。

李邦灵（1990– ），女，中国移动通信有限公司研究院安全技术研究所工程师，主要研究方向为网络与通信安全、商用密码等。

杨凯（1981– ），男，中国移动通信有限公司研究院安全技术研究所副所长，主要研究方向为网络与通信安全、商用密码、区块链、算力网络等。

粟栗（1981– ），男，博士，中国移动通信有限公司研究院安全技术研究所副所长，主要研究方向为网络与通信安全、量子密码、区块链、算力网络等。

何申（1980– ），男，博士，中国移动通信有限公司研究院安全技术研究所所长、正高级工程师，主要研究方向为网络与通信安全、量子密码、区块链、算力网络等。