第二届商用密码创新应用主题大赛

揭榜赛赛题公布

中国互联网发展基金会、中国互联网投资基金、北京市丰台区人民政府共同举办 2025 中国互联网发展创新与投资大赛（商密）暨第二届商用密码创新应用主题大赛（以下简称 “大赛”），大赛设置创新赛及揭榜赛，组委会通过命题征集、专家评审、综合遴选，确定本届大赛揭榜赛赛题，现予以公布。

参赛团队在揭榜赛报名系统提交信息时，在项目名称前标注赛题序号。（如：赛题1—XXX项目解决方案）

一、赛题 1：大模型参数与数据的密码保护

（1）背景与需求分析

随着大模型在政务、金融、能源、医疗等重点行业广泛应用，私有化部署成为保障数据主权与合规要求的主流模式。在实际部署过程中，模型通常运行于客户或第三方维护的算力基础设施之上，模型提供方对底层操作系统及硬件环境缺乏完全控制能力。在具备 root 权限或物理访问能力的情况下，模型参数文件及相关运行数据可能被直接复制、篡改或非法导出，模型资产面临泄露和滥用风险，严重影响模型厂商的知识产权与商业利益。同时，大模型推理系统对算力、显存及并发能力要求较高，运行过程涉及模型加载、内存映

射、跨进程调用等环节，数据在存储与运行态之间频繁流动，传统基于文件权限或简单加密的防护方式难以覆盖运行全过程。

现有技术方案存在明显局限：一是访问控制机制难以防范高权限越权行为；二是可信执行环境、多方安全计算等技术在高算力场景下存在性能损耗与工程复杂度问题；三是缺乏针对模型参数本身的商用密码保护与完整性验证机制，难以防止权重被复制或替换。

因此，亟需面向大模型私有化部署场景，研究兼顾安全性与性能的模型资产保护技术，实现模型可控运行与有效防导出，推动商用密码在人工智能领域的落地应用。

（2）具体内容与关键要求

围绕大模型私有化部署环境中“模型资产保护与数据主权控制”关键问题，构建基于商用密码技术的整体安全解决方案。在不改变现有业务系统使用方式与算力架构的前提下，实现模型与数据可正常运行、可合法调用，但无法被非法复制、导出或篡改的安全目标。即在真实运行环境中达到“功能等价、性能可接受、资产不可转移”的理想效果。

重点解决模型参数在本地环境中的加密存储与受控加载、运行过程完整性验证、数据访问授权控制及导出审计问题，防止模型权重被复制、替换或植入恶意代码，同时保障合法业务流程不受影响。

基于 SM2、SM3、SM4 等商用密码算法构建模型与数据

保护机制，形成统一密钥管理与授权体系；支持 GPU 及其他主流算力加速卡，兼容主流推理框架与现有应用程序，无需大规模改造即可部署；在高并发推理场景下性能损耗比例 ⩽ 10%；支持多租户环境下的分级授权、远程控制与审计追踪；建立可验证的运行信任机制，实现模型加载与运行过程完整性度量。

（3）提交成果

提交安全技术方案、可演示原型系统及性能与安全测试报告，验证模型防导出与受控运行能力。

形成适用于大模型私有化部署场景的模型资产安全保护解决方案 1 套，完成关键安全机制与密码应用集成，实现可部署的工程化原型系统。

二、赛题 2：数字化系统中基于法定证件的实名授权密码技术应用

（1）背景与需求分析

当前，构建以居民身份证等法定证件为信任根的数字身份认证与核验体系已成为数字中国建设的重要内容。对于金融、通信、政务等强实名业务场景，国家提出了基于国密算法合规地映射权威法定身份与虚拟身份技术关联要求。但目前政企数字化系统并未规范系统用户实名注册机制。为强化数字化系统用户身份管理，亟需构建数字化系统实名认证与

核验体系，防范身份冒用、越权访问等安全风险。

传统身份认证技术依赖认证介质、密码口令、网络服务、人脸特征、自主注册等多因素认证方式，存在内部认证介质易丢失、密码口令易泄露、人脸特征易伪造、注册信息不真实等安全挑战。

系统中传统身份认证的安全挑战一是内部管理用户口令泄露、人脸伪造、信息不准确等因素，导致关键基础设施运营出现重大系统性风险。二是缺少基于法定证件的注册方式，无法确保身份的唯一性与权威性。三是后台管理的人员库隐私信息易泄露、危及组织安全。

因此亟需探索一种基于国密算法、以权威法定身份为信任根、融合高安全生物特征识别、不依赖网络的可信数字身份认证与核验系统。

（2）具体内容与关键要求

研发基于法定证件与高安全生物特征融合的可信身份认证系统。攻克在线、离线、单机等环境下“法定证件—系统用户”安全映射技术，实现高安全等级身份鉴权与数据加密。

实名注册：用户注册以法定证件为信任源，结合国密算法与脱敏身份信息进行密码学绑定，构造可信数字身份。

身份鉴权：支持基于可信数字身份、法定证件、指纹识别等多因素的分级身份鉴权。

隐私保护：原始法定证件信息仅在本地安全硬件环境中

处理，严禁明文传输法定证件身份信息，确保真实身份信息“可用不可见”。

数据安全：敏感业务数据支持基于可信身份的访问控制和全生命周期加密。

（3）提交成果

提供面向数字化系统的基于法定证件的实名授权密码技术原型系统或设计方案。

三、赛题 3：水利物联网边缘安全传输与可信接入一体化平台

（1）背景与需求分析

物联网边缘安全防护系统是智慧水利关键设施运行的重要保障，通过对水利多源设备（水位、流量、墒情等传感器）的数据进行安全采集与加密回传，实现边缘侧集中管理与可信传输。随着物联网向偏远灌区、山区水文站等资源受限区域延伸，边缘设备需在低功耗、弱带宽、供电不稳定的条件下执行安全任务，并依托 MQTT、Modbus 等轻量协议实现监测与回传。

在水利资源受限环境下，物联网终端往往计算能力弱、存储空间小，难以承载传统 SSL/TLS 等复杂协议。现有 SSL VPN 产品亦不支持 UDP 场景的 DTLCP 协议，无法满足水利物联网低延迟、高并发的国密传输需求，易成为攻击入口，威胁整

个水利物联网系统安全。而水利边缘监测数据作为调度、防汛、灌溉决策的基础，其完整性、真实性与机密性至关重要，一旦遭篡改或窃取，可能引发水旱灾害、农田损毁等系统性风险。

因此，需面向水利领域低功耗物联网设备与受限边缘节点开展密码应用创新，研究轻量级国密算法适配、DTLCP/MQTT 安全传输协议及设备可信认证技术，通过轻量化商用密码方案，解决水利设备动态认证、数据安全传输与合规低成本改造等问题，切实保障智慧水利关键基础设施物联网系统安全运行。

（2）具体内容与关键要求

聚焦智慧水利物联网边缘侧安全痛点，围绕“边缘安全传输与可信接入一体化”，研发适配偏远灌区、山区水文站等受限场景的轻量化边缘安全解决方案，解决终端安全接入、数据加密传输及合规改造问题，保障智慧水利基础设施安全运行。

1）适配水利低功耗、弱带宽场景，兼容 MQTT、Modbus 轻量协议，支持各类水利终端接入;

2）核心技术：集成轻量级国密算法，支持 DTLCP 国密传输协议，解决传统协议适配差、不支持 UDP 场景的问题;

3）合规便捷：符合商用密码标准，方案轻量化、部署便捷，适配老旧系统低成本改造。

（3）提交成果

研发适配水利场景的边缘安全传输与可信接入一体化解决方案 1 套，完成核心算法与协议适配，形成可直接部署的轻量化产品原型（包含轻量级边缘加密终端、安全网关、管理中心，演示加密传输、MQTT 设备接入认证、证书管理等核心功能，验证方案可行性），满足水利受限场景安全防护与合规需求。

四、赛题 4：铁路线路环境监测轻量级密码应用

（1）背景与需求分析

铁路线路环境安全监测系统实现铁路线路环境的安全集中监测，随着铁路网络不断向偏远及自然环境复杂地区延伸，安全监测设备须在缺乏电力和网络覆盖的区域执行监测任务，采取基于窄带自组网网络传输实现数据回传和安全集中监测。在这种数据回传受限的通信条件下，传感节点大多计算能力弱、存储空间小，难以直接承载复杂的安全协议，易成为网络攻击的薄弱环节，进一步威胁监测数据以及整个监测网络的系统安全。然而，监测数据作为影响行车安全决策的基础，其完整性、真实性与机密性至关重要，一旦数据在传输中被篡改、窃取或伪造，将直接误导风险研判，甚至可能引发系统性安全风险。因此，需针对基于低功耗监测设备、窄带自组网网络的安全监测系统进行网络安全设计，研究轻量级网络动态密钥生成、安全传输协议及可信认证技术，通过轻量化商用密码创新应用解决监测设备动态接入认证、

监测数据安全传输等问题，保障铁路列车运行安全。

（2）具体内容与关键要求

研究轻量化网络动态密钥生成、安全传输协议以及可信认证技术，针对低功耗监测设备与窄带自组网安全监测系统，解决设备动态接入认证、数据安全传输等问题。

在传感节点计算能力弱、存储空间小的条件下实现高效且轻量化的动态密钥生成，确保密钥生成过程安全可靠；基于轻量化商用密码算法，实现设备动态接入认证，以及传输数据的机密性、完整性和真实性；适应窄带自组网通信条件，保证数据回传的稳定性与实时性。

（3）提交成果

构建轻量化网络动态密钥生成、安全通信协议与可信认证技术解决方案，完成可运行的算法原型，在保障安全性的前提下，具备较低的系统空间、计算资源以及能耗。

五、赛题 5：面向教育领域的多校联合密码攻防实训资源共享统筹

（1）背景与需求分析

随着教育数字化转型的加速推进，网络安全人才缺口日益扩大，传统的单校单点式实训模式已难以满足实战化人才培养需求。多校联合开展攻防实训成为提升学生综合能力的关键路径，然而当前各高校的实训资源（如靶场环境、漏洞

库、攻防工具、师资课程等）多处于“孤岛”状态，缺乏统一的共享机制与高效的统筹平台。这导致优质资源利用率低、重复建设严重、跨校实训协同困难，难以形成规模化、体系化的攻防演练合力。

因此，亟需构建一个面向教育领域的多校联合密码攻防实训资源共享平台。该平台需突破多源异构资源的标准化接入、分布式资源的动态调度、跨域身份认证与安全隔离等关键技术，设计高可用、可扩展的平台架构。通过实现资源的集中纳管与按需分配，不仅能够盘活存量密码实训资源，还能支撑大规模、高仿真的联合攻防演练，从而有效解决教育资源分布不均与实战训练环境匮乏的问题，为国家网络安全战略输送具备实战经验的复合型人才。

（2）具体内容与关键要求

面向教育行业密码安全人才培养与资源统筹需求，建设全国统一、分级部署、资源共享、利旧复用的教育行业密码攻防统筹平台，实现以下核心目标:

1）资源统筹共享：整合全国院校密码攻防靶场、实训环境、工具库、场景库、攻防成果、教学案例，实现跨校、跨区域资源统一调度与共享复用;

2）低成本赋能院校：依托平台集中建设能力，各院校无需单独投入资金搭建攻防平台，通过账号权限即可使用平台资源开展教学、实训、演练;

3）支撑教学科研竞赛：满足密码学院、网络安全学院

日常教学实训、攻防演练、学科竞赛、科研创新、成果交流等全场景需求;

4）行业统一治理：支持教育部层面统一管理、数据汇聚、态势展示、成果推广，形成教育行业密码攻防能力底座与交流生态;

5）合规与安全可控：平台符合商用密码应用、网络安全等级保护、数据安全等合规要求，保障平台及共享资源安全可控。

（3）提交成果

具备资源池化管理、攻防场景编排、实训教学支撑、竞赛组织、成果上传分享、态势大屏、权限分级管控等核心能力;

整体建设与运维成本可控，院校端零/低成本接入，实现“一次建设、全行业复用”;

支持快速部署、分级试点、逐步推广，可先在密码学院、网络安全学院集中的院校先行试点，再向全国教育系统复制。

六、赛题 6：商用密码在等保框架下对工作秘密的深度防护与协同治理新范式

（1）背景与需求分析

当前，工作秘密信息作为机关企事业单位运行的关键资产，其防护面临新的挑战：一方面，传统“边界防御”模式

难以应对内部泄露与高级持续性威胁；另一方面，密码应用与保密管理体系存在“两张皮”现象，技术手段与管理制度脱节，导致防护效能大打折扣。

在此背景下，亟需构建“商密驱动、体系融合”的深度防护新范式。这要求打破密码技术与等级保护的壁垒，将商用密码能力内嵌至等保技术框架的各个层级，推动“价值共生”的协同治理机制，通过制度创新将密码应用的合规性要求转化为保密管理的内生动力。探索如何通过技术与管理的双向赋能，建立一个以商用密码为基石、等级保护为骨架、工作秘密信息防护为目标的动态、闭环的安全治理体系。

（2）具体内容与关键要求

构建一个以商用密码为技术底座、深度融合等级保护框架的工作秘密信息防护体系。打破传统安全域的壁垒，实现密码保障体系与等级保护技术体系的架构级融合，建立“技术－管理”双轮驱动的协同治理机制，将密码应用的合规性要求嵌入到工作秘密信息防护体系的规划建设整改与运维流程中。

支持密码资源的弹性调度，具备可扩展性；

充分考虑基于零信任架构的身份鉴别与访问控制技术，利用动态口令、数字证书等手段强化身份真实性；

针对工作秘密数据，结合水印技术，实现数据流转的可追溯与防泄露；

能够充分结合等级保护和工作秘密的防护要求，保持技

术应用的一致性。

（3）提交成果

提交技术方案、可演示原型系统等，可以通过模拟验证，证明该范式能有效提升工作秘密信息防护合规性、安全性。

其他说明:

大赛报名及更多详细信息见官网：www.cciaccn.com

本次大赛报名截止日期为 2026 年 4 月 10 日

第二届商用密码创新应用主题大赛组委会

2026 年 3 月 16 日