天津商密

总第五期

主办单位：天津市商用密码行业协会　www.tccia.org.cn　2024年01期

国家密码管理局公告（第45号）
国家密码管理局公告（第46号）

南开大学数据与智能系统安全教育部重点实验室揭牌
天津市国家密码管理局丛局出席并致辞

天津市商用密码行业协会第三期密码应用工作培训班成功举办

天津市商用密码行业协会
Tianjin Commercial Cryptography Industry Association

天津商密

主办　天津市商用密码行业协会

总第五期

关注天津商密

2024 年是《密码法》实施的第五年。五年来，密码应用保障领域全面拓宽，产业生态持续繁荣，科技创新成果显著，社会公众密码安全意识进一步增强，密码在维护国家安全、促进经济社会发展、保护人民群众利益中的作用日益凸显。为贯彻落实《密码法》，国家相关部门在 2023 年相继出台了新修订的《商用密码管理条例》、《商用密码检测机构管理办法》、《商用密码应用安全性评估管理办法》以及多项商用密码产业政策，为我们加强新时代密码工作提供了强大的政策武器。

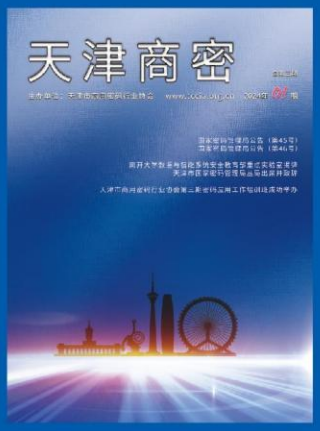
密码是国之重器，是保障网络与信息安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段，它可以提供机密性、完整性、真实性、抗抵赖性、可控性等一系列重要安全服务和保障，在网络安全防护中具有不可替代的重要作用。信息化、网络化、数字化高度发达的今天，密码技术已经渗透到了社会生产生活各个方面，重要网络和信息系统、关键信息基础设施、数字化平台都离不开密码的保护。5G、物联网、云计算、大数据、人工智能、区块链、量子技术、数字经济等新技术新业态都与密码紧密融合。密码与老百姓日常生活也息息相关，身份认证、消费支付、网络交易、个人信息保护、财产保护等，背后都有密码在发挥着作用，密码的应用可谓无处不在，有力维护了社会正常运转和交易秩序，保障了公民、法人和社会组织的合法权益。

作为天津市商用密码行业协会副会长单位，天津国芯科技有限公司多年来坚持在商用密码科技创新和技术研发领域深耕细作，认真学习和领会密码法律法规精神，积极抓住当前商用密码发展的良好机遇，推出了搭载商用密码的“云”“边”“端”系列化安全芯片及模组，已成为国内领先的信创和信息安全芯片及模组研发企业。与此同时，公司持续瞄准科技前沿，在量子技术、人工智能、区块链、智能网联汽车等新兴领域，积极进取，提前布局，争取在提升上述新兴领域密码服务保障能力的过程中，提供国芯方案及国芯智慧，为密码产业的高质量发展保驾护航。

天津市商用密码行业协会 副会长
天津国芯科技有限公司 总经理 艾方

contents

目录



《天津商密》2024年01期

主办单位
天津市商用密码行业协会

编委
艾　方　李忠献　刘哲理
李梦菲　陈旭杨　汪　定
张俊辉　张秋璞　胡双喜
按照姓氏笔画排序

主编
张俊辉

执行主编
胡双喜

责任编辑
陈旭杨　李梦菲

美术编辑
陈旭杨

协会地址
天津市河西区泰山路 6 号

邮编
300210

联系方式
15822166181
13512981809

关于做好《商用密码检测机构管理办法》和《商用密码应用安全性评估管理办法》实施工作的公告

2023 年 9 月 26 日，我局公布《商用密码检测机构管理办法》（国家密码管理局令第 2 号）和《商用密码应用安全性评估管理办法》（国家密码管理局令第 3 号），自 2023 年 11 月 1 日起施行。为做好相关工作衔接，现就有关事项公告如下。

一、按照《商用密码检测机构管理办法》第七条有关规定，现委托各省、自治区、直辖市密码管理部门，新疆生产建设兵团密码管理部门负责受理本行政区域的商用密码检测机构资质申请，负责对申请材料进行形式审查，出具受理通知书或者不予受理通知书。自2023年11月1日起，有关申请机构可以参照《商用密码检测机构资质申请表（模板）》（见附件）向所在地省级密码管理部门提交书面申请材料。

二、按照《商用密码检测机构管理办法》第三条有关规定，有意愿继续从事商用密码应用安全性评估业务的商用密码应用安全性评估试点机构，应当于2023 年 11 月 30 日前提交商用密码检测机构资质申请。对提交申请的商用密码应用安全性评估试点机构依法实施资质认定后，商用密码应用安全性评估试点工作将正式结束。未经认定，任何单位不得面向社会开展商用密码应用安全性评估业务。

特此公告。

附件：商用密码检测机构资质申请表

国家密码管理局

2023 年 10 月 31 日

转载自国家密码管理局官方网站

国家密码管理局公告
（第45号）

现发布 GM/T 0126-2023《HTML 密码应用置标语法》等 25 项密码行业标准，自 2024 年 6 月 1 日起实施，具体标准编号及名称如下：

GM/T 0006-2023 密码应用标识规范

GM/T 0009-2023 SM2 密码算法使用规范

GM/T 0010-2023 SM2 密码算法加密签名消息语法规范

GM/T 0011-2023 可信计算 可信密码支撑平台功能与接口规范

GM/T 0014-2023 数字证书认证系统密码协议规范

GM/T 0015-2023 数字证书格式

GM/T 0016-2023 智能密码钥匙密码应用接口规范

GM/T 0017-2023 智能密码钥匙密码应用接口数据格式规范

GM/T 0018-2023 密码设备应用接口规范

GM/T 0019-2023 通用密码服务接口规范

GM/T 0020-2023 证书应用综合服务接口规范

GM/T 0021-2023 动态口令密码应用技术规范

GM/T 0022-2023 IPSec VPN 技术规范

GM/T 0023-2023 IPSec VPN 网关产品规范

GM/T 0024-2023 SSL VPN 技术规范

GM/T 0025-2023 SSL VPN 网关产品规范

GM/T 0026-2023 安全认证网关产品规范

GM/T 0033-2023 时间戳接口规范

GM/T 0126-2023 HTML 密码应用置标语法

GM/T 0127-2023 移动终端密码模块应用接口规范

GM/T 0128-2023 数据报传输层密码协议规范

GM/T 0129-2023 SSH 密码协议规范

GM/T 0130-2023 基于 SM2 算法的无证书及隐式证书公钥机制

GM/T 0131-2023 电子签章应用接口规范

GM/T 0132-2023 信息系统密码应用实施指南

以下 18 项密码行业标准自 2024 年 6 月 1 日起予以废止：

GM/T 0006-2012 密码应用标识规范

GM/T 0009-2012 SM2 密码算法使用规范

GM/T 0010-2012 SM2 密码算法加密签名消息语法规范

GM/T 0011-2012 可信计算 可信密码支撑平台功能与接口规范

GM/T 0014-2012 数字证书认证系统密码协议规范

GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范

GM/T 0016-2012 智能密码钥匙密码应用接口规范

GM/T 0017-2012 智能密码钥匙密码应用接口数据格式规范

GM/T 0018-2012 密码设备应用接口规范

GM/T 0019-2012 通用密码服务接口规范

GM/T 0020-2012 证书应用综合服务接口规范

GM/T 0021-2012 动态口令密码应用技术规范

GM/T 0022-2014 IPSec VPN 技术规范

GM/T 0023-2014 IPSec VPN 网关产品规范

GM/T 0024-2014 SSL VPN 技术规范

GM/T 0025-2014 SSL VPN 网关产品规范

GM/T 0026-2014 安全认证网关产品规范

GM/T 0033-2014 时间戳接口规范

国家密码管理局

2023 年 12 月 4 日

转载自国家密码管理局官方网站

国家密码管理局公告
（第46号）

现发布《国家密码科学基金首批面上项目申报指南》和《国家密码科学基金首批重点项目申报指南》。

特此公告。

附件：1. 国家密码科学基金首批面上项目申报指南

2. 国家密码科学基金首批重点项目申报指南

国家密码管理局

2023 年 12 月 12 日

国家密码科学基金
首批面上项目申报指南

为落实“十四五”期间密码科技创新有关部署安排，聚焦国际密码科技前沿，支持密码科研团队开展密码理论和共性关键技术探索，努力实现基础性、前沿性、前瞻性研究原创成果的重大突破，进一步增强密码领域原始创新能力，培养密码领域人才和团队，现发布国家密码科学基金首批面上项目申报指南。

一、支持计划

面上项目计划对 11 个密码研究方向进行支持，项目执行期为 3 年，经费额度为 20-40 万元 / 项，每个项目应由 1 家单位独立承担。

（一）抗量子公钥密码理论与技术

研究内容：研究抗量子公钥密码实用化设计技术；研究抗量子公钥密码底层困难问题的新型量子求解算法及量子安全强度评估模型；研究现有主流抗量子公钥密码算法的安全快速软硬件实现技术；研究抗量子公钥密码认证体系及抗量子公钥密码迁移技术。

（二）密码学困难问题求解算法

研究内容：研究有限域上代数方程组求解问题、纠错码译码问题等现有密码学困难问题的新型经典或量子求解算法；研究 SAT/MILP/CP 等问题的新型求解算法；探索新的困难问题并给出其密码学应用。

（三）身份认证与访问控制密码关键技术

研究内容：研究实用化非交互零知识证明、具有附加功能的数字签名、分布式数字签名、属性密码、可搜索加密、可更新加密等身份认证与访问控制密码技术，提出其在大数据细粒度访问控制、数据库安全防护、云存储、区块链等场景下的密码方案。

（四）新型应用场景下的密码协议设计

研究内容：研究物联网应用场景下抗多用户合谋攻击的大规模对称密钥分发方法；研究高安全高可靠集群通信应用场景下基于预共享秘密的组播密钥方案设计技术；研究低可靠集群通信应用场景下丢失容忍的组播密钥方案设计技术；研究带宽极窄、密码同步资源受限通信条件下的密码协议设计。

（五）量子计算模型下对称密码的设计与分析

研究内容：研究量子计算模型下对称密码的设计方法和可证明安全理论；研究基于量子计算的对称密码分析方法，针对典型对称密码算法或结构，提出更优的通用量子攻击或专用量子攻击；研究对称密码量子电路的综合与优化方法，分析典型对称密码算法

量子电路的宽度、深度和门复杂度等指标。

（六）新型对称密码组件与算法的设计和分析

研究内容：研究新型对称密码组件、结构和算法的设计与分析，包括但不限于：16 比特及以上 S 盒和 128 比特及以上线性扩散层等大规模组件；高效非线性序列生成器；加解密计算效率不对等非线性组件；512 比特及以上安全强度分组密码；可调分组密码；自同步序列密码；动态对称密码；适用于全同态加密、零知识证明或安全多方计算的对称密码；对称密码密钥延展模式；认证加密、纠错加密等多功能对称密码。

（七）密码学与人工智能融合关键技术

研究内容：研究基于人工智能技术的密码分析技术及其可解释性问题；研究基于机器学习的对称密码组件和结构设计方法；针对人工智能应用中数据或模型的机密性、完整性、隐私性等需求，提出基于密码技术的高效解决方案。

（八）量子密码理论与技术

研究内容：研究量子单向函数构造和量子基础密码原语设计理论；研究量子密钥分发（QKD）协议实现安全模型和测试评估技术；研究测量设备无关类、双场类、连续变量类等 QKD 协议；研究量子网络中继节点可信动态认证技术；研究量子随机数理论安全分析模型和安全评估准则；研究器件无关、半器件无关量子随机数生成技术；研究高速量子随机数生成器集成电路实现技术。

（九）密码安全实现及评估技术

研究内容：研究实用抗泄露和抗侧信道攻击密码设计理论与技术；研究密码算法在多种应用场景下的安全高效实现技术和攻击方法；研究密码算法实现抗侧信道攻击综合评估方法；研究抗干扰高速物理熵源设计理论与技术；研究安全高效的随机数生成方法和大样本数据的随机性高效检测方法。

（十）密码设备安全防护关键技术

研究内容：研究密码设备抗网络攻击、抗电磁域攻击、抗侧信道攻击等关键技术；研究密码系统安全性形式化分析与验证方法；研究密码资源和密码设备的安全监管关键技术；研究密码设备安全风险量化评估、密码设备安全防护等级评估准则。

（十一）其他探索性密码研究问题

研究内容：鼓励探索新型密码基础理论和应用技术，阐明研究问题的新颖性、原创性和可行性。

二、成果形式与考核指标

面上项目应围绕上述 11 个支持方向中的一项或多项研究内容开展创新性研究，提出新思想、新理论和新方法。各项目须提交本研究方向高质量的综述报告至少 1 份，并根据实际研究情况提交论文、著作、专利、软件代码、原型系统等形式的研究成果。

三、申请程序及要求

（一）申请条件

1. 项目申请人应具有高级专业技术职称或者具有博士学位，年龄不超过 60 周岁（截至 2023 年 12 月 31 日），具备独立开展研究和组织开展研究的能力，能够承担实质性研究工作，每年用于项目的工作时间不得少于 6 个月。

2. 项目申请人所在单位应符合《国家密码科学基金管理办法（试行）》规定的依托单位有关要求。

（二）限项申请规定

项目申请人同年只能申请 1 项国家密码科学基金项目（重点项目和面上项目均计算在内）。

（三）申请要求

面上项目申报截止时间为2024年1月15日24时，请有意向申报的科研人员按照模板填写项目申请书，电子版材料及签字盖章材料扫描件发送至电子邮箱。

（四）注意事项

1. 项目负责人应将主要精力投入项目的研究中，依托单位应加强对项目实施的监督、管理和服务，减轻项目负责人不必要的负担，为项目研究提供必要的制度和条件保障。

2. 国家密码管理局将把相关项目负责人项目执行情况计入信誉档案。

（五）联系方式

填报过程中遇到问题或进行咨询，可联系国家密码科学基金管理办公室。

联系人：苏老师、徐老师

联系电话：010-82789912

电子邮箱：ncsf@sca.gov.cn

国家密码科学基金
首批重点项目申报指南

为落实“十四五”期间密码科技创新有关部署安排，服务国家重大战略需求，支持密码科研团队开展密码理论和共性关键技术研究，努力实现战略性、引领性、基础性研究原创成果的重大突破，进一步增强密码领域原始创新能力，培养密码领域人才和团队，现发布国家密码科学基金首批重点项目申报指南。

一、支持计划

重点项目计划对 6 个密码研究方向进行重点支持，国家密码管理局将为重点项目设置责任专家，对项目实施进行指导把关。

（一）抗量子公钥密码算法安全性分析评估技术

1. 研究内容：研究格密码、基于编码的密码、基于 Hash 函数的数字签名、多变量密码和同源密码等抗量子公钥密码算法的量子及经典安全性分析与评估方法，包括但不限于：

（1）各类底层困难问题的安全性归约；

（2）各类底层困难问题的新型攻击方法及复杂度分析；

（3）各类算法安全性评估模型及其合理性有效性分析；

（4）各类算法的安全评估指标和评估方法；

（5）各类底层困难问题攻击方法和评估方法的高效实现库；

（6）各类国际国内抗量子征集算法的安全性分析及评估。

2. 研究周期：分为两个阶段，总计 4 年，其中第一阶段为 2 年，第二阶段为 2 年。

3. 支持数量：第一阶段不超过 8 个项目，可选择某类或某几类抗量子公钥密码算法的 1 项或多项研究内容开展研究。第二阶段不超过 3 个项目，应完成某类或某几类抗量子公钥密码算法的全部研究内容。

4. 经费额度：第一阶段不超过 30 万元 / 项，第二阶段不超过 120 万元 / 项。

5. 考核指标

第一阶段：

（1）提交至少 1 类抗量子公钥密码算法安全性分析综述报告，包括：困难问题求解算法类型、安全性评估方法、已有攻击方法和攻击结果等；

（2）提出至少 1 种针对主流抗量子公钥密码算法底层困难问题的更优求解算法；

（3）给出至少 1 种主流抗量子公钥密码算法的更优安全性分析结果。

第二阶段：

（1）提出底层困难问题新型求解算法，刷新 LWE、SVP、Ring-LWE、多变量密码等相关国际挑战纪录至少 1 项；

（2）研制至少 1 类抗量子公钥密码算法底层困难问题求解算法和该类抗量子公钥密码算法安全性评估方法的高效代码库；

（3）形成至少 1 类抗量子公钥密码算法安全性评估技术要求建议稿。

（二）抗量子密码协议设计理论与分析方法

1. 研究内容：研究密码基础设施、密码设备抗量子迁移的总体技术架构；针对“先存储后解密”攻击，研究现役密码协议与抗量子公钥密码算法的融合技术，满足过渡期应用需求；研究网络层、传输层、应用层等密码协议（如 TLS、IPsec、SSH 等）的抗量子安全模型及可证明安全性分析方法，提出相关协议的设计理论与方法，设计实用化协议并给出参数选取方法，给出底层抗量子密码算法的适配指标，研制抗量子密码协议实现库；研究数字认证体系等基础设施

的抗量子安全适配性方法，提出算法参数与综合性能等方面的需求。

2. 研究周期：分为两个阶段，总计 4 年，其中第一阶段为 2 年，第二阶段为 2 年。

3. 支持数量：第一阶段支持不超过 4 个项目，可选择现役密码协议与抗量子公钥密码算法的融合方法或 TLS、IPsec、SSH 中某类抗量子密码协议进行研究。第二阶段支持不超过 2 个项目。

4. 经费额度：第一阶段不超过 40 万元 / 项，第二阶段不超过 120 万元 / 项。

5. 考核指标

第一阶段：

（1）提出不少于 2 种抗量子密码协议（如 TLS、IPsec、SSH 等）的设计方法，给出不少于 2 个具体抗量子密码协议并选取满足 128、192、256 比特量子安全强度的参数，其计算代价或传输负载显著优于经典协议标准的抗量子密码算法直接替换，握手延迟达到国际先进水平；或提出 1 套现役密码协议与抗量子公钥密码算法的融合方法并进行技术验证；

（2）申请发明专利不少于 2 项。

第二阶段：

（1）提出密码基础设施、密码设备抗量子迁移的总体技术架构，包含对底层抗量子密码算法、数字证书的适配指标要求；

（2）研制抗量子密码协议实现库并进行技术验证，至少包含第一阶段优选的抗量子密码协议；

（3）研制抗量子密码协议的安全性与综合性能自动化评估平台；

（4）向国际互联网工程任务组（IETF）、密码行业标准化委员会等国际国内标准化组织提交抗量子密码协议标准草案 2~3 项；申请发明专利不少于 2 项。

（三）实用化全同态加密算法设计

1. 研究内容：针对云计算、边缘计算、大数据、人工智能等领域密态计算需求，研究实用化全同态加密算法设计技术，包括：

（1）新型高效同态乘法技术、自举技术、噪音控制技术，不同形态明文空间紧致编码及切换技术；

（2）新型精准算术运算、近似算术运算、布尔逻辑运算的高效同态计算技术；

（3）紧致密文多密钥全同态加密算法设计技术；

（4）新型同态加密高效实现技术，基于 SIMD 指令通用平台及 GPU、FPGA、ASIC 等专用平台的优化实现技术；

（5）面向典型应用场景的综合优化技术。

2. 研究周期：4 年。

3. 支持数量：1~2 项。

4. 经费额度：不超过 240 万元。

5. 考核指标

（1）提出全同态加密高效自举算法，综合性能优于已有同类算法，自举密钥规模或计算效率较已有算法提升不少于 20%（128 比特安全强度）；

（2）设计实用化全同态加密算法不少于 2 个，综合性能与 BGV/BFV/CKKS/TFHE 等现有算法相当，在至少 2 个典型应用场景的计算性能超越上述同类算法 10%（128 比特安全强度）并进行技术验证；

（3）提出基于标准假设的新型多密钥全同态加密算法设计方法，渐进联合密文尺寸与参与方个数为亚线性关系；

（4）研制全同态加密算法开源代码库，至少包含 2 个自研全同态加密算法，综合性能与 SEAL、HELib、TFHE、OpenFHE、Lattigo 等现有开源库具有可比较性；

（5）向 IETF、密码行业标准化委员会等国际国内标准化组织提交全同态加密算法标准草案 1~2 项；申请发明专利不少于 3 项。

（四）安全多方计算协议实用化关键技术及其应用

1. 研究内容：研究关于任意布尔电路的安全多方计算（MPC）协议及其基础组件，提出常数级轮数复杂度 MPC 协议的高效设计与实现方法；研究关于任意算术电路基于秘密分享 MPC 协议及其基础组件的实用化设计方法；研究 MPC 实现关键技术，研制 MPC 协议开源库；开展 MPC 示范应用研究，打

破跨部门、跨安全域的数据孤岛，实现高安全需求应用场景下敏感数据的高效流通。

2. 研究周期：3 年。

3. 支持数量：1~2 项。

4. 经费额度：不超过 260 万元。

5. 考核指标

（1）关于布尔电路的 MPC 协议，在恶意敌手模型下满足可证明安全性，具有常数级轮数复杂度，平均每个与门计算时间低于 1 微秒，提升之前同类协议性能至少 50%；

（2）关于算术电路的 MPC 协议，在诚实大多数恶意敌手模型下具有可证明安全性，可实现大域（至少 40 比特）上任意算术电路计算，平均每次乘法计算时间低于 2 微秒，提升之前同类协议效率至少 50%；

（3）研制自主可控的 MPC 协议开源库，包含至少 2 种不同类型 MPC 协议，支持任意布尔和算术电路的安全计算，协议性能与 EMP-toolkit、MP-SPDZ 等国际 MPC 协议开源库可比较；

（4）基于 MPC 协议库，研制高安全需求应用场景下联合数据分析应用验证系统，具备均值、方差、中位数、线性回归、逻辑回归等统计分析能力，可实现高安全需求应用场景下敏感数据的高效流通；

（5）向 IETF、密码行业标准化委员会等国际国内标准化组织提交 MPC 相关密码标准草案至少 1 项。

（五）信息系统属性密码融合应用验证评估

1. 研究内容：面向信息系统中数据安全共享、细粒度访问控制等数据安全需求，针对信息系统中数据库和云存储等数据存储、处理和应用等场景，突破兼具高安全性、高计算效率和高功能性的属性密码设计关键技术，提出高效实用的属性加密算法，研究针对属性密码应用中撤销、追责等问题的高效解决方案；提出针对信息系统中数据库和云存储 2 种应用场景的属性密码应用方案并开展技术验证；研究提出抗量子属性密码方案并开展安全性实用性评估。

2. 研究周期：2 年。

3. 支持数量：1~2 项。

4. 经费额度：不超过 130 万元。

5. 考核指标

（1）设计提出能够精准刻画信息系统中数据库和云存储 2 种应用场景应用需求及安全需求的系统模型和安全模型，支撑属性密码应用方案设计；

（2）提出并实现针对信息系统中数据库和云存储 2 种应用场景的安全高效属性加密方案，能够支持灵活的用户加入、撤销和权限变更等功能，支持的属性规模不少于 200 个，在百万量级数据库应用中，同一数据集相同操作下使用属性密码后整体性能下降不超过 10%，完成方案技术验证；

（3）提出 1~2 个抗量子属性密码方案，并完成小规模属性规模（约 50 个属性）条件下密码方案安全性和实用性评估分析。

（六）对称密码自动化分析理论、方法与工具

1. 研究内容：针对对称密码分析的实际需求，开展对称密码自动化分析理论、方法与工具研究。下述研究内容可选择 1 项或多项进行：

（1）基于一般约束规划问题（MILP、SMT/SAT、CP 等）的对称密码自动化分析建模与求解；

（2）对称密码自动化分析前端工具链研制；

（3）面向密码分析的一般约束规划问题专用求解器研制。

2. 研究周期：3 年。

3. 支持数量：研究内容（1）（2）（3）支持均不超过 1 项。

4. 经费额度：研究内容（1）不超过 30 万元 / 项；研究内容（2）不超过 80 万元 / 项；研究内容（3）不超过 150 万元 / 项。

5. 考核指标（分项对应研究内容）：

（1）提出基于 MILP、SMT/SAT 或 CP 的对称密码自动化分析建模理论、方法及相关模型的高效求解算法，包含已有自动化方法未支持的分析技术或提

高已有分析的求解效率，给出至少 1 个国内外密码标准算法或竞赛获胜算法更优分析结果；

（2）研制面向对称密码自动化分析的领域专用描述语言及其工具集，包括编辑器、调试工具、编译器（将领域专用语言编译成面向后端自动化分析建模的可扩展中间表示）和基于 MILP 或 SMT/SAT 的对称密码自动化分析模型构建工具；

（3）求解器应实现分支定界、割平面等主流约束规划问题求解算法，具备适用于密码分析相关约束规划模型求解的优化策略，实现相关模型求解和可行域遍历功能，在若干典型密码分析模型求解方面性能表现优于现行求解器，支持主流平台实现。

二、组织方式

1. 对支持方向（一）至（二），采用“赛马”制组织方式。在项目立项时择优选择多个主体并行攻关，在项目开展过程中采取阶段性竞争考核、竞争性淘汰机制，充分激发创新活力和动力，让优秀团队脱颖而出。

实施步骤主要分为两个阶段，第一阶段支持若干项目，与项目团队签订任务合同书，启动实施“赛马”；第一阶段结束后，由国家密码管理局组织考核，根据考核结果确定后续支持方式。若开展第二阶段项目支持，须重新签订任务合同书。

（1）若只有一个团队达到考核要求，可视为唯一优势主体予以第二阶段项目支持；

（2）若多个团队达到考核要求，择优遴选技术路线最先进、攻关能力与综合水平最高的团队予以第二阶段项目支持。如多个团队技术路线均较为先进，且攻关能力与综合水平相当，可对各团队继续进行第二阶段单独项目支持；如几个团队的相关技术路线或方案互补，能够各补长短，可组织现有团队强强联合组成新团队，予以第二阶段项目支持；

（3）若无团队达到考核要求，不进行第二阶段支持。

2. 对支持方向（三）至（六），采用常规项目组织方式。原则上支持方向（三）至（五）为每个方向支持 1 项，仅在申报项目评审结果前两位评价相近、技术路线明显不同时，可同时支持 2 项，若同一支持方向支持项目为 2 项时，原则上总经费额度不超过该方向计划支持经费额度；支持方向（六）为每个研究内容支持不超过 1 项。项目一般由 1 家单位承担，确有必要进行合作研究的，合作研究单位不得超过 2 家。

三、申请程序及要求

（一）申请条件

1. 项目申请人须具有高级专业技术职称或者博士学位，具有承担国家级基础研究课题的经历，年龄不超过 60 周岁（截至 2023 年 12 月 31 日），每年用于项目的工作时间不得少于 6 个月。

2. 项目申请人所在单位应符合《国家密码科学基金管理办法（试行）》规定的依托单位有关要求。

（二）限项申请规定

项目申请人同年只能申请 1 项国家密码科学基金项目（重点项目和面上项目均计算在内）。

（三）申请要求

重点项目申报截止时间为 2024 年 1 月 15 日 24 时，请有意向申报的科研人员按照模板填写项目申请书，电子版材料及签字盖章材料扫描件发送至电子邮箱。

（四）注意事项

1. 项目负责人应将主要精力投入项目的研究中，依托单位应加强对项目实施的监督、管理和服务，减轻项目负责人不必要的负担，为项目研究提供必要的制度和条件保障。

2. 国家密码管理局将把相关项目负责人项目执行情况计入信誉档案。

（五）联系方式

填报过程中遇到问题或进行咨询，可联系国家密码科学基金管理办公室。

联系人：苏老师、徐老师

联系电话：010-82789912

电子邮箱：ncsf@sca.gov.cn

转载自国家密码管理局官方网站

关于印发《国家密码科学基金管理办法（试行）》的通知

各有关单位：

为进一步加强对密码基础研究的顶层规划，优化科技资源配置，国家密码管理局对国家密码发展基金进行了优化，更名为国家密码科学基金。现将《国家密码科学基金管理办法（试行）》印发你们，请认真贯彻执行。

国家密码管理局

2023 年 12 月 12 日

国家密码科学基金管理办法（试行）

第一章 总 则

第一条 为规范国家密码科学基金管理，提高国家密码科学基金使用效益，根据《中华人民共和国密码法》以及相关规定，制定本办法。

第二条 国家密码科学基金面向国家战略需求，瞄准国际密码科技前沿，聚焦原创性、前沿性密码理论和共性关键技术研究，着力加强对密码基础研究的顶层规划和科技资源优化配置，提升密码领域原始创新能力，培养密码领域人才和团队，为实现密码科技高水平自立自强提供重要支撑。

第三条 国家密码科学基金管理遵循公开、公平、公正的原则，采取宏观引导、自主申请、平等竞争、同行评审、择优支持的机制。

第二章 组织与职责

第四条 国家密码管理局负责管理国家密码科学基金，制定国家密码科学基金规划（以下简称基金规划）和国家密码科学基金项目申报指南（以下简称项目指南），组织实施国家密码科学基金项目（以下简称项目）管理，对国家密码科学基金管理中的重大问题作出决定。

第五条 国家密码管理局设立国家密码科学基金咨询委员会，对国家密码科学基金发展战略、支持政策、优先发展方向及关键科学问题提出咨询意见。

第六条 国家密码管理局设立国家密码科学基金管理办公室，负责基金的日常管理工作。

第七条 国家密码管理局设立国家密码科学基金专家库，选取在库专家参与基金规划和项目指南的编制、项目的论证和把关等工作，专家库实行动态更新。

第八条 国家密码科学基金项目依托单位（以下简称依托单位）应为在中华人民共和国境内注册、具有独立法人资格、具备良好密码科研基础和科研条件的高等学校、科研院所及企事业单位。依托单位在项目管理过程中履行下列职责：

（一）审核申请人或项目负责人所提交材料的真实性、准确性和完整性；

（二）提供项目实施的必要条件，保障项目负责人和参与者实施项目的时间；

（三）跟踪项目实施，监督项目经费的使用；

（四）配合国家密码管理局对项目进行监督管理。

第三章 规划与组织

第九条 国家密码管理局面向国家密码战略需

求，结合密码科学技术发展趋势，在广泛听取意见和专家评审论证的基础上制定基金规划和项目指南。

第十条 国家密码管理局每五年制定基金规划，明确未来五年的优先发展方向、经费概算以及年度分配建议。

第十一条 国家密码管理局定期发布项目指南，规定优先支持的研究方向、项目类型和组织方式。项目指南原则上每年发布一次。

第十二条 为激发科研人才创新创造活力，国家密码科学基金根据项目实际需求，可实行“揭榜挂帅”“赛马制”等新型项目组织管理模式。

“揭榜挂帅”是指由需求方提出具体技术研发需求，以国家密码科学基金为平台，发布揭榜任务、促成供需对接并予以立项，加快解决技术难题的项目管理模式。

“赛马制”是指针对同一个研究内容，经专家论证后，对遴选的多家项目承担单位先进行平行立项，然后重点聚焦，最终优中选优的项目管理模式。

第四章 申请与评审

第十三条 依托单位的科学技术人员具备下列条件的，可以申请项目：

（一）拥护中国共产党的领导，遵守中华人民共和国宪法和法律；

（二）具有独立开展研究和组织开展研究的能力，能够承担实质性研究工作；

（三）具有高级专业技术职称或者具有博士学位；

（四）申请人应当是项目实际负责人，限为 1 人。

第十四条 申请项目的数量应当符合下列要求：

（一）作为申请人同年申请项目限为 1 项；

（二）作为项目负责人正在承担项目，且该项目与所申请的项目存在执行周期重叠的，不得申请；

（三）项目指南中对申请数量的限制。

第十五条 申请人应当按照项目指南要求，在规定期限内提出申请，申请人应当对所提交申请材料的真实性、准确性和完整性负责，依托单位应当对申请材料进行审核。

第十六条 项目申请人应当根据政策相符性、目标相关性和经济合理性原则，根据项目研究需要和资金开支范围，科学合理、实事求是地编制项目预算。

有多个单位共同承担一个项目的，依托单位的项目申请人和合作研究单位参与者应当根据各自承担的研究任务分别编报项目预算，由项目申请人汇总编制。

第十七条 项目经费是指在项目实施过程中发生的相关费用，主要包括设备费、业务费、劳务费等。

第十八条 国家密码管理局应当自项目申请截止之日起 45 日内，完成对申请材料的形式审查。符合本办法规定的，予以受理，有下列情形之一的，不予受理：

（一）申请人不符合本办法规定条件的；

（二）申请材料不符合项目指南要求的；

（三）申请人申请项目超过规定的数量的；

（四）未在规定期限内提交申请的；

（五）申请人、参与者处于列入黑名单期间的；

（六）依托单位处于列入黑名单期间的。

第十九条 国家密码管理局从专家库中随机选取同行专家对受理的项目申请进行评审，评审形式包括通讯评审和会议评审。

第二十条 评审专家从申请项目的科学价值、创新性、社会影响、研究方案可行性、预算相关性和合理性等方面进行独立判断和评价，提出客观公正的评审意见，确定项目经费额度。

第二十一条 国家密码管理局根据本办法的规定、年度支持计划以及专家提出的评审意见，确定支持项目清单，及时将评审结果通知申请人和依托单位，并反馈专家评审意见。

第二十二条 申请人对评审结果持异议的，可以自收到通知之日起 7 日内，向国家密码管理局提出书面

异议申请。对评审专家的学术判断有不同意见，不得作为提出异议的理由。申请人只能提出一次异议申请。

国家密码管理局应当自收到申请之日起 30 日内给出处理意见，并通知申请人。

第二十三条 在项目评审工作中，评审专家有下列情形之一的，应当申请回避或由国家密码管理局决定回避：

（一）评审专家本人申请或参与申请本年度项目的；

（二）评审专家与申请人、参与者存在近亲属关系的；

（三）评审专家与申请人、参与者属于同一单位的；

（四）其他利益冲突或可能影响评审公正性的。

第二十四条 基金管理工作人员不得申请或者参与申请项目，不得干预评审专家的评审工作。

基金管理工作人员和评审专家不得向外披露未公开的评审专家的基本情况、评审意见、评审结果等与评审有关的信息。

第五章 立项与实施

第二十五条 获得项目支持的申请人应当自收到通知之日起 20 日内，按照评审意见和确定的经费额度填写项目合同书，提交国家密码管理局审核，无特殊情况，逾期未提交视为自动放弃。

申请人除根据评审意见和确定的经费额度对已提交的申请书内容进行调整外，不得对其他内容进行变更。

国家密码管理局应当自项目合同书提交截止之日起 30 日内审核项目合同书，核准后的项目合同书作为项目实施、资金拨付、监督检查和结项的依据。

第二十六条 国家密码管理局根据不同类型科研项目特点、研究进度、资金需求等，合理制定经费拨付计划。国家密码管理局应当在项目合同书签订后 30 日内，将经费按计划拨付至依托单位，切实保障科研活动需要。依托单位自收到项目经费之日起 15 日内，向国家密码管理局提供资金到位相关凭证。

有多个单位共同承担一个项目的，依托单位应当及时按项目合同书转拨合作研究单位资金，并加强对转拨资金的监督管理。

第二十七条 项目资金应当纳入依托单位财务统一管理，单独核算，专款专用。

项目负责人应当严格按照经费预算使用项目经费，依托单位应当对项目负责人使用项目经费的情况进行监督。项目实施过程中，应当严格执行国家关于政府采购、招投标、资产管理、支出管理等相关规定，原则上实行“公务卡”结算和银行转账方式结算。

项目资金管理使用不得存在以下行为：

（一）编报虚假预算；

（二）未对项目资金进行单独核算；

（三）列支与本项目任务无关的支出；

（四）未按规定执行和调剂预算、违反规定转拨项目资金；

（五）通过虚假合同、虚假票据、虚构事项、虚报人员等弄虚作假，转移、套取、报销项目资金；

（六）截留、挤占、挪用项目资金；

（七）设置账外账、随意调账变动支出、随意修改记账凭证、提供虚假财务会计资料等；

（八）使用项目资金列支应当由个人负担的有关费用和支付各种罚款、捐款、赞助、投资、偿还债务等；

（九）其他违反国家财经纪律的行为。

第二十八条 项目实施过程中，项目预算有以下情况确需调剂的，应当按相关程序报国家密码管理局审批：

（一）由于研究内容或者研究计划作出重大调整等原因需要对预算总额进行调整的；

（二）有多个单位共同承担一个项目的，各单位之间资金需要调剂的。

项目实施过程中，在项目预算额度不变的情况下，预算确需调剂的，按以下规定予以调剂：

（一）设备费预算如需调剂，由项目负责人根据科研活动的实际需要提出申请，报依托单位审批。依托单位应当统筹考虑现有设备配置情况、科研项目实际需求等，及时办理调剂手续；

（二）劳务费、业务费预算如需调剂，由项目负责人根据科研活动实际需要自主安排。

第二十九条 项目负责人应当按照项目合同书组织开展研究工作，作好项目实施情况的原始记录，经依托单位审核后向国家密码管理局提交项目年度进展报告。

第三十条 国家密码管理局在项目实施的关键节点组织专家对项目进展及资金使用和管理等进行检查，并将检查结果和处理意见通知项目负责人和依托单位。

第三十一条 依托单位和项目负责人应当保证参与者的稳定。由于客观原因确实需要变更参与者的，由项目负责人作出书面说明，经依托单位审核后报国家密码管理局备案。

第三十二条 项目实施过程中，不得擅自变更研究内容和研究计划，因特殊原因需要作出重大调整的，项目负责人应书面提出申请，经依托单位审核后，报国家密码管理局审批。

第三十三条 项目实施过程中，原则上不得变更依托单位或项目负责人，因特殊原因需要作出调整的，依托单位应当书面提出申请，报国家密码管理局审批。

经国家密码管理局批准的依托单位发生变更的项目，原依托单位应当及时向新依托单位转拨需转拨的项目资金。

第三十四条 有下列情形之一的，依托单位应当及时提出终止项目实施的申请，报国家密码管理局审批；国家密码管理局也可以直接作出终止项目实施的决定：

（一）项目负责人不能继续开展研究工作，且无可替代人选的；

（二）项目执行中有剽窃他人科学研究成果、侵犯知识产权或者弄虚作假等学术不端行为的；

（三）经实践证明，项目技术路线不合理、不可行，或项目无法实现任务书规定的进度且无改进办法的；

（四）完成项目任务所需的资金、原材料、人员、支撑条件等未落实或发生改变导致研究无法正常进行的；

（五）发生其他重大问题导致项目无法进行的。

终止项目的，依托单位应对已开展工作、经费使用、已购置设备仪器、阶段性成果、知识产权等情况作出书面报告，经国家密码管理局核查批准后，依规完成后续相关工作。对于因非正当理由致使项目终止的，纳入依托单位或项目负责人信誉档案。

第三十五条 由于客观原因不能按期完成研究计划的，项目负责人可以申请延期 1 次，申请延长的期限不得超过 1 年。项目负责人应当于项目支持期限届满 60 日前书面提出延期申请，经依托单位审核后，报国家密码管理局审批。批准延期的项目在结项前应提交项目年度进展报告。

第三十六条 发生本办法第二十九条、第三十三条至三十六条所列情形，国家密码管理局作出批准、不予批准或终止决定的，应当及时通知项目负责人和依托单位。

第三十七条 自项目支持期满之日起 30 日内，项目负责人应当向国家密码管理局提交结项报告、经费决算等结项材料，配合做好结项和审计工作，项目负责人应当对结项材料的真实性负责。依托单位应当对结项材料进行审核。

第三十八条 国家密码管理局及时组织专家对项目完成情况进行结项审查，并将结项审查结果和验收意见通知项目负责人和依托单位。

项目完成情况纳入依托单位和项目负责人信誉档案，作为后续立项评审的重要参考依据。

有下列情况之一的，责令限期改正，逾期不改正的，不予结项：

（一）未按时提交结项材料的；

（二）提交的结项材料不齐全、不符合填报要求或手续不完备的；

（三）其他不符合国家密码管理局要求的情况。

第三十九条 国家密码管理局准予结项、不予结项和因故终止执行的项目，依托单位应当负责将结余资金在通知书下达后 30 日内按原渠道退回。

因故被依法撤销的项目，依托单位应当负责将已拨付的资金在通知书下达后 60 日内全部按原渠道退回。

第四十条 项目取得的研究成果应按照国家密码

管理局要求进行成果署名和标注。

第四十一条 项目取得的研究成果归属，按照《中华人民共和国科学技术进步法》第三十二条和有关法律、法规、规章的规定执行。国家密码管理局、依托单位、项目负责人应当签订三方合同，对研究成果的占有、使用、收益、处分等事项作出具体规定。

第六章 监督与处理

第四十二条 国家密码管理局对项目实施情况进行抽查，抽查时应当查看项目实施情况的原始记录。

第四十三条 国家密码管理局建立申请人、项目负责人、依托单位的信誉档案，并将其作为批准项目申请的重要依据。

第四十四条 国家密码管理局定期对评审专家履行评审职责情况进行评估；根据评估结果，建立评审专家信誉档案。

第四十五条 申请人、参与者伪造或者变造申请材料的，由国家密码管理局给予警告；其申请项目已决定支持的，撤销原支持决定，追回已拨付的经费；情节严重的，列入黑名单，3 至 5 年不得申请或者参与申请项目。

第四十六条 项目负责人、参与者违反本办法规定，有下列行为之一的，由国家密码管理局暂缓拨付经费，并责令限期改正；逾期不改正的，撤销原支持决定，追回已拨付的经费；情节严重的，列入黑名单，5 至 7 年内不得申请或者参与申请项目：

（一）不按照项目合同书开展研究的；

（二）擅自变更研究内容或者研究计划的；

（三）不依照本办法规定提交项目年度进展报告、结项材料的；

（四）提交弄虚作假的报告、原始记录或者相关材料的；

（五）侵占、挪用经费的。

第四十七条 依托单位有下列情形之一的，由国家密码管理局责令限期改正；情节严重的，列入黑名单，3 至 5 年不得作为依托单位：

（一）不履行保障项目研究条件职责的；

（二）不对申请人或项目负责人提交材料或者报告的真实性、准确性和完整性进行审查的；

（三）纵容、包庇申请人、项目负责人弄虚作假的；

（四）不配合项目监督、检查工作的；

（五）截留、挪用经费的。

第四十八条 评审专家有下列行为之一的，由国家密码管理局责令限期改正；情节严重的，国家密码管理局不再聘请其为评审专家：

（一）不履行国家密码管理局规定的评审职责的；

（二）未依照本办法规定申请回避的；

（三）披露未公开的与评审有关的信息的；

（四）对项目申请不公正评审的；

（五）利用工作便利谋取不正当利益的。

第四十九条 基金管理工作人员有下列行为之一的，给予处分：

（一）披露未公开的与评审有关的信息的；

（二）干预评审专家评审工作的；

（三）利用工作便利谋取不正当利益的。

第五十条 申请人或者项目负责人、参与者违反本办法规定，构成犯罪的，终身不得申请或者参与申请项目。

第五十一条 国家密码管理局对违反本办法规定的情况进行公告。

第七章 附 则

第五十二条 本办法由国家密码管理局负责解释。

第五十三条 本办法自公布之日起施行。

国家密码管理局办公室 2023 年 12 月 12 日印发

转载自国家密码管理局官方网站

交通运输部关于
加快智慧港口和智慧航道建设的意见

索引号:	000019713O08/2023-00105	机构分类:	水运局
文号:	交水发〔2023〕164号	主题分类:	其他
公开日期:	2023年12月04日	行业分类:	航道养护管理;港口管理
主题词:	智慧港口;智慧航道;意见	公文类型:	部文件

各省、自治区、直辖市、新疆生产建设兵团交通运输厅(局、委),长江航务管理局、珠江航务管理局:

为贯彻习近平总书记关于大力发展数字经济、智慧交通等重要指示精神,落实《交通强国建设纲要》《国家综合立体交通网规划纲要》《数字中国建设整体布局规划》,按照《加快建设交通强国五年行动计划(2023—2027 年)》《水运“十四五”发展规划》等有关要求,推动智慧港口和智慧航道建设发展,加快建设交通强国水运篇,提出以下意见。

一、总体要求

(一)指导思想。

以习近平新时代中国特色社会主义思想为指导,全面贯彻落实党的二十大精神,完整、准确、全面贯彻新发展理念,服务加快构建新发展格局,着力推动高质量发展,以加快建设交通强国为统领,以数字化、网络化、智慧化为主线,以提效能、扩功能、增动能为导向,以智慧化生产运营管理服务为重点,推动水运行业实现质的有效提升和量的合理增长,着力建设安全、便捷、高效、绿色、经济、包容、韧性的可持续交通体系,书写好交通强国水运篇章,奋力加快建设交通强国,努力当好中国式现代化的开路先锋,为全面建设社会主义现代化国家提供坚实有力的服务保障。

(二)基本原则。

统筹谋划、注重质效。坚持系统观念,统筹区域间、产业间、方式间融合发展,强化港口和航道建设、生产、运营、管理、服务全流程协同。注重集约共享、质效齐升,推动资源有效整合、业态开放共享。

因地制宜、分类指导。坚持需求导向,立足港口和航道发展条件及功能定位,尽力而为、量力而行,科学确定建设重点与路径,分类指导推进港口和航道智慧化建设。

创新驱动、数字赋能。坚持守正创新,以技术创新、业务流程创新、机制创新全面推动港口和航道转型升级。夯实数字基础,强化数字技术与业务深度融合,加快技术迭代,延伸产业链、打造供应链、提升价值链。

上下联动、政企协同。坚持协同联动,充分发挥市场在资源配置中的决定性作用,充分发挥各级政府的引导推动和支持保障作用。营造良好发展环境,强化要素保障,推动共同发力、可持续发展。

(三)发展目标。

到 2027 年,全国港口和航道基础设施数字化、生产运营管理和对外服务智慧化水平全面提升,建成一批世界一流的智慧港口和智慧航道。国际枢纽海港 10 万吨级及以上集装箱、散货码头和长江干线、西江航运干线等内河高等级航道基本建成智能感知网。建设和改造一批自动化集装箱码头和干散货码头。全面提升港口主要作业单证电子化率。加快内河电子航道图建设,基本实现跨省(自治区、直辖市)航道通航建筑物联合调度,全面提升内河高等级航道公共信息服务智慧化水平。

二、夯实数字底座

（一）推进信息基础设施建设。

1. 推进港口信息基础设施建设。推进港口智能感知设备部署应用，增强港口基础设施、港区环境、运行状态的动态监测能力。加快推动上海港、天津港、青岛港、宁波舟山港等具备条件的国际枢纽海港和南京港、武汉港、重庆港等具备条件的内河主要港口重要港区基本建成智能感知网。推动新建集装箱、散货、客运等码头同步实现基础设施自动化监测。

2. 推进航道信息基础设施建设。推进航道智能感知设备部署应用，加强水位、气象、海况、航标状态、航道尺度、整治建筑物、桥梁通航净空尺度、通航建筑物运行状态的动态监测。加快长江干线、西江航运干线、京杭运河以及水网地区高等级航道智能感知网建设，提升其他内河高等级航道的限制性桥梁河段、重点滩险河段、通航建筑物等智能感知水平。推动新建通航建筑物等同步实现基础设施自动化监测。提升沿海航道的透彻感知及精确定位能力。

3. 推进信息通信技术融合应用。推进港口和航道基础设施与云计算、大数据、物联网、人工智能（AI）、区块链等技术融合应用。扩大第五代移动通信网络 / 第五代固定通信网络（5G/F5G）、北斗卫星导航等技术在港口大型装卸设备远程控制、智能水平运输设备全流程作业、港区人员安防、多功能航标、视频监控等方面的应用规模。促进建筑信息模型（BIM）技术应用，推动“智慧工地”建设。鼓励建设港口和航道数字孪生平台。

（二）构建水运数据资源体系。

1. 提升行业数据共享水平。按照国家综合交通运输信息平台的总体框架，建立“部 - 省 - 运行单位”三级数据资源体系。建立健全港口和航道信息资源共享机制，依托部省数据共享交换系统，实现相关数据资源共享共用。

2. 推动“数据大脑”建设。推动港口企业、航道建设养护单位打造数据、服务、算法为一体的“数据大脑”，加强云服务、AI 大模型应用，按需构建技术支撑平台和数据支撑平台，强化多层次智能算力支持。

3. 加强数据资源管理。推动建立公共数据、企业数据、个人数据的分类分级确权授权制度。依法开展港口和航道数据的挖掘、评估、流通、交易和服务。培育形成统一的数据标准体系。推动培育数据服务生态，发展数据要素产业链。

（三）提升网络和数据安全能力。

1. 完善网络安全防护体系。强化港口和航道关键信息基础设施的网络安全防护能力建设。加强码头自动化控制、生产作业、通航建筑物运行调度等重要信息系统的网络安全管理、安全检测与风险评估。依法严格落实信息安全等级保护制度，强化网络安全监测预警和态势感知，加强攻击性测试手段应用。推进重要信息系统商用密码技术应用。

2. 加强数据安全保护。推进港口和航道领域数据安全管理，落实分类分级保护工作，加强数据容灾备份。加强港口和航道等基础设施重要数据和个人信息的安全保护，推进数据的全生命周期安全管理。严格落实数据出境安全评估有关要求。

三、推进生产运营管理智慧化

（一）推进港口生产智慧化。

1. 有序推进集装箱码头作业自动化。加快推动上海港、大连港、天津港、青岛港、宁波舟山港、厦门港、深圳港、广州港等具备条件的国际枢纽海港和苏州港、南京港、芜湖港、武汉港、济宁港等具备条件的内河港集装箱码头自动化建设或改造。鼓励港口企业实施岸桥、场桥等大型设备设施远程操控改造。推进新一代自动导引车（AGV）、无人集卡等智能化水平运输设备规模化应用。加快研发新一代自主可控的自动化集装箱码头生产管理系统，并有序推广应用。

2. 有序推进大宗干散货码头作业自动化。加快推动秦皇岛港、唐山港、黄骅港、青岛港、日照港、宁波舟山港、苏州港等具备条件的港口干散货码头“翻”“堆”“取”“装”“卸”等全流程自动化改造，推进翻车机、堆取料机、装船机、卸船机、门座式起重机、装车楼等专业化设备设施自动化、智能化升级。推动唐山港、黄骅港、青岛港、北部湾港等港口建设干散货数字堆场。鼓励建设干散货码头生产作业一体化管控平台。

（二）推进航道养护智慧化。

1. 推进养护智慧化。推动长江干线、西江航运干线、京杭运河、江淮运河、平陆运河等建设完善航道智慧养护管理系统。推进内河高等级航道长期

跟踪观测和演变分析预测预报，强化重要干线航道重点航段泥沙原型观测、水情水文、过闸区域气象动态跟踪。推动建设船闸设备设施健康监测系统，加强对水工建筑物、输水系统、金属结构及启闭机等的实时监测和动态评估。

2. 推进养护装备设施智能化。推广无人机、无人船和视频监控技术在航道巡查中的应用。推进智能疏浚装备及配套系统应用。全面推广航标遥测遥控、水位遥测遥报技术应用。推广应用多波束探测、船载激光扫描、实时 3D 声呐、水下探测机器人等技术，实现航道测量技术智能升级。利用 BIM、地理信息系统（GIS）、物联网以及数字孪生等新技术，推进长江干线、西江航运干线和京杭运河等高等级航道船闸智慧化升级。

（三）推进运营管理智慧化。

1. 强化运行安全管理。提升风险分级管控、隐患排查和预防预警能力，建立健全港口和航道智慧安全防控体系。提升港口保安、航道拥堵、船闸火灾、行业防汛防台、航道地质灾害、港口航道突发环境保护事件等应急处置和调度指挥智慧化水平。提升设备设施、作业人员安全监管智能化水平。强化对危险货物港口作业、危险货物船舶运行及过闸状态等的实时掌控。

2. 提高船舶过闸效率。推进船闸自动化运行，推广船闸区域集中控制技术。实现过闸船舶禁停线、过闸船舶超速监测。推动多闸联动一体调度，优化完善西江、北江等通航建筑物联合调度机制，持续推进京杭运河、嘉陵江、乌江等通航建筑物跨省联合调度。

3. 加强数字赋能绿色发展。推进港口岸电信息系统建设，提高岸电服务水平和岸电使用监管能力。鼓励“光伏 +”储能、“风电 +”储能等清洁能源多能互补及设备迭代升级。推动码头运载设备电动化，提升新能源水平运载设备比例。推进能耗智能监测、能源智能管理、环境智能监测等系统的应用。鼓励应用喷淋抑尘智能联动控制系统，提高用水节水智能管理水平。

4. 增强综合管控效能。鼓励港口企业及航道建设养护单位实现财务会计、人力资源、资产管理等数据资源一体化整合。鼓励建设基于“数据大脑”的综合管理系统，加强运营监管与风险防控，实现人、财、物精细化管理。

四、推进对外服务智慧化

（一）推进港口对外服务智慧化。

1. 推进物流服务便利化。支持港口提升集疏港智能化水平，推进作业单证“无纸化”和业务线上办理。以国际枢纽海港为重点，推动建设面向全程物流链的“一站式”智慧物流协同平台，强化与航运、铁路、公路、船代、货代等数据互联共享，支撑发展多式联运“一单制”“一箱制”。支持铁路、公路、水路运输企业及船代、货代、第三方平台等企业组建多式联运经营主体。大力推广智能理货和智能闸口。巩固进口电商货物港航“畅行工程”成果，深入推进冷藏集装箱港航服务提升行动。

2. 推进商贸服务协同化。支持大型港航企业与国际贸易“单一窗口”的合作对接，发展“通关 + 物流”一体化联动服务。推进国际枢纽海港进口集装箱、干散货区块链电子放货平台应用。鼓励创新港口数据服务，依托全流程数字化凭证和区块链等技术，推进国际贸易、航运信息、交易平台、融资授信、航运保险等商贸增值服务，为货主、船公司、物流企业等提供定制化服务。

（二）推进航道公共服务智慧化。

1. 建立智慧航道服务体系。推进船舶过闸服务智慧化，加强船闸智能调度、智能诱导等技术应用，提供过闸申报、缴费等“一站式”服务。推进水上服务区智慧化建设，实现船舶锚泊、污染物接收和岸电供水供油等服务的网上预约、智能结算，推广水上无人超市、智能快递等应用场景。总结推广“长江e+”“浙闸通”等服务模式，通过移动终端、门户网站、手机App、微信公众号等提供导航助航、过闸、锚泊、安全预警等多元化的航道信息服务，打造基于移动智能终端的伴随式航行服务。

2. 推动电子航道图建设和应用。推广长江干线电子航道图，加快实现长江支流航道与干线航道电子航道图有效衔接、一体联动。推进京杭运河、西江航运干线等干线航道和长三角等水网地区高等级航道率先实现电子航道图全覆盖，加强跨省联通、统一服务。加强电子航道图与电子海图推广升级、融合应用，服务江海联运。

3. 提升长江航运智慧化水平。完善长江数字航道建设。完善长江航运智能管理平台、综合保障平台和公共服务平台。汇聚港口、航道、船员、船舶、货物等要素信息，构建长江航运资源数据库。强化监测预警、运行分析、智能研判，加强三峡船闸过闸信息共享，完善政务服务“一网通”，提供全方位、全要素、全时段公共服务。

五、强化科技创新与国际交流合作

（一）强化科技和标准支撑。

1. 强化科技创新。鼓励围绕智慧港口和智慧航道关键技术开展联合科技攻关，加快推进自动化港作机械等装备、自动化码头生产管理系统、内外集卡运输系统协同、航道智能化测绘、船岸协同等关键技术研发与应用。推动国家高端智库开展智慧港口和智慧航道发展战略研究。

2. 强化标准支撑。建立健全智慧港口和智慧航道标准体系。制修订出台智慧港口和智慧航道建设相关技术指南和标准规范。鼓励各地方、学会协会、企业先行先试，探索出台地方标准、团体标准、企业标准。

（二）强化协同联动和交流合作。

1. 强化协作互动。强化港航和海事的信息互换和监管互动，加强与海关、国检、边检等部门信息互换、执法互助合作。完善信用考评制度，建立“互联网+”信用监管模式。推动港口和航道间数据共享、业务协同，推进港航一体化发展。引导信息技术企业参与智慧港口和智慧航道建设与运营。

2. 加强国际交流合作。开展智慧港口和智慧航道的国际交流，推动我国相关技术和标准“走出去”。开展智慧港口国际对标评估。统筹做好与国际标准的衔接，推进国际交流合作。鼓励相关单位和企业作为有关国际标准的主要制订者或参与者，贡献更多的中国智慧、中国方案。

六、实施要求

（一）加强组织领导。

部加强总体设计，强化宣贯、指导与督促。各级交通运输主管部门和长江航务管理局、珠江航务管理局按职责加强对港口企业和航道建设养护单位的指导，加强组织协调，扎实推进各项任务实施。

（二）加强试点示范。

发挥交通强国建设试点工作引领作用，推动建设一批智慧港口和智慧航道示范项目。深化智能交通先导应用试点，继续支持开展港口集装箱水平运输和集疏运自动驾驶试点。

（三）加强政策保障。

各级交通运输主管部门要积极争取对智慧港口和智慧航道建设的政策支持，推动建立多元化资金保障机制。加强人才保障，推进智慧港口和智慧航道规划、咨询、设计、施工、运营以及网络安全等各类人才队伍建设。充分发挥市场主体作用，引导形成相互竞争、优势互补、协同发展格局。

（四）加强跟踪评估。

各级交通运输主管部门要统筹工作要求，加强上下联动，完善考核工作机制，对目标完成情况、任务实施情况开展跟踪评估，重要进展及面临的共性问题及时报部。

交通运输部

2023年11月24日

转载自中华人民共和国交通运输部官方网站

南开大学数据与智能系统安全教育部重点实验室揭牌 天津市国家密码管理局丛局出席并致辞

12 月 23 日，南开大学数据与智能系统安全教育部重点实验室揭牌仪式暨学术委员会会议在津南校区综合业务东楼举行。

南开大学校长陈雨露、中国科学院院士冯登国、天津市国家密码管理局局长丛为民出席仪式。南开大学科研部负责人宣读了教育部关于重点实验室的批文，计算机学院、网络空间安全学院负责人主持仪式。

天津市国家密码管理局局长丛为民致辞，对重点实验室获批和揭牌表示热烈祝贺。

她说，我们将一如既往支持南开大学密码学科和实验室建设发展，希望南开大学担负好密码学科建设排头兵的使命，孵化出更多标志性成果，培养出更多创新型人才。

南开大学校长陈雨露与中国科学院院士冯登国共同为数据与智能系统安全教育部重点实验室揭牌。

南开大学校长陈雨露为实验室学术委员会主任、副主任致送聘书。学术委员会由中国科学院院士冯登国担任主任，北京邮电大学教授杨义先担任副主任。

北京航空航天大学教授刘建伟，上海交通大学教授刘胜利，复旦大学教授张新鹏，哈尔滨工业大学教授张宏莉，中国科学技术大学教授陈恩红，合肥工业大学教授汪萌，西北工业大学教授王震，南开大学教授符方伟、贾春福受聘学术委员会委员。

实验室学术委员会会议同期召开。实验室主任刘哲理就实验室建设基础、建设任务和年度进展等作汇报。

学术委员们肯定了实验室的阶段性研究成果和研究方向，对实验室的建设和发展进行深入讨论。

冯登国作总结发言，希望实验室在未来建设中进一步明确发展定位，锚定发展方向，拓展交流合作，彰显科研优势特色，培养聚集高素质人才，全力把实验室建设成高质量科研高地。

会后，天津市国家密码管理局有关负责人，南开大学科研部、党委网信办、计算机学院、网络空间安全学院相关负责人，及重点实验室教师代表等一同参观密码科普与“豪密”爱国主义教育基地。

2023物联网密码应用峰会在无锡召开
天津市国家密码管理局和天津商密协会参会

10 月 22 日，2023 物联网密码应用峰会在江苏无锡召开。本届峰会以“智联世界密码赋能”为主题，旨在宣传普及新修订的《商用密码管理条例》及配套规章制度，促进新时代商用密码应用与创新发展。会上，行业主管部门领导和业内专家学者齐聚一堂，聚焦密码政策法规、前沿技术、创新应用等，分享成果、交流经验、开展合作、共谋发展，赋能网络强国、数字中国和智慧社会建设。作为 2023 世界物联网博览会重要系列活动之一，峰会由国家密码管理局指导，中国密码学会支持，江苏省国家密码管理局、无锡市人民政府主办，江苏省商用密码产业协会、无锡市国家密码管理局、无锡国家高新技术产业开发区管理委员会承办。

以法护航
商用密码法治建设愈发完善

近年来，数字化发展浪潮席卷全球，面对机遇与挑战，商用密码法治建设的引领作用更加突出，推动商用密码管理模式发生重大变化。2019 年颁布的《密码法》和今年新修订的《商用密码管理条例》，对商用密码管理制度进行了结构性重塑，体现了鼓励创新与促进发展相结合，重点管控与保障安全相结合，放宽准入与规范监管相结合，总体设计与统筹衔接相结合的商用密码管理新思路。商用密码管理模式的变化，归根到底是为了促进商用密码应用，鼓励和推动商用密码产业发展和进步，保障网络和信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。

会上，国家密码管理局商用密码管理办公室对新修订的《商用密码管理条例》及《商用密码检测机构管理办法》《商用密码应用安全性评估管理办法》进行了详细解读，强调要牢固树立以人民为中心的发展理念，不断强化法治思维，完善政策法规体系，严格执法监督，以良法善治推动商用密码高质量发展。

面向未来
物联网密码应用不断创新

随着物联网蓬勃发展，物联网信息安全问题日益凸显，更加要求推进物联网密码应用，构建物联网安全新秩序。无锡坚持统筹发展和安全，着力推动密码与物联网融合发展，积极引进和建设政产学研协作创新平台，培育一批技术实力雄厚密码科研企业，密码产业年产值位居全省前列。物联网密码应用呈现良好的发展态势，展现广阔发展前景。

智能网联汽车是物联网重要应用之一，通过车

联网与智能车的有机接合，来实现车辆与人、路、后台系统的共享交互。无锡充分发挥国家级车联网先导区优势，进一步推动密码在车联网领域的技术攻关和应用。会上，举行了国家级车联网先导区密码应用试点项目启动仪式，以密码科技国家工程研究中心为主导，与无锡市有关管理部门和科研院所、产业单位，结合无锡高新区车联网建设高质量发展先行先试场景，共同推进在车与云、车与路、车与车、车与设备，以及电子导航地图、车辆隐私信息、车联网大数据等方面的密码体系化保护。

围绕车联网安全问题，密码科技国家工程研究中心总工程师秦小龙和公安部交通管理科学研究所所长孙正良分别作题为“智能网联汽车密码应用发展构想”和“面向车路协同安全的交管数字身份和密码应用”专题报告，探讨了基于内生密码安全技术的智能网联汽车发展模式，和基于商用密码算法解决城市道路管控问题的若干应用实践。

探索密码应用实践
赋能数字经济发展

2018 年，全国首届以物联网为主题的密码应用峰会召开。五年来，经过持续的探索、创新和沉淀，峰会知名度和影响力不断扩大，已经成为全国密码领域极具特色的交流平台。推动了密码产业创新链、资金链、人才链的深度融合，在推动密码应用与创新，服务社会经济发展中展现了江苏作为。

今年，行业大咖以各自的实践经历为例，展示行业如何将密码的学术理论、科技成果、工程实践有效衔接。

中国科学院大学密码学院院长、中国密码学会电子认证专委会主任荆继武教授在无锡物联网小镇建立了“密码科研和产业化平台”，积累了丰富的经验，并在峰会现场分享了基于物理不可克隆技术（PUF）的密码应用成果。中电科申泰信息科技有限公司副总经理韩磊介绍了申威自主处理器的安全防护体系，申威作为国内自主指令集技术的优秀代表，实现了密码和安全的深度融合，全面提升了信息系统、关键信息基础设施的网络安全防护能力。

当前，商用密码应用不断深入。中电科网络安全科技股份有限公司系统总体与方案中心总经理吴波针对新型电力系统“点多面广”、“无人值班少人值守”的特点，介绍了电科网安在新型电力系统方面的密码应用实践。北京卫星信息工程研究所卫星加密领域首席专家金星虎，针对我国卫星互联网面临的安全威胁，介绍了基于密码安全的卫星互联网一体化安全保障体系架构。联通数字科技有限公司安全事业部副总经理张建桁表示，中国联通已经打造了基于商用密码的泛在连接一体化安全服务平台，构建起基于商用密码的网络安全、应用安全和设备安全体系。北京神州龙芯科技有限公司副总裁谢巍、深圳奥联信息安全技术有限公司副总经理程朝辉、清华大学集成电路学院研究员杨博翰围绕物联网密码关键技术攻关及应用实践做交流分享。

天津市国家密码管理局
和天津市商用密码行业协会参会

天津市国家密码管理局和天津市商用密码行业协会积极参会，就万物智联时代下如何推动密码技术深度融入现代化建设与与会领导及专家学者进行探讨交流，有助于推动天津形成以创新发展商用密码为目标，以构建“产学研用测”全方位生态为路径，以商用密码与数字安全为主导的发展新模式。

天津市商用密码行业协会召开会员大会暨主题论坛筹备工作座谈会

为更好履行《密码法》《商用密码管理条例》中行业协会职责，推动密码在保障网络与信息安全中的支撑作用，促进天津市商用密码产业发展，同时，为了更好举办会员大会暨主题论坛工作，天津市商用密码行业协会于 2023 年 12 月 13 日组织召开了协会会长工作会议，市国家密码管理局派代表参加。

天津市商用密码行业协会秘书长胡双喜介绍会员大会暨主题论坛举办的目的、意义及初步工作开展流程，号召参会众人群策群力，为会员大会暨主题论坛的成功举办集思广益、谋篇布局。

大家一致认为，值此契机，协会组织会员大会暨主题论坛正当其时，并就活动方案提出多项可行性

建议，强调大会暨主题论坛的举办要主题明确、形式丰富、贴近实际工作，扩大邀请范围，增加更多针对法律法规、标准等的解读，提供更多商密领域技术交流、成果展示机会，展示天津在商密应用和实体经济融合发展方面的成果，提升天津商密产业综合竞争力，将天津商用密码产业打造为“天津名片”，携手共创天津商密辉煌。

各位会长纷纷表示，随着商用密码在信息领域新技术、新业态、新模式中更广泛、更深入的应用，在政策、市场和技术的多重驱动下，我国商用密码应用需求越来越强烈，市场规模迅速扩大，商用密码产业迎来巨大发展机遇。

刘处强调坚持党管密码的根本原则，并对协会扎实开展各项工作表示了肯定，希望协会能够充分发挥桥梁纽带作用，依托天津市高质量发展“十项行动”助推商密企业、商密产业进一步发展，推动天津经济社会建设。

郝处说到，协会要积极联动相关部门、科研院校和企业，努力搭建政企沟通、创新合作、产业交流重要平台，组织开展更加丰富的学术交流、业务合作和友好交往活动，将商密大会和主题论坛办好，助力天津商密做大做强。

供稿人：陈旭杨

宝坻区密码管理局多举措全方位开展密码宣传教育活动

密码是保障网络安全与信息安全的核心技术和基础支撑，也是维护国家安全、促进经济社会发展、保护公民、法人和社会组织合法权益的重要手段。宝坻区始终高度重视密码法治宣传教育工作，多措并举推动密码安全知识的宣传普及，在全区上下营造“密码安全为人民 密码安全靠人民”的浓厚氛围。

一、统筹谋划，精心组织

一是方案引领。区密码管理局将密码宣传教育工作纳入全年工作重点之一，结合全区实际，制定2023 年密码法治宣传教育活动工作方案，在“4·15”全民国家安全教育日、网络安全宣传周、国家宪法日和《密码法》颁布实施等重要时间节点，统筹开展宣传教育活动。

二是各有侧重。根据不同宣传对象，组织开展专题学习、线上答题、社区宣传等内容丰富、形式多样的宣传教育活动，保证宣传效果。

三是精心筹备。活动开展前，积极与上级部门沟通协调，收集整理线上线下宣传素材，及时传递最新密码政策法规和密码安全知识。今年以来，区密码管理局印制宣传单 5000 份，宣传购物袋 1000 个，以及挂图、易拉宝等宣传用品，以实实在在的行动推进密码法治宣传教育活动走深走实。

二、三学联动，层层推进

在全区党政机关开展密码安全宣传教育，一是密码干部带头学，组织全体密码干部开展密码安全专题教育，认真学习《密码法》《商用密码管理条例》等法律法规，并结合学习贯彻党的二十大精神开展研讨交流，明确职责任务，切实提高密码工作水平。

二是关键少数引领学，9 月 11 日，在 2023 年网络安全宣传周宝坻区启动仪式现场，设立“密码安全专区”，向区内各党政机关相关负责同志宣传密码知识。

三是全区机关跟进学。向全区 110 家机关单位线上推送密码法公益宣传片和宣传海报等，动员各单位通过组织专题学习、观看宣传视频、张贴宣传海报等形式开展学习教育，着力增强领导干部和机关工作人员的密码安全素质。

三、面向社会，广泛宣传

在企业、社区、学校积极开展形式多样的宣传活动，进一步扩大宣传覆盖面和影响力，增强广大群众的密码安全法治观念。一是做好线下集中宣传。在人流量密集的劝宝购物广场，通过设立展板、发放资料、现场答疑等形式，向市民宣传讲解《密码法》。

二是推进密码安全宣传向基层延伸。4 月 13 日，走进周良街道陈庄子村开展“4·15”国家安全教育宣传，通过举办密码知识讲座、互动交流答疑释惑等形式，向群众普及密码安全相关知识。

三是做好青少年教育引导工作。在宝坻区第一中学开展密码安全教育专题宣讲，向学生讲述密码工作红色历史，并组织师生扫码关注“国家密码管理局”公众号、学习强国“密码视界”学习平台，充分调动学生对密码知识学习的热情，增强爱国主义情感。

四、凝聚合力，扩大声量

积极沟通协调区内有关部门，凝聚合力，形成宣传声势，进一步加大对密码法律法规、密码基础常识的普及力度。4 月 8 日至 22 日，联合区委国安办、区委网信办、区国家保密局，组织开展国家安全网上知识竞答活动，得到全区广大群众积极响应，2 万余人次参与答题。以“网信宝坻”两微多端、“宝坻机关党建”“宝坻融媒”“法治宝坻”等区级政务新媒体矩阵为抓手，全方位、多角度宣传密码安全知识，推发《话说密码法，增强全民密码安全意识》《关于密码法，这些事儿都和你有关!》《商用密码管理条例》等重要稿件，10 月 26 日《密码法》颁布四周年之际，开设密码知识专栏，累计阅读量超过 3 万人次，持续推动密码安全意识深入人心。

供稿人：史馨怡

史馨怡，宝坻区国家密码管理局，四级主任科员。积极参与全区密码知识宣传普及工作，踏实肯干，责任心强。

天津市商用密码行业协会
第三期密码应用工作培训班成功举办

为贯彻《中华人民共和国密码法》和《商用密码管理条例》，提升重要领域密码应用广度和深度，落实信息化建设项目密码应用工作要求，学习掌握商用密码知识和政策法规，增强密码应用意识、厘清工作思路，天津市商用密码行业协会于 2023 年 12 月 14-15 日在天津光电科技园举办第三期密码应用工作培训班，会员单位及相关单位信息化工作负责人共计 50 余人参加培训。

本次培训内容涉及商用密码法律法规、《信息安全技术信息系统密码应用基本要求》(GB/T39786-2021)、密码应用安全性评估体系、量化评估与高风险判定规则解读，网络与信息系统密码应用方案编制、实施及密码应用典型案例分享等。

天津市商用密码行业协会秘书长胡双喜围绕《密码法》《商用密码管理条例》《商用密码应用安全性评估管理办法》对商用密码应用安全性评估进行讲解，他强调开展商用密码应用安全性评估是国家密码法律法规的明确要求，对于规范密码应用，切实保障网络安全，具有不可替代的重要作用。

云安科技李月老师对密码应用现状进行分析，

详细讲解了密码与信息系统安全、密评政策法规依据、密评规则与流程、密码应用改进等内容。

北京数字认证徐亚龙老师谈到，构建数字化是企业发展的重要趋势之一，密码助力企业数字化转型创新，并详细分析了国家对国有企业数字化转型提出的相关要求。

赢达信彭竹老师从密码产品的目标入手，对商密产品、商密方案进行了细致分析，讲解了密码基础产品在密码测评中的应用及优势。

灵创智恒朱勋老师通过背景、产品组成、标准规范、硬件架构、产品部署等方面对商用密码产品中签名验签服务器和安全认证网关进行了详细讲解。

云安科技徐士元老师以《密码应用安全风险与对策》为题，强调密码作为数据安全的重要基石，在推进数字经济健康、安全发展方面具有重要作用。

光电安辰姚嘉老师针对国密门禁系统、国密监控系统的建设、改造方案，以及国密堡垒机、服务器密码机产品功能、应用场景等内容进行了讲解。

宝牧科技邱锋老师以 VPN 架构为切入点，详细介绍了 VPN 的分类及 VPN 安全网关应用，强调了 VPN 为用户带来的节省资金、保障数据私有性及完整性等优势。

道普信息闫安老师围绕商用密码安全性评估情况、工作机制以及实施内容、实施计划、保障措施、经费概算等内容进行讲解，强调密评的重要性。

光电安辰杨林老师对密码应用需求展开分析，介绍了密码应用方案模板结构、设计流程，密码应用技术方案、管理方案，云上信息系统编制要点等内容。

本次培训内容丰富，参训人员纷纷表示，培训既让大家对相关法律法规及政策标准有了更加深入的理解，也为今后密评、方案编制等工作的开展提供了积极的指导意义。

天津商密协会在天津市国家密码管理局的指导下，始终秉承服务广大商密企业的宗旨，努力提供形式丰富、内容全面的培训课程，不断推进密码创新研究和人才培养，积极促进商用密码人才交流，在助力中国式现代化进程中为商密行业的发展持续贡献力量。

供稿人：陈旭杨

坚定行业发展信心
为强国复兴伟业提供有力金融支撑

恒银金融科技股份有限公司

时光走笔，岁月成章，又是一年冬来秋往。11月6日，恒银科技举行11月份升旗仪式，全体在津员工齐聚园区，迎着朝阳，面向国旗，高唱国歌，庄严肃立，满怀敬意。

升旗仪式结束后，党员移步党建厅。党员宣誓环节由党委副书记梁晓刚领誓，全体党员举起右拳，在党旗下重温入党誓词。

公司党委委员、总裁助理张雪晶作了以“为强国复兴伟业提供有力金融支撑”为主题的微党课分享。

张雪晶带领大家集体学习了中央金融工作会议精神。习近平总书记的重要讲话全面总结了党的十八大以来的金融工作，科学回答了金融事业发展的一系列重大理论和实践问题，提出了一系列新思想、新理念、新论断和战略举措，具有极强的政治性、思想性、战略性和实践性，为新时代推动金融高质量发展提供了根本遵循和行动指南。全体恒银人要切实增强责任感、紧迫感，认真学习贯彻会议精神，与开展主题教育充分结合起来、与企业主责主业结合起来、与谋划未来工作充分结合起来，切实把思想和行动统一到习近平总书记重要讲话精神和党中央决策部署上来，为建设金融强国、服务中国式现代化做出新的贡献。

聚力思变向未来，乘势笃行跃新峰。恒银科技坚定行业发展信心，坚守主业、做好主业，扎实推动“十八字经营方针”和“四个转变”落地落实，咬定业务目标不放松，心往一处想、劲往一处使、拧成一股绳，共同把公司做大、做强、做精。

供稿人：恒银金融科技股份有限公司党办

和平河北分公司党支部与中国通建天津通服党支部开展主题教育暨党建翼联实践活动

中国电信集团有限公司天津分公司

为进一步深入贯彻习近平新时代中国特色社会主义思想主题教育，牢牢把握“学思想、强党性、重实践、建新功”总要求，发挥文明单位示范引领作用，2023 年 10 月 25 日下午，由和平区文明办、和平区志愿服务联合会主办，天津电信和平河北分公司等多家单位共同参与的主题为“践行文明有礼 志愿你我同行”志愿服务广场日活动在和平区金街举办。和平河北分公司党支部与中国通建天津通服党支部的党建翼联活动同步开展，双方领导及部分党员代表出席了活动。

和平河北分公司通过文明共建模式全面融合开展本次活动，以党建引领、业务融入的方式，在集中学习和宣传实践的互动体验中，既开展政治理论学习，又将防诈等内容有机融入，共同营造了良好的文明共创氛围。

在活动现场，和平河北分公司及中国通建天津通服党员同志们齐力搭设了宣传场景，准备了宣传品与礼品并共同开展志愿服务活动，向来参加活动的广大群众介绍相关的知识，尤其对网络信息诈骗的方式和手段进行了透彻的展示和剖析，提示常见的诈骗手段，列举出有效的防范工具，提升了广大群众防范意识，避免财产损失，得到了现场群众的一致认可与好评，为活动奠定了热情与积极的基调。

此次文明共建志愿服务活动，开启了文明办、志愿服务联合会、电信公司多方的精神文明建设新模式，探索建立了党建融入社区基层一线，为民排忧解难的联动机制。同时，此次活动也是在区文明办、区企业、用户之间搭建沟通、交流、互动的桥梁和平台的一次有益尝试。

接下来和平河北分公司也将继续推进精神文明建设共建合作，发挥党建翼联优势，与区主管部门及核心企事业单位深度融合，提高电信的品牌影响力与业务水平，积极贯彻落实上级党组织对志愿服务的相关要求，实现融通互促的跨越式发展。

供稿人：刘美惠

麒麟软件“学思想 启新程 ‘麒’心向未来”主题辩论赛决赛圆满收官

麒麟软件有限公司

为深入学习贯彻习近平新时代中国特色社会主义思想，全面落实党的二十大精神，进一步推动主题教育实践活动走深走实，在中国电子党组和中国软件党委的坚强领导下，以青年素养提升工程为依托，12 月 14 日上午，麒麟软件 2023 年“学思想 启新程 ‘麒’心向未来”主题辩论赛决赛圆满收官。

双方队伍围绕“在打造世界一流企业进程中，麒麟软件应更倾向于以‘数字’为先驱扩大市场占有率和品牌影响，还是应更倾向于以‘价值’为先驱提升产品功能性和文化属性”进行决赛大比拼，呈现一场精彩绝伦的视听盛宴。麒麟软件科技委副主任兰雨晴，党委副书记刘浩驰，党委委员、高级副总经理程寨华，高级副总经理宋介鹏，高级副总经理洪苌婧作为嘉宾出席活动，并邀请公司副总经理李震宁作为点评嘉宾，相关部门负责人以及在京党支部书记、广大党员青年以现场 + 视频的方式观看了本场比赛。

赛场上，辩手们立足论点展开激烈的思辨，双方皆备战充足，引用大量理论知识及案例强化各自观点，你来我往、针锋相对，在一次次唇枪舌战的交锋之中抓住对方的破绽，依托扎实的理论积累和丰富的工作经验，展现出青年辩手强大的逻辑思维能力，赢得了场下观众的阵阵掌声和喝彩。

麒麟软件2023年“学思想 启新程 ‘麒’心向未来”主题辩论赛由所属 18 个党支部推选出共计 10 支代表队伍参赛，历时 2 个月，经过初赛、复赛、半决赛和决赛，最终由行业营销党支部选送的“麟麟麒队”成功夺冠，业务第二党支部选送的“林下之风队”获得亚军。除以上奖项外，职能第二党支部选送的“团团队”和职能第三党支部选送的“必须第一队”获得季军，杨旭、贾静、拓改改、赵晨、张蕊、任春喜、高飞驰、高昕、陈奕彤、周源获得“最佳辩手”。与会领导为以上获奖团队和个人现场颁奖并合影留念。

以辩促学，以辩促思。本次辩论赛不仅为麒麟软件青年员工们提供了一个展示自我的平台，也为他们锻炼自身能力提供了机会。同时，本次辩论赛是麒麟软件贯彻落实主题教育实践活动的一项重要举措，进一步坚定了公司青年员工的理想信念，不畏艰难、奋勇向前。麒麟软件将以践促学提本领，以学践行强使命，不断铸魂强基，真正淬炼出一支积极、健康、向上的青年队伍，坚守打造中国操作系统核心力量的初心使命，紧跟时代浪潮，团结奋进、锐意进取，为国产操作系统事业和企业高质量发展作出更大的贡献。

供稿人：麒麟软件有限公司天津事业部

中汽智联技术有限公司
党总支第二次党员大会成功召开

中汽数据（天津）有限公司

为进一步加强党的建设，按照第二批主题教育工作要求，10 月 16 日下午，中汽智联技术有限公司党总支召开党员大会，开展党总支委员增补选举工作并讲授主题教育党课。中汽数据党委书记史永万出席并讲话，中汽智联党总支委员张亚楠主持会议。

东丽会议现场

西青会议现场

大会严格按照党总支增补委员流程，通过无记名投票，选举增补中汽智联党总支委员。随后，中汽智联党总支书记杜志彬、网联党支部书记张亚楠、智能党支部书记赵帅分别为全体党员讲授专题党课。

杜志彬讲授专题党课

张亚楠讲授专题党课

赵帅讲授专题党课

史永万对本次党员大会进行指导点评，他强调，中汽智联党总支作为中汽数据改革创新先锋队，要进一步带动全体党员凝聚思想共识，营造浓厚主题教育学习氛围。下一步，中汽智联党总支将持续深化主题教育成果转化，为中汽数据、中汽智联实现高质量发展做出更大贡献！

供稿人：中汽数据（天津）有限公司党支部

基于信创平台的机房环境物理安全商用密码应用解决方案

天津光电安辰信息技术股份有限公司

一、方案应用背景

在信息系统中，存放应用服务器、数据库服务器等重要软硬件设备的机房、机柜等区域，是保证信息系统正常运作的关键区域。对于这些区域，需采用特定的技术和手段，来确保相关设备和设施免遭自然以及人为的破坏。目前，业内主要还是采取物理隔离、访问控制、视频监控、专人值守等传统安全防范手段进行防护。

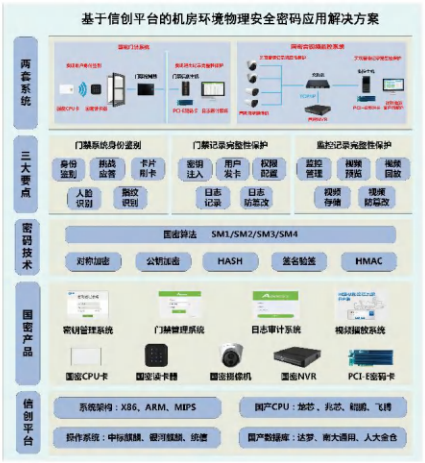
但上述传统安全防范手段所采用的密码产品、算法和技术，都存在各种各样的安全隐患，比如普通的门禁 IC 卡容易被复制，存在用户身份被假冒的风险；又比如门禁日志记录数据和监控音像记录数据未做完整性保护，或采用的密码算法为通用的国际算法，如 AES、DES、RSA、SHA1、MD5 等等，这些密码算法，其核心技术均为欧美国家所拥有，存在植入后门或被暴力破解的隐患，从而导致相关数据面临被截取和被篡改的风险。

为解决上述安全隐患，近年来，我国陆续颁布了《密码法》、《网络安全法》等相关法律法规，为我国重要网络信息系统的安全提供了法律保障，并开始大力推行网络安全等级保护、涉密信息系统分级保护、商用密码应用安全性评估等信息安全管理制度，为我国重要网络信息系统的安全构筑了多道防线。其中，根据 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》等国家标准要求，采用合规的商用密码产品、密码算法和密码技术，实现对信息系统机房物理环境等各个层面的安全防护，消除信息系统机房物理环境各个层面上所存在的安全隐患，更是实现商用密码应用规模化、产业化和市场化的重中之重。

另一方面，作为国家“十四五”发展目标的重要抓手，信创产业的发展也是势在必行，从信息基础设施国产化程度来看，国内重要信息系统中使用的核心产品和关键服务国产化进程不断加快。这就意味着：在未来很长一段时间内，越来越多的信息系统机房等关键区域，其所涉及的基础软硬件设备，如门禁系统、监控系统等等，必然要满足国产化的应用需求。

因此，基于上述情况，如何采用符合相关法律法规规定和标准要求的商用密码产品、算法和技术，设计开发可适用于国产 CPU、国产操作系统、国产数据库等信创平台软硬件环境的国密门禁系统和国密监控系统，搭建基于信创平台的机房物理环境物理安全商用密码应用解决方案，为信息系统机房的物理环境，提供高强度的、全方位的安全防护，是当前信息安全和商用密码领域所需要解决的首要问题。

二、方案简介



为解决上述问题，天津光电安辰推出了基于信创平台的机房环境物理安全商用密码应用解决方案，其基本框架如上图所示：

1、由信创平台，如 X86、ARM、MIPS 等硬件平台，龙芯、兆芯、鲲鹏等国产 CPU，麒麟、统信等国产操作系统，达梦、南大通用、人大金仓等国产数据库提供基础支撑平台。

2、采用经国家商用密码检测中心认证的国密

CPU 卡、国密读卡器、国密摄像机、国密 NVR、PCI-E 密码卡、密钥管理系统、门禁管理系统、日志审计系统、视频播放系统等密码产品提供底层软硬件支持。

3、采用经国家密码管理局审批的 SM1、SM2、SM3、SM4 系列国密算法，以及对称加密、公钥加密、签名验签、HMAC 等密码技术，实现基于信创平台的商用密码技术应用。

4、根据《密码法》、GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》等商用密码相关法律法规和标准要求，以及国家保密办 BMB48、公安部 GB/T 37078-2018、GB 35114-2017 等标准要求，并在实现门禁管理、权限配置、日志记录、监控管理、视频预览、视频回放等通用安防功能的基础上，重点实现门禁系统用户身份鉴别、门禁记录完整性保护、监控数据完整性保护这三点密码应用要求。

5、基于上述研发基础，输出国密高安全门禁系统和国密音视频监控系统这两套即可独立使用又可联合使用的国密级系统产品。

6、基于国密门禁系统和国密监控系统这两套系统级国密产品，最终形成一套完整的、基于信创平台的机房环境物理安全商用密码应用解决方案，实现基于信创平台的机房环境的全方位、高强度的安全防护。

三、方案部署方式

1、国密门禁系统安装部署

本方案包含国密门禁系统和国密音视频监控系统两套产品，其中，国密门禁系统安装部署方式如下：

(a) 在机房门禁后端信创主机上部署 PCI-E 密码卡，并安装部署门禁管理系统、门禁日志审计系统、密钥管理系统等软件；(b) 使用密钥注入器和发卡器对国密 CPU 卡进行密钥注入和发卡操作；(c) 在机房门禁前端安装部署国密门禁读卡器和门禁控制器，并为用户配发代表其身份的国密 CPU 卡；(d) 通过交换机将信创主机和门禁控制器连接起来，完成国密门禁系统的部署。

2、国密音视频监控系统安装部署

国密音视频系统安装部署方式如下：

(a) 在机房监控后端信创主机上部署 PCI-E 密码卡，并安装部署视频播放客户端软件；(b) 在机房监控前端安装部署国密网络摄像机和国密 NVR；(c) 通过交换机将国密网络摄像机、国密 NVR 和信创主机连接起来，完成国密音视频监控系统的部署。

按照上述方案完成国密门禁系统和国密音视频监控系统的部署之后，在进行商用密码应用测评时，在物理和环境物理安全层面，可获得满分 10 分。

四、方案典型应用案例

按照国家密码相关法律法规和标准的要求，本方案可应用于重要信息系统、关键信息基础设施等对国计民生有重大影响的信息系统所在的机房环境，包括且不限于基础信息网络、等保三级信息系统、重要工业控制系统、政务信息系统等各种重要基础信息系统，可广泛应用于委办局、公检法、金融、电力、教育、医疗、大数据、环保等各大行业和领域。

目前，本方案已成为商用密码领域物理和环境物理安全层面的领先示范型应用方案，已在全国多个行业得到推广和应用，获得了广大客户的高度认可和一致好评。

供稿人：姚嘉 13021347800

姚嘉，天津光电安辰信息技术股份有限公司产品总监，高级工程师，曾获天津市科技进步奖三等奖，主要负责公司商用密码产品的规划和研制，以及商用密码解决方案的应用和推广。

国芯科技安全芯片产品群为视频安防全生态安全提供解决方案

天津国芯科技有限公司

随着 GB 35114-2017《公共安全视频监控联网信息安全技术要求》的深入实施，越来越多的视频安防设备及系统厂商选用搭载了商用密码算法的安全芯片及安全模组来升级产品及系统的信息安全水平。作为国内领先的安全芯片供应商，国芯科技（证券代码688262.SH）的安全芯片、安全 TF 卡、高速 USBKey 以及 PCI-E 密码卡等系列产品组成的视频安防安全芯片产品群已经被中星电子、恒生、大华、宇视、科达等头部视频安防设备及系统厂商选用，并实现批量出货，得到了全生态合作伙伴的一致认可，助力了这些厂商视频安防业务的信息安全升级。

GB 35114-2017 规范的发布背景以及实施的必要性：视频安防系统是提高社会治安防控体系建设法治化、社会化、信息化水平的重要载体。然而，视频监控信息涉及个人隐私、企业机密和国家安全等多方面的问题，因此，制定相应的技术标准和管理规范，保障视频监控信息安全显得尤为重要。

在这样的背景下，GB 35114-2017《公共安全视频监控联网信息安全技术要求》应运而生。此标准由公安部提出，于 2018 年 11 月 1 日正式实施。该标准规定了公共安全领域视频监控联网视频信息以及控制信令信息安全保护的技术要求，适用于公共安全领域视频监控系统的信息安全方案设计、系统检测及与之相关的设备研发与检测。

GB 35114标准与我们熟知的GB/T 25724规范，GB/T 28181 规范有哪些区别和分工?

GB/T 25724 在媒体层规定了公共安全视频监控应用的数字视音频压缩编码的解码过程。该标准适用于公共安全领域的视音频实时压缩、传输、播放和存储等业务，其他需要视音频编解码的领域也可参考采用。

GB/T 28181 在协议层规定了视频监控系统（前端 / 平台 / 客户端）的互联架构和各个模块间的控制信令流程、协议接口等进行了规范；包含了对基于数字证书的接入认证、基于数字摘要的信令认证流程；但只支持 RSA、MD5、SHA 等国外加密标准的应用。

GB 35114-2017 在系统层对 GB/T28181 进行扩展，采用商用密码算法实现基于数字证书的接入认证和基于数字摘要的信令认证。完善了整体视频监控体系应用密码算法技术的安全架构，为视频监控安全体系的架构的具体实现提供了详细规范，是国际国内第一个视频监控联网信息安全方面的技术标准，对于保障视频监控联网信息的安全具有重要作用。

GB 35114 标准中，A 级 /B 级 /C 级各自的安全要求是什么?

能力	目标	关联标准	国密算法	A级	B级	C级
基于数字证书与管理平台双向身份认证能力	身份真实	GB/T 28181（SVAC）	SM2、SM3	✔	✔	✔
对视频数据签名的能力	视频真实（来源真实、内容真实、未被篡改）	GB/T 25724（SVAC）	SM2、SM3		✔	✔
视频内容加密	防止泄露	GB/T 25724（SVAC）	SM1/SM4、SM2			✔

A 级：应基于数字证书与管理平台双向身份认证的能力，达到身份真实的目标。B 级：在 A 级技术要求基础上，增加对视频数据签名的能力，确保视频数据身份真实、来源于真实设备，能够校验视频内容是否遭到篡改。C 级：在 A 级和 B 级技术要求的基础上，增加视频数据加密的能力，使视频数据在确保

身份真实、视频来源于真实设备、能够校验视频内容是否遭到篡改的基础上，达到对视频内容加密保护的目标。

视频安防系统依据 GB 35114 标准进行信息安全改造的难点是什么？

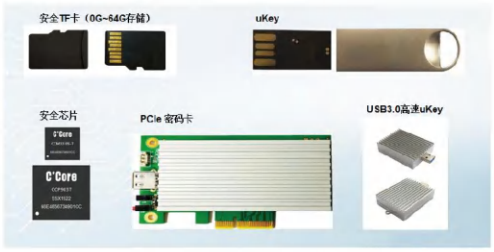
前端设备主要是各种摄像头设备：新摄像头设备可以通过 PCB 贴装安全芯片的方式实现信息安全改造；但是大量已安装的老摄像头无法重新 PCB 制版，此时，如何进行信息安全升级?此外，在项目实践中，还存在大量的因施工条件限制或者成本限制无法对前端摄像头设备予以升级改造的情况，又该如何处理？

安全管理平台以及 CA 认证系统：涉及多并发高速数据加解密，证书签发及认证等。这涉及全国上千个省市平台的建设，如何平衡建设成本，高性能高并发与高安全高可靠之间矛盾？

客户端 / 上墙大屏：通常四分屏或者九分屏需要支持多路并发加解密，需要适配各种操作系统，需要提供从 A 级到 C 级的安全功能，需要支持从 1 到 16 路高清（1080P）摄像加解密的性能分配，这种需求如何高性价比地解决？

高性能加密 / 脱密网关：视频安防的海量视频数据既是社会治安的保险池，同时也是一个待开发的数据宝藏，如何通过高速脱密网关向授权第三方提供视频数据资源，实现资源共享，数据增值？

国芯科技视频安防安全芯片产品群如何解决上述难点问题？经过 20 多年的厚积薄发，国芯科技在信息安全芯片及模块领域已拥有多项核心技术和知识产权。针对上述难点问题，国芯科技推出了视频安防安全芯片产品群，该产品群包括安全芯片、安全 TF 卡、高速 USBKey 以及 PCI-E 密码卡等系列产品，可完美解决视频安防系统依据 GB 35114 标准进行信息安全改造的难点问题。

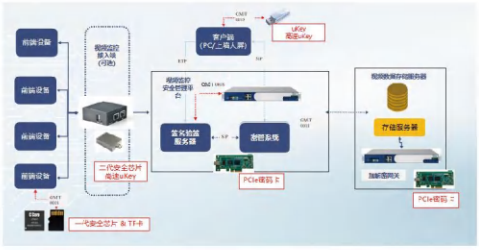


◆ CCM3310S-T 前端安全芯片：符合 A 级—C 级安全要求，支持 1—4 路加解密 / 签名验签，支持 2/4/8 颗并行处理 / 密钥同步，支持 USB2.0 通信接口和 SD2.0 通信接口，可以通过 PCB 贴片方式应用于摄像头前端，汇聚端网关盒子设备等。

◆ CCM3302S 安全 TF 卡产品：符合 A 级—C 级安全要求，支持 1 路数据加解密 / 签名验签，支持 0G—32G 前端设备支持本地加密存储，可应用于老摄像头的改造升级。

◆ CCM3305S 前端 / 汇聚端安全芯片以及高速 USB3.0 USBKey 产品：符合 A 级—C 级安全要求，支持 16 路加解密 / 签名验签，支持 2/4/8 颗并行处理 / 密钥同步，支持 USB3.0 通信接口和 SD3.0 通信接口，可以通过 PCB 贴片方式应用于汇聚端网关盒子设备，高速 USB3.0 USBKey 应用于客户端 / 上墙大屏的数据解密应用。

◆ CCP907T 服务器安全芯片以及 PCI-E 密码卡产品：符合 A 级—C 级安全要求，SM2 签名可达 6 万次 / 秒，SM4 加解密性能可达 20GbpS，可以支持 32 路—512 路高清摄像（1080P）数据加解密 / 签名验签。可应用于签名验签服务器，KMS 密管系统，以及高速加解密网关产品中。



根据国家主管部门的“十四五”视频安防规划，未来几年将会迎来大范围的、从上到下的公共安全视频监控联网依据 GB 35114-2017 标准的信息安全升级改造。国芯科技视频安防安全芯片产品群，为国家保障社会治安、维护国家安全、预防和打击犯罪站岗，为人民个人隐私、企业机密和数据安全护航，为全生态合作伙伴提供优秀的安全解决方案！

供稿人：李煜 18701069946

李煜，天津国芯科技有限公司信创和信息安全芯片事业部行业总监，商用密码以及集成电路行业 10 余年的 R&D、BD、Marketing 从业经验。负责云安全、物联网安全等行业的市场及销售工作。

数据库透明加密方案

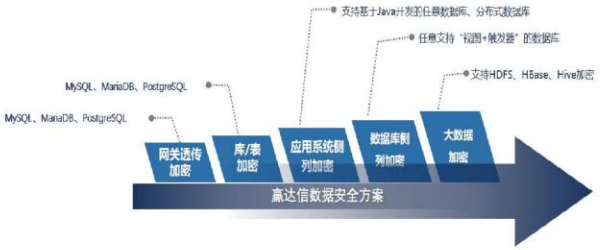
天津赢达信科技有限公司

密码应用改造的实施难度在于业务系统与密码产品的集成改造。业务系统厂商往往不熟悉密码应用，其沟通、实施成本较高。尤其是历史项目，难以协调业务系统开发商配合进行实施改造。

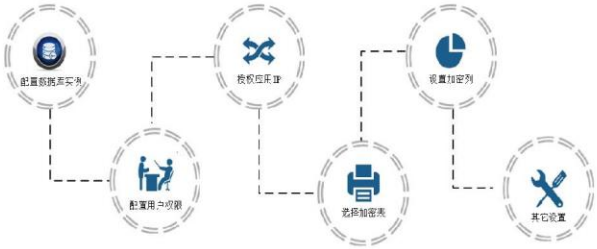
其中，在数据存储安全上，传统的数据存储加密要求业务系统调用密码机，实现数据存储的机密性、完整性，业务系统的改造工作量较大，增加了大量的沟通成本、时间成本和实施成本，导致项目进展困难、缓慢。一旦项目需求变更，所有的沟通、开发、实施需要再来一次。

因此，在数据存储安全上，其核心是实现数据库的“透明”加密，即不需要业务系统开发商做改造，就能实现敏感数据的机密性、完整性保护。

数据库的品牌繁多，不同的数据库的原理不同，因此，在实现数据库加密时，需要根据不同数据库的原理，采用不同的方式实现数据库加密。



天津赢达信科技有限公司利用数据库技术、数据库连接技术，综合使用不同的密码算法模式，针对不同的数据库，实现了表加密、应用系统列加密、数据库侧列加密。对于不同的数据库与不同的应用场景，支持采用最合适的方案实现数据库的存储透明加密。



在使用时，只需部署数据库加密管理系统，即可实现对数据库表空间级或列级别的数据透明、无缝加密，业务系统开发商无需进行任何开发，只需在服务器端进行配置、部署，即可实现基于国产密码算法的数据库加密，实现敏感数据的机密性、完整性保护。即对于业务系统和使用用户而言，数据库加密是“透明的”。

其中，采用 SM4-CBC 实现数据的机密性保护，采用 SM3-HMAC 实现数据的完整性保护，对于机密性和完整性都需要的字段，采用 SM4-GCM 算法，

可同时实现数据机密性和完整性的保护，并保证数据字段加密后的整体性能。

在列加密的密文检索上，赢达信通过自有的密文索引算法，实现了字符串的密文模糊查询、数值类的比较查询，在数据不解密的情况下支持多种条件的快速查询，可以避免全表扫描，可以在保证安全性的前提下保证性能，保证业务系统的可用性。

同时，对于手机号、身份证号等特殊格式的字段，支持基于 SM4 的保留格式加密，在加密后可直接进行密文的模糊查询，并做到性能无损。

在实际操作时，只需在数据库加密的管理端进行配置即可，其核心操作是选择需要加密的数据库实例，并进行“账号 + 权限”、加密表、加密列的配置。

在某些场景，典型的如医疗，数据库中的密文数据需要导出给第三方系统，此时，必须导出明文，否则第三方系统无法使用。赢达信数据库加密支持配置数据库连接的“账号 + 权限”，对于密文列，对于合法用户，导出的数据为明文，不影响第三方业务系统使用，对于非法用户，导出的数据为密文，可以同时保证数据的安全性和可用性。

同时，赢达信数据库加密支持不停机操作，即在业务系统运行时，可对数据库加密管理系统进行操作，直接选择加密表、加密列。允许在对历史数据加密时，业务系统不停机，此时，业务系统可以对密文数据字段插入新的数据，并对数据字段进行查询操作。

在数据库加密后，支持使用数据库自带的运维工具和第三方运维工具进行数据库的运维，即数据库加密不影响 DBA 的正常运维。

赢达信数据库加密实现了对关系型数据库的全线支持，包括但不限于达梦、人大金仓、神通、南大通用等国产数据库，以及 MySQL、MariaDB、Oracle、PostgreSQL、SQL Server、DB2、informix 等主流数据库的透明加密，并支持 MongoDB、GoldenDB 等分布式数据库。

赢达信数据库加密无需修改业务系统，即可实现数据库的透明加密，上线工作量小，可以实现数据存储加密的快速应用。

供稿人：彭竹 18601092821

彭竹，持有信息系统项目管理师（高级）、NPDP 国际产品经理、CISP（注册信息安全专业人员）等任职资格证书，曾获密码科技进步二等奖（省部级）。负责公司产品管理与对外合作。

周恩来亲手编制的“豪密”原理简单却从未被破译

从清末电报技术传入中国以来，曾出现过许多电报密码，最为著名也最为神秘的电报密码也许就是“豪密”。

熟悉我党历史的朋友都知道，周恩来因为革命工作保护身份的需要，曾用过很多化名，其中“伍豪”是他最早使用、也是最为人熟知的化名。

早在 1919 年五四运动爆发时，也就是 21 岁的周恩来就读于天津南开大学的时候，他就已经作为天津进步青年的领袖，开始领导天津的学生运动。1920 年初，周恩来创办的“觉悟社”出版了自己的刊物《觉悟》，他本人担任主编。为方便联络及确保工作的保密性，周恩来提出，觉悟社社员无论男女人人平等，为了公平起见，大家通过抽签的方式决定自己的笔名（化名），以号码的谐音取名。年纪最小的邓颖超抽到了“1 号”，于是取笔名为“逸豪”，周恩来抽到了 5 号，谐音“伍豪”，这个传奇化名就这样诞生了。

豪密，是中共早期无线电通讯中使用的密码，因其编制者为伍豪（周恩来）而得名。豪密是中国密码史上的一次重要技术突破，在中国革命中发挥了特殊的作用。这套密码随着“伍豪”这个化名，更增添了一份神秘色彩。

自清末到民国，政府、军队等部门在使用电报时，因其保密需要，一般都以明码为基础编制只有收发电报方持有的电码本，即密码。在密码的编制上，基本上都是参照明码编制办法，使用四位数字来对应汉字，与明码的区别只在于排列顺序上。这种类型的密码，在密码学上属于古典密码体制的“单表代替密码”，其优点是编制简便、使用方便，因而得到广泛使用。但是，这类密码却有保密性差的致命缺点，因其是以固定的数字对应汉字形式来传递讯息的，即同码同字，这势必使得某些使用频率高的汉字在电报中会重复出现，而截获电报的人只要对报文进行分析，特别是从重复出现的电码进行分析，就不难还原发送电报的密码。

民国时期，电报，特别是无线电报的应用更加广泛，密码技术却停滞不前，从北洋军阀混战时期开始，破译密码电报成为各派势力进行斗争的秘密手段。

1928 年，周恩来同志开始筹建中共的无线电通讯系统。当年夏天，他在莫斯科参加中共六大期间，向共产国际提出选派留苏的中共党员学习无线电通讯技术，得到共产国际的支持，选调毛齐华等六人参加了国际无线电训练班。在莫斯科，周恩来曾前去看望

学习无线电的中国学员，并说：“你们要抓紧学习，国内急需无线电通讯。”

回国后，周恩来调中央特科工作人员李强和张沈川在上海负责研制无线电台，第二年冬天即在上海、香港分别设立了电台，1930 年 1 月实现了沪港之间地下党第一次无线电通讯，这次通讯中双方使用了事先制定的密码，这也是中共第一次使用无线电密码。

当时，中共在各地的武装斗争风起云涌，在上海的党中央与各地苏区之间基本上还依靠交通员携带密写信件来沟通信息，这显然已不能满足斗争形势需要。

周恩来是中共无线电通讯工作的创始人和最早领导者。他一手开创了党的无线电通讯事业，在密码编制方面，他以惊人的智慧编制了党的第一部高级密码“豪密”，而由豪密确立的密码体制，成为革命战争年代党和军队核心机密安全的可靠保证。

陈琮英在回忆豪密时提到，“因为周恩来的聪明才智，他编的密码，好记好用，却极不容易破译。很长一段时间，国民党无可奈何，直到今天，我们的密码还是延用了‘豪密’的核心部分，换句话说，时间过去了七十多年，至今仍不落伍”。

密码作为机要通讯的核心部分，历来都是无线电技术侦察与保密斗争的关键所在，从这个角度来看，任何密码尤其是核心密码都会是敌人所着力攻破的，但豪密历经多年仍不落伍，不能不说是个奇迹。

那么，豪密究竟是什么样的?准确地说，豪密既是一部密码，也是一种密码体制。说它是一部密码，即专指 1931 年由任弼时携往中央苏区，与党中央通电报中使用的那部密码，这部密码因为年代过于久远，已无法找到原件，也不可能再现它本来的面貌；说它是一种密码体制，则是泛指根据最初那部豪密的原理编制的密码，在后来的应用中，凡是使用豪密原理的密码都称为豪密。

周恩来创造的豪密，在中国革命中发挥了特殊的作用。革命战争时期，党中央与各根据地、解放区之间的通讯联络主要依靠无线电台，正是有了豪密，才保证了党和军队无线电通讯的绝对安全，也正是豪密的使用，才使中共在对敌无线电斗争中始终掌握主动，夺取了隐蔽战线上的胜利。

基于联邦学习的入侵检测机制研究

Research on Intrusion Detection Mechanism Based on Federated Learning

天津大学 智能与计算学部

摘要：大数据时代的到来使得数据成为社会发展的重要战略资源。然而随着网络环境日趋复杂化，隐私泄露和恶意攻击事件层出不穷。联邦学习作为一种新型数据共享模型，能够在保护数据隐私的前提下进行数据共享，有效解决传统入侵检测模型的弊端。文章首先介绍了联邦学习及入侵检测模型的构成及特点，提出了基于联邦学习的入侵检测机制，并深入分析了该检测机制在检测准确率及效率上有效提升的可行性。通过对模型进行需求分析和设计，并以函数编程进行模拟仿真实验，实现原型系统开发。发现联邦学习机制能够在保证参与客户端数据隐私安全的前提下实现多方攻击行为日志的共享。同时通过多组控制变量的对照实验也证明基于联邦学习的入侵检测机制在检测准确率及效率上得到明显改善。

关键词：联邦学习；恶意攻击；入侵检测；网络安全

0 引言

大数据技术飞速发展，每天都会产生海量的数据。作为互联网的“燃料”，数据可谓十分重要。可是随着人们对数据安全与隐私问题的关注日益增加，数据的传播、聚合成了一个难题，数据孤岛现象日益严重[1]，数据的传输交流和隐私保护成了一对难以调和的矛盾。而作为当前人工智能研究与应用领域的热门技术，联邦学习技术的出现，展现出强大的打破“数据孤岛”的能力和用户隐私保护能力[2]。

同时，在复杂的网络环境下，为获取隐私数据而获利的攻击行为层出不穷，破坏作用越来越强大。因此针对各类网络攻击的入侵检测系统（Intrusion Detection System，IDS）便应运而生。然而传统的入侵检测技术检测的准确率与效率不足，因此本文引入联邦学习机制，利用联邦学习框架使得多方协作参与，在提高标签数据数量的同时保证了本地数据的安全性[3]，并对基于联邦学习的入侵检测系统进行探究。

1 相关概念

1.1 联邦学习

随着人工智能的利用率越来越高，产生了一个两难的局面，一方面机器学习需要以大量的互联网数据作为基石，另一方面近些年来世界各国越来越重视网络安全和隐私保护问题。在这样的实际背景条件下，联邦学习应运而生[4]。

联邦学习是一种分布式的机器学习技术，能够有效解决“数据孤岛”问题。在合法合规的基础上，参与各方处在一个联邦机制之下，共同协作，训练模型[5]。训练完成的模型在各个参与者的区域仅为本地的目标进行服务，在各方共建模型时不会暴露底层节点的隐私信息，因此能够保障数据隐私的安全。此外，联邦学习的每个参与方都具有相对平等的地位，对共建模型的适应程度完全取决于其贡献程度，即数据的质量与数量。

联邦学习主要可分为 3 类：横向联邦学习、纵向联邦学习和联邦迁移学习[6]。横向联邦学习即样本联合，适用于特征重叠多、样本重叠少的情况；纵向联邦学习即特征联合，适用于特征重叠少、样本重叠多的情况；联邦迁移学习，适用于特征重叠少、用户重叠少的情况。

联邦学习框架如图 1 所示，各个客户端在本地保留有完整的数据，同时拥有初始化的模型。每个客户端可单独通过本地数据对模型进行训练。但由于不同的客户端数据不同，训练出的模型将存在参数差异。

因此将不同的模型参数上传至云端，云端在完成模型参数的更新与聚合后各个客户端又可以下载新的模型进行训练。如此反复迭代，直至整个训练结果收敛。这样通过分布式的方法来训练模型，一方面减轻了网络通信的压力，另一方面也能保障用户数据不被泄露。

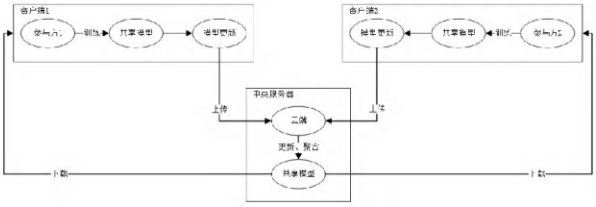


图 1 联邦学习网络框架

1.2 入侵检测

入侵检测主要指识别对计算机或网络信息的恶意行为，并对此行为作出响应。作为一种具有主动性的安全防护技术，入侵检测系统可以监视数据流、保护服务对象的安全 [7]。

入侵检测系统有很多类别，根据数据的来源可将入侵检测分为主机型、网络型两种 [7]。基于主机的入侵检测系统设置在主机上，将主机系统和本地用户作为数据源，主要涉及审计数据的获取及预处理；基于网络的入侵检测系统设置在网段的关键点进行流量监测 [8]，将原始数据包作为数据源，主要利用网络协议和工作原理对网络数据包进行捕获。根据分析方法可分为异常入侵检测和误用入侵检测两种 [7]。异常入侵检测定义一组正常访问的数值，建立正常访问模型。如果数据不符合这些特征，则被归纳为入侵行为。误用入侵检测是将所有违反安全策略的行为归纳为一个模型。如果数据中存在这些特征，则被归纳为入侵行为。此外还有很多种分类方法，在此不再赘述。

入侵检测系统在结构上可分为传感器、控制台两部分 [9]，如图 2 所示。传感器完成对流量数据的监测和分析，对恶意攻击行为进行报警处理，并做出相应的防御响应。控制台接收来自传感器的行为特征和分析结果，集成和存储数据，并设置传感器的参数。

图 2 入侵检测系统结构

入侵检测系统的模型如图 3 所示。主体（如计算机操作系统的进程等）将审计记录交付至规则集处理引擎，规则集处理引擎根据其既定的规则判断是否为入侵行为，若是攻击行为则采取防御措施。其规则由异常记录和活动简档决定，异常记录存储已发生过的入侵类别，活动简档存储正常活动的有关信息。如果新的审计记录并未有历史记录与之相匹配，则根据其是否导致网络入侵判断其为普通行为还是异常行为，并更新在相应的记录日志中。

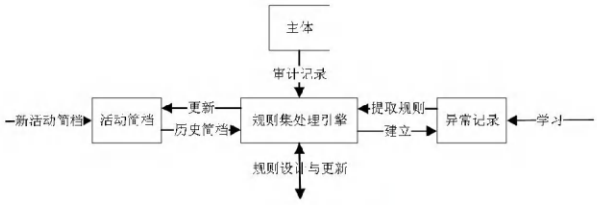


图 3 入侵检测系统模型

根据模型，IDS 的工作流程大体可分为防护、检测、响应三个阶段 [10]。防护阶段主要进行对大量网络流量信息的收集，信息收集是从不同的主机不同的网段中收集数据；检测阶段主要就是对搜集到的信息进行分析，从大量的信息中分析找出具有入侵行为特征的信息；响应阶段即检测到入侵后通知管理员系统或者采取一定的响应措施阻止该入侵继续。

1.3 联邦学习与入侵检测系统

对于单一的入侵检测系统而言，在一定时间内所能产生的异常行为标签非常有限，因此在面对大规模网络入侵时很难及时进行防御处理。而引入联邦学习机制以后多个参与方能够在同一时间进行训练并利用共享模型能够有效扩充入侵检测系统的行为记录日志，提升了入侵检测系统在复杂网络情况下的性能，有效缩短了训练时间。同时联邦学习是通过模型参数的形式将每个参与方在一次迭代后更新的模型上传至云端，经过云端对多方模型参数的整合后又重新下载至各个参与方，并不直接进行数据的传递，有效保证了数据的隐私和安全。

2 基于联邦学习的入侵检测系统

2.1 需求分析

随着人们对互联网依赖程度的提高，越来越多的隐私信息被上传到网络上保存。因此，隐私的窥探

从离线向在线转移，针对隐私安全的恶意攻击层出不穷。为了应对这种情况，需要一种网络保护机制来保护用户的隐私，因此，需要设计一个能够实时检测恶意攻击并保护用户的系统。但随着大数据时代的到来，网络流量呈现爆炸式增长，传统的入侵检测系统在检测成功率和效率上都存在不足。为了提高系统的检测成功率和效率，有必要对传统的入侵检测系统进行改造，实现隐私保护条件下的多方系统数据共享。因此引入联邦学习机制，在保护用户隐私和安全的前提下共享各参与方的数据，协调各参与方进行联合建模，提高各参与方检测的成功率和效率。

因此基于联邦学习的入侵检测系统需具有流量数据检测、数据处理与分析、分析结果判断与响应、行为数据存储、系统参数与标准设置等功能。同时在数据分析、结果响应、数据存储中引入联邦学习机制，提高系统检测效率。

同时基于联邦学习的特性，其需要在云端和多个客户端之间进行交互，因此本文基于网络型的入侵检测系统进行设计。

2.2 框架设计

整个基于联邦学习的入侵检测系统大致流程如图 4 所示。首先在网段上部署基于联邦学习的入侵检测系统，对于流经的数据进行捕获，然后对收集到的数据进行分析和预处理，判断其是否为入侵行为并存入日志。在此期间对于未记录过的新的行为特征利用联邦网络将其上传到共享模型中，经过迭代后重新下载共享模型，更新本地模型。最后对系统的分析结果进行响应，若为攻击行为则调用防御措施进行保护。

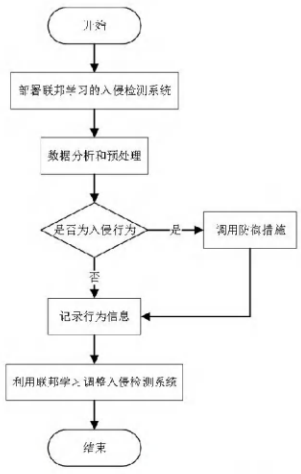


图 4 基于联邦学习的 IDS 流程

基于联邦学习的 IDS 在总体架构上可分为入侵检测和联邦学习两个模块。其中入侵检测模块参考 P2DR 模型 [11]，又细分为安全策略（Policy）、防护（Protection）、检 测（Detection）以 及 响 应（Response）4 个部分。安全策略作为入侵检测系统的总体指导思想，贯穿于整个 IDS 系统，规定了系统运行模式、参数等重要信息。防护部分根据返回的检测结果，采取相应的防护措施，保护检测主体不受入侵。安全策略和防护在结构上属于控制台的范畴。检测模块通过对行为数据流的监控，可以提取和分析行为数据的特征，发现恶意攻击。响应部分接收检测返回的行为数据的判断结果，并采取相应措施进行处理。检测和响应是互补的，在结构上属于传感器的范畴。因此整个基于联邦学习的 IDS 基本框架如图 5 所示，其中安全策略模块与联邦学习模块相连，通过联邦学习网络共享系统数据库和更新模型。

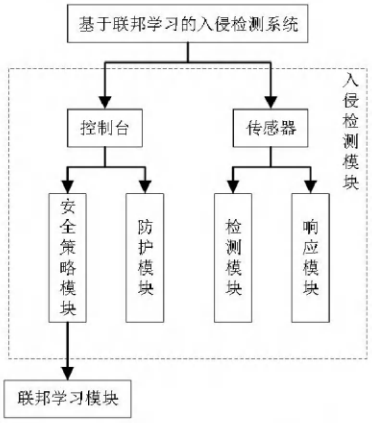


图 5 基于联邦学习的 IDS 框架

对于网络型入侵检测系统来说，检测方法分为基于标志的误用检测方法和基于异常情况的异常检测方法。前者需要建立入侵行为事件数据库，后者则需要建立正常行为事件数据库 [12]。考虑到一般情况下，通过监控点的异常流量数据远小于正常流量数据，因此本系统采用基于标志的误用检测方法，只记录恶意攻击事件的数据，减少了记录行为事件的工作量，节省了事件数据库资源，提高了系统的整体效率。

IDS 的详细结构模块如图 6 所示。在入侵检测模块中，入侵检测系统搭建在网段上接入流量必经节点，捕获流量数据信息，将获取的行为数据交付给行为数据分析器进行数据分析。行为数据分析器

一方面调用系统日志数据库来分析行为数据，若匹配成功则进行响应，若匹配失败则表示未检测到入侵行为，将此类行为数据存入系统日志中，并标记为未知类型 [13]；另一方面向响应器反馈分析结果，响应器在接受到判断为入侵的结果后则调用防火墙实时防御措施。系统日志数据库主要存储行为数据，并将新型攻击行为数据在经过数据脱敏预处理后上传至联邦学习网络中，同时能够定期从联邦学习网络中下载新的共享模型更新数据库。

在联邦学习模块中，可以将其分为各个参与方系统部分和中央服务器部分 [14]。其与入侵检测系统对接的客户端在一轮迭代中发起通信回合，上传入侵行为特征数据，即模型参数至中央数据库，使得局部参数更新。中央数据库接受入侵行为特征数据以后进行存储，并经过中央控制台的调用使得多个参与方的局部参数得以整合成新的全局模型。在中央控制台整合局部参数完毕后，中央控制台就能将全局模型共享至所有的参与客户端，而中央数据库则共享全局参数。

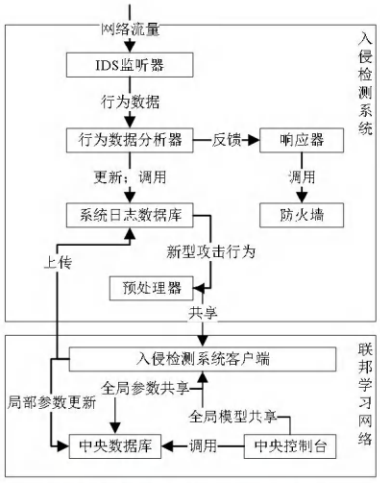


图 6 基于联邦学习的 IDS 结构

传统的基于标志的入侵检测系统是相对封闭的，它基于少量的入侵数据库样本，更新速度慢。本文设计系统在这方面得到了改进，在联邦机制下各个参与者的 IDS 数据库实现交互。新的攻击行为数据在本地提取，然后通过联邦网络共享。只要同一联邦系统中的其他参与者遭受新类型的攻击，上传并共享其模型参数，即使本地入侵检测系统从未面对过这类攻击，也能成功检测并实现防御，大大提高了入侵检测的成功率，削弱了入侵行为的攻击能力，增加了攻击者的攻击成本。

2.3 系统部署

因为入侵检测系统具有监听功能，其并不跨接在链路上，并且工作时不需要有流量流经此系统 [15]，所以在部署入侵检测系统的时候，将其跨接在所有需要监视的流量都必须流经的链路上是很重要的前提条件。

本文系统基于网络型的入侵检测系统进行设计，根据网络环境的不同，系统的部署方案也会不同。因此需考虑两种情况的网络环境：网络中没有部署防火墙的情况和网络中已部署防火墙时的情况 [16]。

对于网络中没有部署防火墙的情况，入侵检测系统一般部署在网络入口处的交换机上，以便于监听所有进出网络的数据包并进行相应的保护。对于网络中已部署防火墙的情况，入侵检测系统一般部署在防火墙之后，以便于实现在防火墙完成初次防御之后的第二次防御。但无论哪种方式，入侵检测系统都是部署在网络外的，而在网络前真正起防御作用的应该是入侵防御系统。

3 实验及分析

根据对基于联邦学习的 IDS 的理解，设计实验对联邦学习机制能够有效提高 IDS 的检测成功率和检测效率加以证明。本文设计了一个对照实验来模拟相同网络环境下恶意攻击的检测成功率。传统的入侵检测系统和基于联邦学习的入侵检测系统相比，通过改变攻击次数、攻击类型、参与联邦的入侵检测系统个数，探讨了影响检测成功率的参数条件，从而设计出更好的系统。

3.1 实验设计

实验程序分为 3 个模块：主函数模块、入侵检测模块和联邦学习模块。

主函数模块定义攻击轮次、攻击类型、攻击对象等参数，其中每一轮次的攻击类型和攻击目标通过随机数的方式生成。同时统计多轮次循环后的检测失败次数以及整个模型的训练时间对检测成功率以及检测效率进行计算。此外循环攻击部分需要调用入侵检

测模块。主函数模块的关键代码如下。

```
Function:main
Output:training_time,number_of_attacks,miss,success_rate
Begin
    number_of_attacks = 100;miss = 0;success_rate;training_time;type = 100;node =3; tag = 0;
    for (i = 0; i < number_of_attacks; i++){
        type_of_attack = random(type);
        target_of_attack = random(node);
        miss = miss + ids(type_of_attack, target_of_attack);
        if(tag==0) {
            if(miss == type) {
                print("i2 is: " + i);
                training_time = (i + 1) / number_of_attacks;
                print("proportion of training time: " + training_time);
                tag = 1;
            }
            else if(i==number_of_attacks-1) {
                print("i2 is: " + i);
                training_time = (i + 1) / number_of_attacks;
                print("proportion of training time: " + training_time);
                tag = 1;
            }
        }
    }
    print("attack num: "+number_of_attacks);
    print("miss: "+miss);
    success_rate = ( number_of_attacks - miss ) / number_of_attacks;
    print("success_rate = " + success_rate);
End
```

入侵检测模块定义分析器、数据库（行为日志）等基本系统配置，需要使用攻击类型和攻击目标两个参数进行调用。其中分析器使用contains函数模拟，数据库通过 set 容器表示，每一轮次检测中通过接收到的随机数（攻击类型）与数据库中已储存的整型数进行匹配，实现入侵行为的匹配检测。若匹配成功则表示成功检测到攻击行为，若发现无匹配则表示匹配失败，并将新的攻击类型通过 insert 函数以整型数方式存入 set 容器，实现数据库的更新。此外入侵检测模块能够调用联邦学习模块。入侵检测模块的关键代码及注释如下。

```
Function:ids
Input:type_of_attack,target_of_attack
Output:missing
Begin
    missing = 0;
    switch(target_of_attack) {
        case 0:{ //随机选择 ids_0 系统作为本轮攻击对象
            ids_0 = fed(ids_0);
            if (!ids_0.contains(type_of_attack)){
                missing++;
                ids_0.add(type_of_attack);
                ids_0 = fed(ids_0);
            }
        }
        break;
        case 1: //随机选择 ids_1 系统作为本轮攻击对象
            方法同 case0
        case 2: //随机选择 ids_2 系统作为本轮攻击对象
            方法同 case0
        return missing;
End
```

联邦学习模块定义云端服务器的数据库和模拟器，需要通过客户端（单轮攻击的攻击对象）作为参数来调用。数据库通过 set 容器进行表示，处理器根据 set 容器的 addAll 函数来模拟客户端入侵检测行为日志与中央数据库日志进行交互的过程，通过该集合操作规则模拟联邦网络中的数据共享。此外该模块能够接受入侵检测模块的调用。

联邦学习模块的关键代码及注释如下。

Setids_0,ids_1,ids_2,ids_center// 设置三组 set 类型集合分别表示 ids_0,ids_1,ids_2 三个入侵检测系统日志，ids_center 作为联邦结构的中央系统

```
Function:fed
Input:ids_n
Output:ids_n
Begin
        ids_center.addAll(ids_n);
        ids_n.addAll(ids_center);
        return ids_n;
End
```

3.2 结果分析

基于控制变量的思想，本文进行了四组控制实验，实验参数及实验结果如下：

1）在第 1 组对照实验中，我们将攻击次数和攻击类型总数都设为固定值，探讨在静态环境下引入联邦学习对入侵检测系统性能的影响。实验参数如表 1 所示，并进行了 10 组对照实验。

表 1 实验一参数

	攻击次数/次	攻击类型/种
基于传统的IDS	100	100
基于联邦学习的IDS	100	100

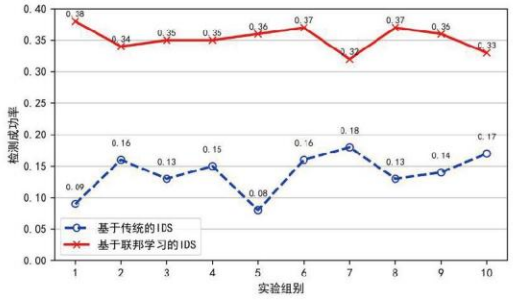


图 7 控制攻击次数和攻击类型实验结果

本组实验在控制攻击次数和攻击类型的基础上重复进行 10 组，对照实验的结果如图 7 所示。从图

中可以看出，基于传统的 IDS 平均成功率为 0.139，而基于联邦学习的 IDS 平均成功率为 0.353，可见在同等条件下，引入联邦学习机制可以提高有效入侵检测系统的检测成功率。同时可以发现联邦学习组的实验结果方差更小，组别之间的差异更为平均，具有更高的稳定性。

2）在第 2 组对照试验中，我们将攻击次数总数设置为定值，将攻击类型数量设置为从 100 到 1000 的十组等距递增。探讨在攻击次数总数不变、攻击类型动态变化的情况下，引入联邦学习对入侵检测系统性能的影响。实验参数见表 2，并进行了 10 组对照实验。

表 2 实验二参数

	攻击次数/次	攻击类型/种
基于传统的IDS	100	100→1000
基于联邦学习的IDS	100	100→1000

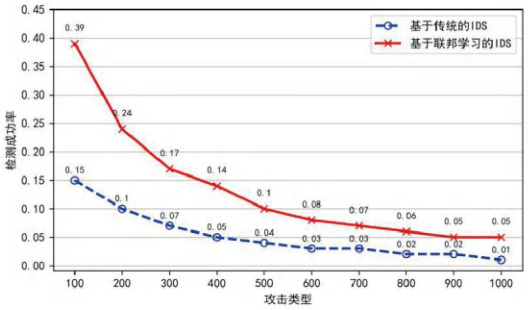


图 8 控制攻击次数改变攻击类型实验结果

本组实验在控制攻击次数为 100 的基础上以 100 为间隔从 100 至 1000 递增改变攻击类型，对照实验结果如图 8 所示。从图中可以看出，在不断变化的网络环境下，无论是传统组还是联邦学习组，恶意攻击类型越多，与入侵检测日志匹配的概率越小，使得入侵检测系统的检测成功率越低。在攻击类型总数较少的情况下，检测成功率对攻击类型总数的变化更为敏感。而当攻击类型达到一定数量后，检测成功率趋于稳定。此外对比两组实验结果还能发现在相同条件下，引入联邦学习机制可以提高入侵检测系统的检测成功率。

3）在第 3 组对照试验中，我们将攻击类型总数设置为定值，将攻击次数数量设置为从 100 到 1000 的十组等距递增。旨在探讨在攻击类型总数不变、攻击次数动态变化的情况下，引入联邦学习对入侵检测系统性能的影响。实验参数见表 4-2，并进行了 10 组对照实验。

表 3 实验三参数

	攻击次数/次	攻击类型/种
基于传统的IDS	100→1000	100
基于联邦学习的IDS	100→1000	100

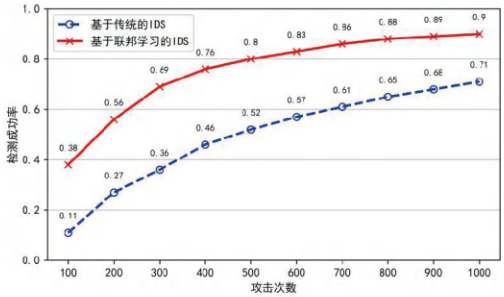


图 9 控制攻击类型改变攻击次数实验结果

本组实验在控制攻击类型为 100 的基础上以 100 为间隔从 100 至 1000 递增改变攻击次数，对照实验结果如图 9 所示。从图中可以看出，在相同的网络环境下，无论是传统组还是联邦学习组，入侵检测系统受到攻击的次数越多，其日志中存储的攻击行为数据样本越丰富，检测成功率越高。这是因为在攻击次数较少的情况下，检测成功率对攻击次数的变化更为敏感。而当攻击达到一定数量后，检测成功率趋于稳定。此外对比两组实验结果还可以发现在相同条件下，引入联邦学习机制可以有效提高入侵检测系统的检测成功率。

4）对于检测效率的探究，拟采用训练时间比例的形式，即在行为日志数据库中遍历所有攻击类型时所需要的攻击轮次占总设定的攻击轮次的百分比，对基于传统的 IDS 和基于联邦网络的 IDS 进行比较。

在第 4 组对照试验中，本文将攻击类型总数设置为定值。经过大量实验发现当攻击次数约为攻击类型的 5 倍时有极大概率确保行为日志数据库中能记录下所设定的所有攻击类型。因此将攻击次数数量设置为从 500 到 5000 的十组等距递增。旨在探讨在攻击类型总数不变、攻击次数动态变化的情况下，引入联邦学习对入侵检测系统效率的影响。实验参数如表 4 所示，并进行了 10 组对照实验。

表 4 实验四参数

	攻击次数/次	攻击类型/种
基于传统的IDS	500→5000	100
基于联邦学习的IDS	500→5000	100

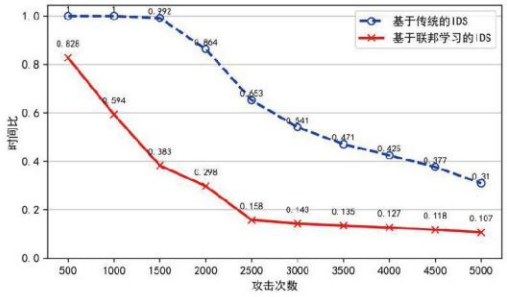


图 10 控制攻击类型改变攻击次数入侵检测效率实验结果

本组实验在控制攻击类型为 500 的基础上以 500 为间隔从 500 至 5000 递增改变攻击次数，对照实验结果如图 10 所示。从图中可以看出，在相同的网络环境下，无论是传统组还是联邦学习组，入侵检测系统受到攻击的次数越多，随机数模型越容易遍历所有的攻击类型，其日志中存储的攻击行为数据样本越丰富。当攻击次数达到一定数量后，就能遍历所有的攻击类型可能。而随着攻击次数的不断增加，遍历所有攻击类型所占时间比就越小，检测效率越高。而当攻击达到一定数量后，检测效率趋于稳定。此外对比两组实验结果还可以发现在相同条件下，引入联邦学习机制可以有效提高入侵检测系统的检测效率。

通过 4 组实验可以得出结论，基于联邦学习的 IDS 相较于基于传统的 IDS，无论是在遭受多次攻击的情况下，还是在不断变化的网络环境中，其检测成功率和检测效率都更加健壮和稳定。

4 结束语

自互联网发展以来，网络攻击入侵与与入侵防御一直处于不断博弈之中。而伴随着大数据技术的蓬勃发展，当今的网络环境日益多元化，传统的入侵检测系统已难以对复杂的网络流量进行侦测，因此引入基于联邦学习的入侵检测系统，通过分布式的机器学习方式以提高入侵检测系统的检测准确率及效率，同时保障各参与方的数据隐私安全。联邦学习是大数据时代连接数据孤岛、保护用户隐私的有效解决方案。入侵检测系统作为一种网络安全防御手段被广泛应用。结合联邦学习可以有效地提高入侵检测系统的效率，为网络安全领域做出贡献，这是未来发展的必然趋势。

但在未来需要更多面对的是能够使攻击者自身利益最大化的理性攻击。因此，仅用联邦学习仍具有其难以分析的劣势。还需不断引入更新的前沿技术加以辅助以使入侵检测系统更加健壮，相关的完善工作还任重而道远。

参考文献：

[1] MA Aiping.AI Training Meets Privacy Problem Federal Learning Opens up Data Island in This Way[N].Science and Technology Daily,2019-11-19（5）.

马爱平 . AI 训练遇隐私难题 联邦学习这样打通数据孤岛 [N]. 科技日报 ,2019-11-19（5）.

[2] WANG Yakun.Survey of Federated Learning Technology for Data Sharing and Exchange[J].Unmanned Systems Technology,2019,2(6):58-62.

王亚珅 . 面向数据共享交换的联邦学习技术发展综述 [J]. 无人系统技术 ,2019,2(6):58-62.

[3] WANG Rong,MA Chunguang,WU Peng.Intrusion Detection Method Based on Federal Learning and Convolutional Neural Network[J].Netinfo Security,2020,20(4):47-54.

王蓉，马春光，武朋 . 基于联邦学习和卷积神经网络的入侵检测方法 [J]. 信息网络安全 ,2020,20(4):47-54.

[4] YANG Qiang.Federal Learning: the Last Mile of AI[EB/OL]. http://kns.cnki.net/kcms/detail/23.1538.tp.20200317.1133.002.html,

2020-05-20.

杨强．联邦学习：人工智能的最后一公里[EB/OL]. http://kns.cnki.net/kcms/detail/23.1538.tp.20200317.1133.002.html, 2020-05-20.

[5] PAN Biying,QIU Haihua,ZHANG Jialun.Research on Federated Machine Learning with Different Data Distribution[C].TD Industry Association.Proceedings of 5G Network Innovation Seminar (2019), August 15,2019, Beijing ,China.Beijing:Mobile Communications ,2019: 271-276.

[6] PAN Rusheng,HAN Dongming,PAN Jiacheng,et al.Visualization of Federated Learning: Challenges and Framework[J].Journal of Computer-Aided Design & Computer Graphics,2020,32(4):513-519.

潘如晟，韩东明，潘嘉铖，等．联邦学习可视化：挑战与框架 [J]. 计算机辅助设计与图形学学报，2020,32(4):513-519.

[7] HUANG Zhenhao.Design and Implementation of Network Intrusion Detection [J].bulletin of science and technology,2019,35 (12):82-86.

黄振昊．网络入侵检测的设计和实现方案 [J]. 科技通报 ,2019,35(12):82-86.

[8] WANG Yan.Design of Network Intrusion Data Detection System Based on Big Data Analysis[J]. Computer Knowledge and Technology,2019,15(19):56-58.

王岩．基于大数据分析的网络入侵数据检测系统设计 [J]. 电脑知识与技术 ,2019,15(19):56-58.

[9] ZHANG Weihua.Design and Development of Network Intrusion Testing System[J].-Network Security Technology & Application,2020,20(1):11-14.

张卫华．网络入侵测试系统的设计与开发 [J]. 网络安全技术与应用 ,2020,20(1):11-14.

[10] HU Jian,SU Yongdong,LI Chao,et al.Research on Intrusion Detection System Based on Machine Learning[J].Information & communication,2019,26(11):163-164.

胡健，苏永东，李超，等．基于机器学习的入侵检测系统探究 [J]. 信息通信 ,2019,26(11):163-164.

[11] YANG Qiang, LIU Yang, CHEN Tianjian, et al. Federated Machine Learning: Concept and Applications[J]. ACM Transactions on Intelligent Systems and Technology (TIST), 2019, 10(2): 1-19.

[12] CHAUHAN H, KUMAR V, PUNDIR S, et al. A Comparative Study of Classification Techniques for Intrusion Detection[C]// IEEE.2013 International Symposium on Computational and Business Intelligence, August 24-26, 2013, New Delhi, India.New York: IEEE, 2013: 40-43.

[13] MULAY S A, DEVALE P R, GARJE G V. Intrusion Detection System Using Support Vector Machine and Decision Tree[J]. International Journal of Computer Applications, 2010, 3(3): 40-43.

[14] Mcmahan H B, MOORE E, RAMAGE D, et al. Federated Learning of Deep Networks Using Model Averaging[EB/OL]. https://arxiv.org/pdf/1602.05629v1.pdf, 2016-02-17.

[15] GUO Chuxu,SHI Yong,XUE Zhi.Port Scan Intrusion Detection Based on Machine Learning[J].Communications Technology,2020,53(2): 421-426.

郭楚栩，施勇，薛质．基于机器学习的端口扫描入侵检测 [J]. 通信技术 ,2020,53(2): 421-426.

[16] YANG Dongxiao,XIONG Ying,CHE Bichen.Network Intrusion Detection and Prevention[M].Beijing:Tsinghua University Press,2020.

杨东晓，熊瑛，车碧琛．入侵检测与入侵防御 [M]. 北京：清华大学出版社，2020.

供稿人：许光全 18649079199

许光全，天津大学教授、博导。主要研究方向包括信任管理、网络与信息安全、安全隐私与信任、可信计算、人工智能安全等，长期从事智能空间下信任、安全与隐私有关的研究工作。

天津市非涉密市级政务信息化项目建设规范和全周期管理培训会成功举办

天津市商用密码行业协会

2023 年 10 月 17 日，天津市商用密码行业协会联合天津市大数据管理中心成功举办了非涉密市级政务信息化项目建设规范和全周期管理培训会。此次培训旨在提高政务信息化项目的建设水平和管理效能，推动政务工作向数字化、智能化和高效化方向发展。

培训会由天津市商用密码行业协会秘书长胡双喜主持

培训开始，市大数据管理中心研发运维二中心徐主任就政务信息化系统如何运用先进的信息技术，提升政务工作效率，优化公共服务体验，加强政府监管和决策支持等工作做了简单介绍。

培训内容涵盖了政务信息化项目的建设理念、发展规划、技术应用、安全管理、密码应用安全性评估等方面，针对非涉密政务信息化项目的建设全周期管理进行了深入的探讨和交流。

市大数据管理中心胡老师围绕天津市政务信息化项目建设规范和方法、天津市大数据管理中心对非涉密市级政务信息化项目建设的全周期管理、项目建

设过程中需要考虑的其他关键点等内容进行讲解，详细阐述了政务信息化项目在规划、设计、开发、实施及运维过程中的规范和要求以及管理方法、技巧，重点在介绍了如何规划项目、如何进行有效的项目控制、如何保证项目的质量和安全等内容。

天津云安科技杨老师就密评工作中商用密码应用等级、编制商用密码应用方案、准备测评工具和资料、进行现场测评、分析和报告编制等多个工作环节进行了耐心的讲解，她强调商用密码应用安全性评估是加强和规范商用密码应用的重要抓手，是深化商用密码“放管服”改革、加强事中事后监管的重要手段，也是重要领域网络与信息系统运营者和主管部门必须承担的法定责任。

此次培训得到了参会人员的一致好评。大家表示，通过这次培训，不仅加深了对政务信息化项目的理解，还学到了许多实用的管理方法和技能。同时，也认识到了政务信息化项目在推动政府数字化转型中的重要性和紧迫性。

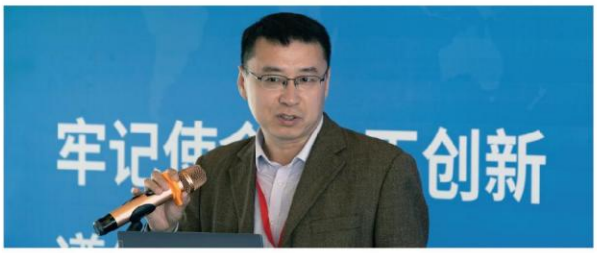
供稿人：陈旭杨

2023太湖密码论坛成功举办 天津商密协会受邀参加

天津市商用密码行业协会

10月23日，2023太湖密码论坛在江苏无锡召开。本次论坛作为 2023 物联网密码应用峰会系列活动之一，由全国密码协会（筹）主办，江苏省商用密码产业协会、深圳市商用密码行业协会共同承办。本次论坛以“全面贯彻落实《商用密码管理条例》，推动商用密码事业高质量发展”为主题，邀请行业主管部门、业内资深专家及全国 22 家行业协会主要负责人围绕如何贯彻落实《密码法》、《商用密码管理条例》，促进密码产业合作与发展、倡导行业自律和诚信经营、开展人才培养与技术创新、推动密码应用与测评、服务商密企业等内容进行交流，展开了热烈讨论。

会上，深圳市商用密码行业协会会长李大为作了题为《发挥行业协会作用，以密码技术创新助力数字经济发展》的主题报告。强调了行业协会要在宣传贯彻密码政策法规，加强密码行业规范和企业自律管理，培养密码领域专门人才，打造密码行业内和行业间合作的专业性平台，搭建企业与政府之间的沟通交流的桥梁等方面发挥充分的作用，同时提出了在新形势下行业协会应凝聚各方力量，形成密码应用推进工作的合力；组织编制有地方产业特色的密码团体标准两方面的工作建议。



张秋璞副会长代表天津市商用密码行业协会围绕贯彻落实《密码法》、《商用密码管理条例》，依法推动密码工作创新发展，加强行业监督管理，规范行业发展秩序，搭建多领域交流合作平台，开展密码人才培育工作，发挥协会职能服务企业等方面对天津商密协会的发展情况做了简要分享。他强调，天津商密产业在产品种类、行业标准建设、产学研融合、多平台搭建等工作上取得了一些阶段性成果，十分欢迎各位领导、专家、密码同仁到海滨城市天津调研，互相学习、交流经验，共筑商密蓝图。

最后中国密码学会副理事长兼秘书长安晓龙发言，就社会组织加强政治引领能力；加强科技创新及产业供给能力；加强行业自律等方面提出期望，希望发挥好社会组织的平台桥梁作用，提供高质量密码服务和安全保障，为商用密码高质量发展做出贡献。

天津商密协会与天津市保密工作协会联合开展“共话津门安全 共探融合发展新模式”座谈会

天津市商用密码行业协会

为贯彻落实党的二十大精神和习近平总书记对网络安全及信息化工作的重要指示，深入施行《中华人民共和国保守国家秘密法(修订草案)》《密码法》《商用密码管理条例》，天津市商用密码行业协会与天津市保密工作协会于 2023 年 10 月 27 日联合开展“共话津门安全 共探融合发展新模式”主题座谈会。

市保密局韩处出席座谈会，谈到在符合国家政策的前提下，欢迎科技企业将科技成果、研发技术与保密工作实际相结合，满足用户需求。同时，要加强商密与保密之间的联合，满足保护国家秘密、工作秘密等的要求。

市保密局伏熙以《如何通过保密科研助力科技企业健康发展》为题谈到，在互联网、大数据、云计算、人工智能、区块链等新技术、新应用层出不穷的现状下，保密工作必须适应日新月异的新形势，结合新保密法征求意见稿，用好保密科研项目，积极参与科研项目申报，面向全国市场，科学统筹，形成保密科技创新强大合力。

天津市商用密码行业协会秘书长胡双喜介绍市商密协会发展情况

天津市保密工作协会张亦驰介绍市保密协会发展情况

参会企业代表围绕各自公司业务发展情况、科技研发情况、研发成果应用等内容轮流进行发言，并从保密、

商密应用前景及用户需求等方面开展交流探讨，大家纷纷表示，畅通高效的信息沟通平台加强了会员单位之间的沟通协作，有助于促进天津保密、商密行业结构优化升级。

座谈会立足行业实际发展情况，聚焦保密、商密两产业融合应用，从科研创新、解决方案、应用实践等角度开展研讨，共探转化落地新模式，共同推进密码技术在网络安全工作中的创新应用与发展。未来，商密协会和保密协会将进一步发挥社团桥梁纽带作用，发挥宣传、引导、服务和交流职能，组织和推动商密、保密理论与实践研究，跟踪研究商密、保密技术领域的新成果、新进展，积极组织开展业务合作和友好交往活动，持续推动天津市商密、保密事业科学发展，为维护国家安全和利益做出贡献。

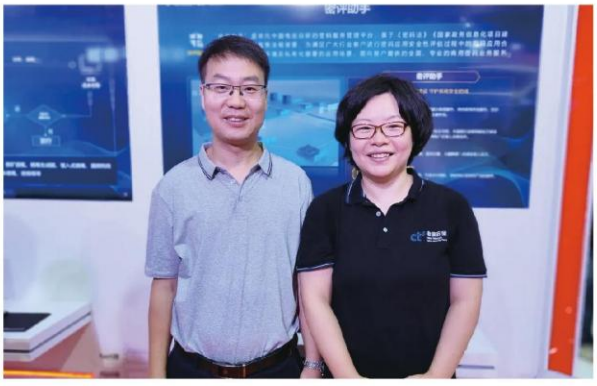
供稿人：陈旭杨

天津市商用密码行业协会受邀参加2023数字科技生态大会

天津市商用密码行业协会

11 月 10 日，中国电信与广东省人民政府在广州联合举办“2023 数字科技生态大会”。本次大会以“数字科技、焕新启航”为主题，聚焦数字中国建设领域，推进科技创新能力发展，聚合生态伙伴展示新型数字基础设施建设成果，携手共商数字科技发展新愿景。

天津市商用密码行业协会受会员单位天翼安全科技有限公司邀请参会。



大会期间，中国电信作为数字生活领域的布局者，在天翼数字生活与天翼视联展区设置科创能力、天翼视联、数字家庭、智慧社区、数字乡村五大板块，携多项数字化领域最新技术及应用成果亮相，其中诸多亮点引人关注。

大会期间，作为 2023 数字科技生态大会“十大主题论坛”之一，由中国电信集团有限公司网络和信息安全管理部、天翼安全科技有限公司主办，中国通信企业协会协办的“数字安全论坛”成功举办。

本次论坛围绕“数字安全，智享未来”这一主题，邀请数字安全生态行业同仁和生态合作伙伴，专题探讨国内数字安全领域的新理念、新技术、新成果、新做法；发布行业白皮书，对数字安全前沿技术趋势进行探讨；同时还邀请了产业链上下游合作伙伴，分享数字安全创新实践，共话数字安全趋势，共筑网信安全体系，推动新时代新征程网信事业高质量发展。

飞腾腾珑E2000助力天津地铁11号线全线路AFC系统投入运营

飞腾信息技术有限公司

近日，天津地铁 11 号线一期东段正式开通初期运营，全线基于飞腾腾珑 E2000 CPU 的 AFC 自动售检票系统在天津地铁整段投入使用，这标志着天津地铁首次在整条线路上实现了自动售检票系统（AFC）的全国产化，将为天津轨道交通发展注入新动能。该线路也是国内首条全线路 AFC 系统采用飞腾腾珑 E2000 CPU 的轨道交通项目。

本次开通的天津地铁 11 号线，是天津市开通的第 10 条地铁线路，也是落实“京津冀一体化”战略、打造“轨道上的京津冀”的重点项目。该线路西起南开区复康路与水上公园西路交口的水上公园西路站，东至东丽区津塘二线与六经路交口的东丽六经路站，共设置 21 座车站，本次初期开通运营东江道站至东丽六经路站，共 11 座车站，开通线路全长 13.68KM。

作为最新投用的一条地铁线路，该线路全部车站的 AFC 系统（包括 AGM 自动检票机、iBOM 自助票务终端、TVM 自动售票机、BOM 半自动售票机），均采用基于飞腾腾珑 E2000 CPU、麒麟操作系统的数城科技全国产化工控机，实现了整个售检票系统的全国产化。

作为飞腾自主研发的最新一代高端嵌入式处理器，飞腾腾珑 E2000 采用柔性设计，最高主频可达 2.0 GHz，同时支持飞腾自主定义的安全架构规范，从硬件层面增强了芯片的安全性。该线路将为天津地铁打造安全、智能、绿色、低碳的地铁出行体验，助力天津地铁实现全面升级。

早在 2019 年底，基于飞腾 FT-2000/4 CPU 的地铁 AFC 系统首次在天津地铁 5 号线顺利应用，至今已稳定运行达 4 年。此次天津地铁 11 号线全线采用飞腾腾珑 E2000 CPU，功耗更低、性能更强，进一步提升了系统自主性、安全性和稳定性。

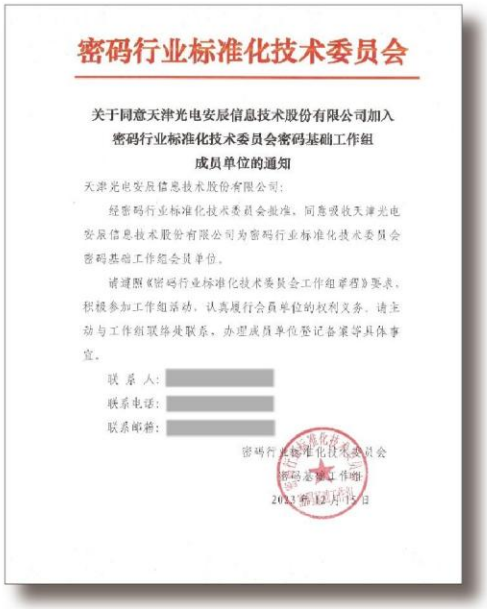
目前，飞腾腾珑 E2000 CPU 已相继在武汉、福州、重庆等城市的地铁 AFC 系统实现部署或应用。同时，在城市轨道交通领域，除了 AFC 系统，飞腾携手生态伙伴研发的列车牵引控制系统、信号系统、综合监控系统（ISCS）、掘进设备 SCADA 系统，已经落地应用或具备应用条件，用中国芯服务社会。

本次天津地铁 11 号线的顺利开通，标志着基于飞腾 CPU 的国产化产品与方案又一次得到了行业充分的检验和验证，将为更多新建线路和旧线改造积累丰富的经验。飞腾公司将不断提升产品算力水平，携手产业链上下游，共同夯实轨道交通行业算力底座，助力数字中国高质量发展。

供稿人：董毅 13920484526

光电安辰获批成为密标委基础工作组成员单位

天津光电安辰信息技术股份有限公司



密码行业标准化技术委员会

关于同意天津光电安辰信息技术股份有限公司加入密码行业标准化技术委员会密码基础工作组成员单位的通知

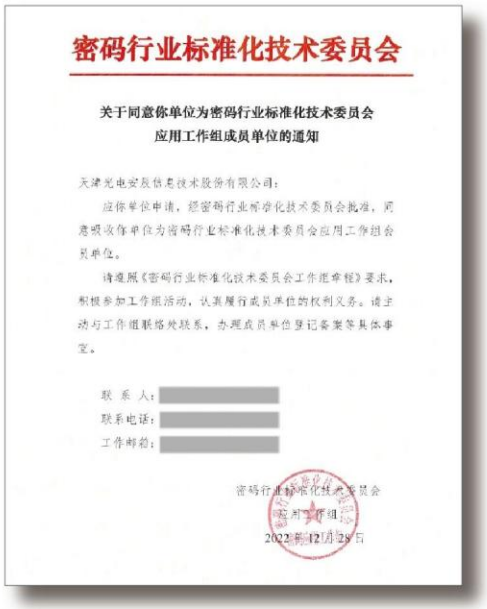
天津光电安辰信息技术股份有限公司：

经密码行业标准化技术委员会批准，同意吸收天津光电安辰信息技术股份有限公司为密码行业标准化技术委员会密码基础工作组会员单位。

请遵照《密码行业标准化技术委员会工作组章程》要求，积极参加工作组活动，认真履行会员单位的权利义务。请主动与工作组联络处联系，办理成员单位登记备案等具体事宜。

联 系 人：
联系电话：
联系邮箱：

密码行业标准化技术委员会
密码基础工作组
2022年12月15日



密码行业标准化技术委员会

关于同意你单位为密码行业标准化技术委员会应用工作组成员单位的通知

天津光电安辰信息技术股份有限公司：

应你单位申请，经密码行业标准化技术委员会批准，同意吸收你单位为密码行业标准化技术委员会应用工作组会员单位。

请遵照《密码行业标准化技术委员会工作组章程》要求，积极参加工作组活动，认真履行成员单位的权利义务。请主动与工作组联络处联系，办理成员单位登记备案等具体事宜。

联 系 人：
联系电话：
工作邮箱：

密码行业标准化技术委员会
应用工作组
2022年12月28日

近日，经国家密码行业标准化技术委员会（简称：密标委）批准，继成为密标委应用工作组成员单位之后，光电安辰又获批加入密标委基础工作组成员单位。

国家密码行业标准化技术委员会是经国家标准化管理委员会和国家密码管理局批准设立，在密码领域内从事密码标准化工作的非法人技术组织，主要从事密码技术、产品、系统和管理等方面的标准化工作。目前下设秘书处和总体、基础、应用、测评四个工作组，是我国密码行业唯一标准化组织。自成立以来，密标委深入贯彻落实党中央、国务院重大决策部署，以为保障我国网络和信息安全为目标，制定发布了一系列行业标准，并积极推动国际标准化活动。

光电安辰获批成为密标委基础工作组和应用工作组的成员单位，既彰显了光电安辰从事密码事业的坚定决心，也展现了其在密码领域的综合实力。密码是保护国家安全的重要战略资源，尤其是在新一代信息技术的推动下，网络安全形势愈发复杂。如何保障数据安全越来越受到人们的重视，关键技术支撑之一就是密码技术。

光电安辰长期专注于密码技术创新和密码产品研发，通过数十年的技术累积，在密码产品，如国密门禁系统、国密监控系统、国密堡垒机、服务器密码机、VPN 综合安全网关、手机盾协同签名系统等基础密码产品，以及密码应用解决方案，包括整体解决方案和物理安全解决方案等相关领域取得了一系列技术突破和成果，积累了大量的理论知识和丰富的实践经验。

未来，光电安辰作为密标委基础工作组和应用工作组的成员单位，将在密标委的领导下，光电安辰将充分发挥公司在密码领域的研究实力和应用创新能力，积极参与密码国家标准和行业标准的制修订工作，加强与行业专家学者、各成员单位的交流与合作，为密码行业标准化工作和标准成果的落地应用贡献应有的力量。

供稿人：姚嘉 13021347800

中汽研软件测评（天津）有限公司荣获“国家知识产权优势企业”

中汽研软件测评（天津）有限公司

2023 年 11 月 29 日，国家知识产权局发布了《国家知识产权局关于确定 2023 年新一批及通过复核的国家知识产权示范企业和优势企业的通知》，中汽研软件测评（天津）有限公司（以下简称“软件测评中心”）成功获评“国家知识产权优势企业”，这是软件测评中心获批的首个知识产权国家级资质。

国家知识产权局

国知发运字〔2023〕201号

国家知识产权局关于确定2023年新一批及通过复核的国家知识产权示范企业和优势企业的通知

各省、自治区、直辖市和计划单列市、新疆生产建设兵团知识产权局，四川省知识产权服务促进中心，各有关单位：

为深入贯彻落实《知识产权强国建设纲要（2021—2035年）》和《“十四五”国家知识产权保护和运用规划》决策部署，根据《国家知识产权局办公室关于面向企业开展2023年度知识产权强国建设示范工作的通知》（国知办函运字〔2023〕372号）要求，经企业申报、初次测评、地方知识产权管理部门推荐、国家知识产权局审核并公示，确定730家企业为新一批国家知识产权示范企业（名单见附件1），2980家企业为新一批国家知识产权优势企业（名单见附件2），培育期限为2023年11月至2026年10月；确定88家国家知识产权示范企业（名单见附件3）、338家国家知识产权优势企业（名单见附件4）通过复核，与2022年通过复核的企业一并继续作为国家知识产权示范企业或优势企业资格，培育期限分别为2022年10月至2025年9月。

我局将进一步加大政策协同支持力度，鼓励将企业重点工作部署，组织企业深入参与专利转化运用专项行动方案（2023—2025年）》实施，强化通过实施来培育、通过实施来评价的企业知识

产权能力提升工作机制，引导和支持企业有效运用知识产权提高核心竞争力，推动产业高质量发展，有力支撑知识产权强国建设。各地方知识产权管理部门要强化知识产权强国建设示范工作和专利转化运用专项行动的统一部署，结合地方工作实际，进一步完善本地区优势示范企业梯度体系，加大工作指引、政策支持、保障投入力度，加强对企业的针对性指导和服务。各知识产权优势示范企业要结合自身发展定位，制定切实建设工作方案，明确建设任务和目标，建立健全知识产权工作领导和保障机制，切实发挥优势示范引领带动作用，全力加好专利转化运用专项行动重点任务落实，不断提升知识产权运用效益和竞争优势，努力打造知识产权强企建设第一方阵。

特此通知。

附件：1. 2023年新确定的国家知识产权示范企业名单
2. 2023年新确定的国家知识产权优势企业名单
3. 通过复核的国家知识产权示范企业名单
4. 通过复核的国家知识产权优势企业名单

国家知识产权局
2023年11月29日

（此件公开发布）

国家知识产权局办公室　　2023年11月29日印发

—2—

“国家知识产权优势企业”是指企业经营范围属于国家重点发展的产业领域，同时能承接国家重大、重点产业发展项目，且具备自主知识产权能力，能积极开展知识产权保护和运用，建立全面的知识产权管理制度和机制，具有知识产权综合实力的企业。

48	
49	
50	中汽研软件测评（天津）有限公司
51	

本次成功获批“国家知识产权优势企业”，体现了政府主管部门和行业、市场对软件测评中心企业经营、专业发展道路、知识产权管理水平及市场竞争力等综合实力的认可，也有利于软件测评中心突出知识产权综合竞争优势，具有行业影响力和标杆性示范作用。

软件测评中心依托中国汽车技术研究中心有限公司知识产权的资源优势，不断优化完善知识产权工作体系，建立了知识产权创造、管理、保护、运用等全周期服务能力。未来，软件测评中心将继续提升知识产权综合管理水平，高质量推进知识产权的保护与运用，不断提升创新力和企业核心竞争力，为提升公司整体科技实力奠定坚实基础，为促进汽车行业健康发展做出更大贡献。

供稿人：盛苗苗　18622038200

GBASE南大通用荣获2023中国金融科技“扬帆计划”十佳卓越实践奖

天津南大通用数据技术股份有限公司

日前，在 2023 金融街论坛年会同期举办的“第五届成方金融科技论坛—金融科技守正创新论坛”上，北京金融科技产业联盟正式发布“扬帆计划——分布式数据库金融应用研究与实践优秀成果”。GBASE 南大通用案例项目荣获“十佳卓越实践”奖。

当前，随着金融业数字化转型的不断深入，对数据库的功能、性能、扩展性和安全性都提出了更高要求。分布式数据库在金融业的应用正在加速扩大，成为金融业数字化转型的必然选择。金融业数据库转型模式已由“政策驱动”逐步转向“自觉行动”。全行业实现了从上至下理念的转变和认识的提升，确保关键软硬件技术供应链安全稳定已成为共识。经过近几年的积累，我国数据库技术产品供给能力明显提升，应用生态不断完善，大量试点应用为金融行业核心系统数据库转型提供了宝贵的可借鉴经验。

GBASE 南大通用本次申报案例为“某国有商业银行总行大数据平台创新升级项目”，基于 GBase 8a MPP Cluster + Hadoop 技术栈建立创新混搭式基础软件架构，根据目标数据特点分层处理，充分发挥各自技术优势，高效应对海量数据的管理和流转。截至目前，数据平台已平稳运行近十年，部署 MPP 数据库集群近百套，节点总规模超四千台，为总量达数十 PB 的海量数据提供管理和服务。平台建设过程中，系统部署架构、高可用方案、数据安全方案等不断创新发展，是金融机构应用 MPP 数据库进行海量数据处理的优秀实践案例，为同业推进大数据体系建设提供了有效借鉴。由此，项目获得大赛评委会的一致肯定，最终收获分布式数据库金融应用“十佳卓越秀实践”殊荣！

GBASE 南大通用公司是目前国内极少数专注于数据库产品研发，并且在金融、电信等行业实现规模化应用的独立数据库服务商，2010 年即自主研究发布了国产第一款成熟的分析型 MPP 数据库 GBase 8a。目前公司自主研发的 GBase 全栈数据库产品，已部署节点超过 35000 个，管理数据总量超过 400PB；在金融行业已经为中国人民银行、国家金融监督管理总局、大型国有银行、股份制银行、头部保险公司及券商等 150 余家用户提供稳定、高效、可靠的数据库产品及服务。

GBASE 南大通用将在已取得的成熟典型应用案例基础上，坚持创新进取、完善提升产品，更好满足用户的应用需求，携手广大用户共同推进金融业的数字化转型，充分发挥基础设施在数字可信体系中的基础作用，为金融科技守正创新提供有效支撑和保障。

供稿人：苏泓宇 18920666547

中国电信集团有限公司天津分公司入选2023年网络安全国家标准优秀实践案例获奖建议名单

为持续强化网络安全国家标准实施应用，提升标准实施成效，进一步发挥以评选优、以优促学的先进带头示范作用，全国信息安全标准化技术委员会于2023年7月4日组织开展“2023年网络安全国家标准优秀实践案例评选活动”。本次评选活动针对2016年《网络安全法》出台以来，信安标委归口管理并发布的234项网络安全国家标准，公开遴选一批在各行业领域内实施应用效果好的标准实践案例，并对优秀实践案例进行宣传表彰。

经案例征集、形式审查、技术初审、综合评审、现场调研等环节，天津商密协会理事单位——中国电信集团有限公司天津分公司入选2023年网络安全国家标准优秀实践案例获奖建议名单。

三等奖建议名单（24名）		
序号	案例名称	申报单位
1	GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》在政务云场景下的应用	深圳市东进技术股份有限公司
2	GB/T 35275-2017 《信息安全技术 SM2密码算法加密签名消息语法规范》等标准在金融领域交易转账保护场景下的应用	中金金融认证中心有限公司
3	GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等标准在云计算场景下的应用	中国电信股份有限公司天津分公司

天津商密协会两家会员单位上榜2023年工业和信息化领域数据安全典型案例名单

为贯彻落实《中华人民共和国数据安全法》及《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》，充分发挥典型案例在数据安全产业发展中的示范引领作用，切实增强工业和信息化领域数据安全保障水平，工业和信息化部办公厅于2023年9月组织开展2023年工业和信息化领域数据安全典型案例遴选工作。

根据《工业和信息化部办公厅关于组织开展2023年工业和信息化领域数据安全典型案例遴选工作的通知》（工信厅网安函〔2023〕266号）部署安排，经申报推荐、形式审查、专业初审和专家评审，2023年工业和信息化领域数据安全典型案例名单于2023年12月24日在工业和信息化部网络安全管理局官方网站公示。

天津市商用密码行业协会理事单位中国电信集团有限公司天津分公司、会员单位中汽数据（天津）有限公司上榜。

一、工业领域典型案例（共34项）

33	其他方向	汽车数据安全保护类	长安车联网数据安全防护方案	重庆长安汽车股份有限公司	/	重庆市经信委
34		汽车数据安全保护类	车外人脸信息匿名化保护设计方案及量产化应用	卡汽数据（天津）有限公司	卡国第一汽车股份有限公司	天津市工信局

二、电信和互联网领域典型案例（共38项）

29	数据安全体系整体设计实施方向	整体设计实施类	基于“轨感数据不出网、网内受控便捷用”模式的数据安全保障体系	中国移动通信集团浙江有限公司		浙江省通信管理局
序号	申报方向	申报类型	案例名称	申报主体	联合申报单位	推荐单位
30			智慧、泛在、协同的数据安全联防联控体系建设与实践	中移动信息技术有限公司	中国移动通信集团安徽有限公司、中国移动通信集团辽宁有限公司	中国移动通信集团
31			数据安全一体化赋能物联网端到端产业链案例	中国移动通信集团广东有限公司	中移互联网有限公司	广东省通信管理局
32			基于“四平台三网关”的数据安全治理框架和应用典型案例	中国电信股份有限公司江苏分公司	中国电信股份有限公司重庆分公司、中国电信股份有限公司技术创新中心	江苏省通信管理局
33			数据上“云”、行业集“用”、管、控“一体的云端用数主点体系	中国移动通信集团四川有限公司		四川省通信管理局
34			数据安全访问沙箱构建数据治理新模式实践	中国联合网络通信有限公司软件研究院	联通华盛通信有限公司	中国联合网络通信集团
35			通信行业数智一体化数据安全管控平台典型案例	中国移动通信集团江苏有限公司	中国移动新业（江苏）创新研究院有限公司、北京东方通网信科技有限公司	江苏省通信管理局
序号	申报方向	申报类型	案例名称	申报主体	联合申报单位	推荐单位
36			全维度多视角数据安全动态防御管控体系构建	中国电信股份有限公司天津分公司	天翼安全科技有限公司、北京化信股份有限公司	天津市通信管理局

天津商密产品明细表

排序	产品名称	产品型号	产品版本号	安全等级	证书编号	委托人名称	联系人	联系方式
1	CC903TP_CSH PCIe密码卡	CC903TP_CSH	V1.1	安全二级	GM001210420230973	天津国芯科技有限公司	张培培	15011411157
2	Mini PCI-E密码卡	CCUPM2S01	V1.0、V2.0	安全二级	GM001210420230978	天津国芯科技有限公司	张培培	15011411157
3	安全芯片	CCM3310S-LP	V1.0、V1.1、V1.2	安全二级	GM001212020230884	天津国芯科技有限公司	张培培	15011411157
4	安全芯片	CCM4201S	V2.0、V2.1	安全二级	GM001212020230766	天津国芯科技有限公司	张培培	15011411157
5	运维审计堡垒机（密码模块）	AC-GMBH-01	V1.0	安全二级	GM001212220230756	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
6	Mini PCI-E密码卡	CCUPM2001	V1.1	安全二级	GM001210420230706	天津国芯科技有限公司	张培培	15011411157
7	可信密码模块	CCUPMKX01	V1.0	安全二级	GM001212320230687	天津国芯科技有限公司	张培培	15011411157
8	安全输入组件密码模块	SafeInput	V1.0	安全一级	GM001212220230653	天津赢达信科技有限公司	彭竹	18601092821
9	PCI-E密码卡	CCUPH2002	V1.1	安全二级	GM001210420230651	天津国芯科技有限公司	张培培	15011411157
10	安全芯片	CCM3310S-T	V1.0、V1.1、V1.2	安全二级	GM001212020230564	天津国芯科技有限公司	张培培	15011411157
11	工控安全网关	AC-ICSG-01	V1.0	安全二级	GM001210520230513	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
12	光电安辰智能IC卡	AC-GMIC-01	V1.0	安全二级	GM001210220230476	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
13	安全芯片	CCM3305S	V1.0、V1.1	安全二级	GM001212020230477	天津国芯科技有限公司	张培培	15011411157
14	可变口令认证系统密码模块	YDX-DPAuth	V1.0	安全二级	GM001212220230445	天津赢达信科技有限公司	彭竹	18601092821
15	英信IPSec VPN安全网关	YX-A1000	V1.0	安全二级	GM001210520230412	天津英信科技有限公司	田全鹏	18322081988
16	IPSec/SSL VPN综合安全网关	AC-IPSEC/SSL VPN-01	V1.0	安全二级	GM001210620230348	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
17	光电安辰读卡模块（密码模块）	AC-GMACR-01	V1.0	安全二级	GM001212220230342	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
18	密码卡	CCUPN2001	V1.0	安全二级	GM001210420230274	天津国芯科技有限公司	张培培	15011411157
19	Mini PCI-E密码卡	CCUPM2005	V1.0	安全二级	GM001210420230264	天津国芯科技有限公司	张培培	15011411157
20	密码卡	CCUPN2002	V1.0	安全二级	GM001210420230248	天津国芯科技有限公司	张培培	15011411157
21	PCI-E密码卡	CCUPH2Q01	V1.0	安全二级	GM001210420230257	天津国芯科技有限公司	张培培	15011411157
22	安全芯片	CUni360S	V1.0	安全二级	GM001212020230220	天津国芯科技有限公司	张培培	15011411157
23	数字证书认证系统	ADC-CA	V1.0	不涉及	GM001111820230160	中汽数据（天津）有限公司	吴璟希	13042252655
24	灵创智恒安全认证网关	CIST-SAG	V2.0	安全二级	GM001210720230148	天津灵创智恒软件技术有限公司	王城	13752238978
25	IPSec VPN安全通信网关	BSAFE-6000	V7.6.10	安全二级	GM001210520230121	宝牧科技（天津）有限公司	李杰	13920288899
26	数字物理噪声源芯片	CWNG10	V1.0	安全一级	GM001212020230110	天津国芯科技有限公司	张培培	15011411157
27	国密SSL组件密码模块	GMSSL	V1.0	安全二级	GM001212220230112	天津赢达信科技有限公司	彭竹	18601092821
28	IPSec VPN安全通信网关	BSAFE-600	V7.6.10	安全二级	GM001210520230001	宝牧科技（天津）有限公司	李杰	13920288899
29	IPSec VPN安全通信网关	BSAFE-1000	V7.6.10	安全二级	GM001210520230002	宝牧科技（天津）有限公司	李杰	13920288899
30	IPSec VPN安全通信终端	BSAFE-300	V3.1.8	安全二级	GM001210520230003	宝牧科技（天津）有限公司	李杰	13920288899
31	手机盾认证系统服务端(密码模块)	AC-GMMD-S01	V1.0	安全二级	GM001212220220786	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
32	手机盾认证系统客户端(密码模块)	AC-GMMD-C01	V1.0	安全二级	GM001212220220787	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
33	手机盾（ios）密码模块	WinMobile(IOS)	V1.0	安全二级	GM001212220202319	天津赢达信科技有限公司	彭竹	18601092821
34	SD密码卡	SJK1959			GM001219920201499	天津赢达信科技有限公司	彭竹	18601092821
35	手机盾（Android）密码模块	WinMobile(Android)	V1.0	安全二级	GM001212220202387	天津赢达信科技有限公司	彭竹	18601092821
36	智能密码钥匙	SJK1985			GM001219920201628	天津赢达信科技有限公司	彭竹	18601092821
37	赢达信安全浏览器（密码模块）	SuloongBrowser	V4.0	安全二级	GM001212220220008	天津赢达信科技有限公司	彭竹	18601092821
38	数据库加密管理系统密码模块	WinDBS	V1.0	安全二级	GM001212220210363	天津赢达信科技有限公司	彭竹	18601092821
39	手机盾认证系统（密码模块）	WinMobileAuth	V1.0	安全二级	GM001212220202272	天津赢达信科技有限公司	彭竹	18601092821
40	智能密码钥匙	WinKey	V2.0	安全二级	GM001210120220387	天津赢达信科技有限公司	彭竹	18601092821
41	安全芯片	CCM4201S	V1.0、V 1.1	安全一级	GM001212020220658	天津国芯科技有限公司	张培培	15011411157
42	PCI-E密码卡	WinPCIE	V1.0	安全二级	GM001210420220635	天津赢达信科技有限公司	彭竹	18601092821
43	光电安辰安全音视频监控系统服务端（密码模块）	SJT1708	V1.0	安全二级	GM001212220220592	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
44	光电安辰安全音视频监控系统客户端（密码模块）	SJT1709	V1.0	安全二级	GM001212220220593	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
45	IPSec VPN安全网关	AC-GMVPN-01	V1.0	安全二级	GM001210520220461	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
46	服务器密码机	TOEC-GMCM01	V1.0	安全二级	GM001211020220451	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
47	PCI-E密码卡	CCUPH2002	V1.0	安全二级	GM001210420220428	天津国芯科技有限公司	张培培	15011411157
48	安全芯片	CCP907T	V1.0、V1.1、V1.2、V1.3	安全一级	GM001212020220429	天津国芯科技有限公司	张培培	15011411157
49	Mini PCI-E密码卡	CCUPM2003	V1.0	安全二级	GM001210420220430	天津国芯科技有限公司	张培培	15011411157
50	Mini PCI-E密码卡	CCUPM2001	V1.0	安全二级	GM001210420220281	天津国芯科技有限公司	张培培	15011411157
51	PCI-E密码卡	TOEC-GMPCIE01	V1.0	安全二级	GM001210420220256	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
52	PCI-E密码卡	CCUPH2001	V1.0	安全二级	GM001210420220230	天津国芯科技有限公司	张培培	15011411157
53	Mini PCI-E密码卡	CCUPM2002	V1.0	安全二级	GM001210420220231	天津国芯科技有限公司	张培培	15011411157
54	PCI-E密码卡	CCUPH3001	V1.0	安全三级	GM001210420220213	天津国芯科技有限公司	张培培	15011411157
55	灵创智恒签名验签服务器	CIST-SVS	V1.0	安全二级	GM001211120220143	天津灵创智恒软件技术有限公司	王城	13752238978

天津商密产品明细表

排序	产品名称	产品型号	产品版本号	安全等级	证书编号	委托人名称	联系人	联系方式
56	光电安辰国密高安全门禁系统	STC-1	V1.0	不涉及	GM001211320220077	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
57	安全芯片	CCM4208S	V1.0	安全二级	GM001212020220042	天津国芯科技有限公司	张培培	15011411157
58	安全芯片	CCM3320S	V1.0	安全二级	GM001212020210565	天津国芯科技有限公司	张培培	15011411157
59	安全芯片	CCM3310S-L	V1.0	安全二级	GM001212020210562	天津国芯科技有限公司	张培培	15011411157
60	安云印电子印章统一管理服务平台	AYY2007	V1.0	不涉及	GM001211520210533	安云印（天津）大数据科技有限公司	张铭鑫	13312123509
61	SATA接口密码卡（密码模块）	TOEC-GMMIC01	V1.0	安全二级	GM001212220210524	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
62	灵创智恒密钥管理系统V1.0	SYT1604密钥管理系统	V1.0	不涉及	GM001211820210464	天津灵创智恒软件技术有限公司	王城	13752238978
63	灵创智恒数字证书认证系统V1.0	SZT1601数字证书认证系统	V1.0	不涉及	GM001211820210455	天津灵创智恒软件技术有限公司	王城	13752238978
64	可信TCM密码模块	CCT02	V1.0	安全一级	GM001212220210250	天津国芯科技有限公司	张培培	15011411157
65	可信TCM密码模块	CCT01	V1.0	安全一级	GM001212220210251	天津国芯科技有限公司	张培培	15011411157
66	U盘智能密码钥匙	CCK06	V1.0	安全二级	GM001210120210175	天津国芯科技有限公司	张培培	15011411157
67	NM型智能密码钥匙	CCK07	V1.0	安全二级	GM001210120210176	天津国芯科技有限公司	张培培	15011411157
68	智能密码钥匙	CCK05	V1.0	安全二级	GM001210120210177	天津国芯科技有限公司	张培培	15011411157
69	CCP903T安全芯片	CCP903T	V1.0	安全二级	GM001212020210135	天津国芯科技有限公司	张培培	15011411157
70	软盾密钥协同系统（Android客户端密码模块）	SSS-A	1.0.0	安全二级	GM001212220210113	天津市滨海数字认证有限公司	刘杰	13752562684
71	软盾密钥协同系统（IOS客户端密码模块）	SSS-I	1.0.0	安全二级	GM001212220210114	天津市滨海数字认证有限公司	刘杰	13752562684
72	软盾密钥协同系统（密码模块）	TJBHCA-1.1	V1.0	安全二级	GM001212220210038	天津市滨海数字认证有限公司	刘杰	13752562684
73	软盾协同管理密码模块	TJBHCA-1.0	V1.0	安全二级	GM001212220210039	天津市滨海数字认证有限公司	刘杰	13752562684
74	南大通用安全目录服务系统（密码模块）	GBase 8d	V6.0	安全一级	GM001212220202378	天津南大通用数据技术股份有限公司	马海燕	13502171319
75	安全即时消息加密系统（密码模块）	TSIM-ES	V1.0.0	安全一级	GM001212220202353	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
76	FT - 2000/4 通用安全处理器	FT-2000/4	V1.0	安全一级	GM001212020202323	飞腾信息技术有限公司	冯彦朝	13102232653
77	天津光电安全门禁读卡器（密码模块）	STC-1	V1.0	安全一级	GM001212220202202	天津光电通信技术有限公司	焦庆玲	13672004323
78	CC903TP_CSH PCIe密码卡	CC903TP_CSH	V1.0	安全二级	GM001210420202053	天津国芯科技有限公司	张培培	15011411157
79	指纹型智能密码钥匙	SJK19118			GM001219920201772	天津国芯科技有限公司	张培培	15011411157
80	蓝牙型智能密码钥匙	SJK1956			GM001219920201465	天津国芯科技有限公司	张培培	15011411157
81	安全芯片	SSX1922			GM001219920201488	天津国芯科技有限公司	张培培	15011411157
82	签名验签服务器	SRJ1925			GM001219920201529	天津灵创智恒软件技术有限公司	王城	13752238978
83	IPSec VPN安全网关	SJJ1921			GM001219920201284	宝牧科技（天津）有限公司	李杰	13920288899
84	IPSec VPN安全网关	SJJ1922			GM001219920201285	宝牧科技（天津）有限公司	李杰	13920288899
85	安全芯片	SSX1926			GM001219920201645	天津国芯科技有限公司	张培培	15011411157
86	安全芯片	SSX1314			GM001219920201336	天津国芯科技有限公司	张培培	15011411157
87	安全芯片	SSX1208			GM001219920201337	天津国芯科技有限公司	张培培	15011411157
88	安全芯片	SSX1826			GM001219920201107	天津国芯科技有限公司	张培培	15011411157
89	安全芯片	SSX1928			GM001219920201713	天津国芯科技有限公司	张培培	15011411157
90	安全目录服务系统	SJT1002			GM001219920201392	天津南大通用数据技术股份有限公司	马海燕	13502171319
91	安全芯片	SSX1914			GM001219920201395	天津国芯科技有限公司	张培培	15011411157
92	SD密码卡	SJK19112			GM001219920201736	天津国芯科技有限公司	张培培	15011411157
93	加密数据库系统	SHT0905			GM001219920201404	天津南大通用数据技术股份有限公司	马海燕	13502171319
94	ATM密码应用系统	SHT1917			GM001219920201416	恒银金融科技股份有限公司	王斌	18622297399
95	密码键盘	SJM1925			GM001219920201500	恒银金融科技股份有限公司	王斌	18622297399
96	无线POS终端	X990 PINPad	V1.0	安全二级	GM001210320230381	惠尔丰信息系统有限公司	童奥	13810111254
97	无线POS终端	X970	V1.0	安全二级	GM001210320220471	惠尔丰信息系统有限公司	童奥	13810111254
98	无线POS终端	T650m	V1.0	安全二级	GM001210320220075	惠尔丰信息系统有限公司	童奥	13810111254
99	密码键盘	PP1000SE v3	V1.0	安全二级	GM001210820210520	惠尔丰信息系统有限公司	童奥	13810111254
100	无线POS终端	X990	V1.0	安全二级	GM001210320210470	惠尔丰信息系统有限公司	童奥	13810111254
101	POS密码应用系统	SHT1911			GM001219920201303	惠尔丰信息系统有限公司	童奥	13810111254
102	POS密码应用系统	SHT1903			GM001219920201151	惠尔丰信息系统有限公司	童奥	13810111254
103	腾云S5000C通用安全处理器	S5000C	B3432	安全一级	GM001212020230873	飞腾信息技术有限公司	冯彦朝	13102232653
104	腾珑E2000可信密码模块(TCM)	E2000	V1.0	安全二级	GM001212320230874	飞腾信息技术有限公司	冯彦朝	13102232653
105	腾云S5000C通用安全处理器	S5000C	B5796	安全一级	GM001212020230771	飞腾信息技术有限公司	冯彦朝	13102232653
106	腾珑E2000通用安全处理器	E2000	B809	安全一级	GM001212020230371	飞腾信息技术有限公司	冯彦朝	13102232653
107	腾锐D2000 TCM可信密码模块	D2000（GM/T0012-2020）	v1.1.0	安全二级	GM001212320230070	飞腾信息技术有限公司	冯彦朝	13102232653
108	腾珑E2000通用安全处理器	E2000	B705	安全一级	GM001212020220798	飞腾信息技术有限公司	冯彦朝	13102232653
109	飞腾S2500密码模块	SMK001	V1.0	安全二级	GM001212220220799	飞腾信息技术有限公司	冯彦朝	13102232653
110	腾锐D2000通用安全处理器	腾锐D2000	V1.0	安全一级	GM001212020220243	飞腾信息技术有限公司	冯彦朝	13102232653

天津商密应用方案和建设试点单位名录

	公司名称	联系人	联系电话
1	天津光电通信技术有限公司	焦庆玲	13672004323
2	天津数字认证有限公司	崔悦	13012226118
3	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
4	天津灵创智恒软件技术有限公司	王城	13752238978
5	天津赢达信科技有限公司	彭竹	18601092821
6	安云印（天津）大数据科技有限公司	张铭鑫	13312123509
7	北京数字认证股份有限公司	高博	13820886769
8	天津中网基业智能系统工程有限公司	于晨	18920387877
9	天津国芯科技有限公司	张培培	15011411157
10	天津赢达信科技有限公司	彭竹	18601092821
11	宝牧科技（天津）有限公司	张金金	13132219391
12	中汽数据（天津）有限公司	张旺	15922090958

表中所列企业均已在天津市商用密码行业协会进行备案，且有至少5名正式员工参加协会组织的商用密码方案建设培训并考试合格。

天津电子认证服务机构

	机构名称	联系人	联系电话
1	天津数字认证有限公司	崔悦	13012226118
2	北京数字认证股份有限公司	高博	13820886769
3	中汽数据（天津）有限公司	张旺	15922090958
4	天津市滨海数字认证有限公司	刘杰	13752562684

天津商用密码应用安全性评估机构

	机构名称	联系人	联系电话
1	天津云安科技发展有限公司	赵慧	15102221821
2	中互金认证有限公司	李文宝	15201294794
3	道普信息技术有限公司天津分公司	刘越喆	18902146600
4	北京卓识网安技术股份有限公司	段遵义	13583122211
5	安徽科测信息技术有限公司	马国富	18856085098
6	中科信息安全共性技术国家工程研究中心有限公司	王喆	13820159211

表中所列企业均已在天津市商用密码行业协会进行备案，具有相应场地、人员及能力，随时接受天津市商用密码行业协会监督检查，按实际情况进行动态调整。

会员单位

会长单位
天津光电通信技术有限公司

监事长单位
南开大学

常务副会长单位
天津灵创智恒软件技术有限公司

副会长单位
麒麟软件有限公司
飞腾信息技术有限公司
天津国芯科技有限公司
天津数字认证有限公司
天津赢达信科技有限公司
恒银金融科技股份有限公司
天津长城计算机系统有限公司
中汽研软件测评(天津)有限公司

秘书长单位
天津光电安辰信息技术股份有限公司

监事单位
天津英信科技有限公司
天津光电聚能专用通信设备有限公司

理事单位
中互金认证有限公司
兴唐通信科技有限公司
道普信息技术有限公司
天津航天信息有限公司
天津恒御科技有限公司
惠尔丰信息系统有限公司
宝牧科技(天津)有限公司
北京数字认证股份有限公司
曙光信息产业股份有限公司
天津云安科技发展有限公司
天津百望金赋科技有限公司
天津市滨海数字认证有限公司
天津联信达软件技术有限公司
天津七所精密机电技术有限公司
天津市天河计算机技术有限公司
天津正元星捷信息科技有限公司
安云印(天津)大数据科技有限公司
中国电信集团有限公司天津分公司
天津中网基业智能系统工程有限公司
天津南大通用数据技术股份有限公司
联通数字科技有限公司天津市分公司
江西智慧云测安全检测中心股份有限公司

会员单位
天津戎行技术有限公司
浪潮软件集团有限公司
天翼安全科技有限公司
润成安全技术有限公司
天津优扬科技有限公司
中科安永科技有限公司
天地融科技股份有限公司
天津市海益电子有限公司
深信服科技股份有限公司
中汽数据(天津)有限公司
天津国科量子科技有限公司
渔翁信息技术股份有限公司
恒利德(天津)科技有限公司
天津鲲鹏信息科技有限公司
天津鲲奥世达科技有限公司
天津市兴先道科技有限公司
天津安恒数据安全有限公司
北京国泰网信科技有限公司
北京江南天安科技有限公司
三未信安科技股份有限公司
安徽科测信息技术有限公司
天津顺时信息技术有限公司
天津盛创科技发展有限公司
天津中邦信息技术有限公司
天津市康恒信息科技有限公司
流光(天津)量子科技有限公司
中保网盾(天津)科技有限公司
天津安华易科技发展有限公司
天津华安保信息技术有限公司
天津安力信通讯科技有限公司
天津娜绮林科技发展有限公司
北京海泰方圆科技股份有限公司
天津华汇工程建筑设计有限公司
北京卓识网安技术股份有限公司
北京安盟信息技术股份有限公司
宏信旺(天津)科技发展有限公司
佰运俐(天津)科技发展有限公司
天津睿信康达科技发展有限公司
北京信安世纪科技股份有限公司
中科问天量子科技(天津)有限公司
北京航天七零六信息科技有限公司
成都卫士通信息产业股份有限公司
中安云科科技发展(山东)有限公司
天津市国瑞数码安全系统股份有限公司
天津大学建筑设计规划研究总院有限公司
北京海量数据技术股份有限公司天津分公司
中科信息安全共性技术国家工程研究中心有限公司
……

天津云安科技发展有限公司
Tianjin Cloud Security Technology development Co.Ltd

商用密码应用安全性评估试点机构

云启未来 因密而安

公司介绍

天津云安科技发展有限公司，成立于2013年1月，是国家高新技术企业、天津市专精特新企业，天津市商用密码协会创始单位与理事单位、中国密码学会密评联委会成员单位，密码行业标准化技术委员会成员单位，致力于网络安全服务与商用密码应用安全性评估与系统咨询等有关工作。

2021年6月，公司正式被纳入**《商用密码应用安全性评估试点机构目录》**（国家密码管理局第42号公告），可以面向全国、全社会开展商用密码应用安全性评估工作，为用户提供密码应用方案评估、信息系统密码应用安全性评估以及密码应用规划、密码安全管理等咨询服务工作。

云安科技配备了能够模拟多种密码应用与测评场景的实验室，拥有高水平的密码测评能力。

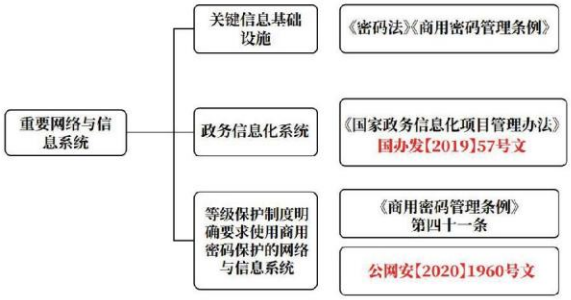
公司自开展密评工作以来，精心实施好每一个项目，已经为 300 多个重要网络信息系统提供密码测评服务，测评系统涵盖党政机关、公检法司、卫生健康、金融期货、能源电力、广播电视、教育、交通、水务等多个领域，服务的客户涉及天津市、重庆市、甘肃省、江苏省、浙江省、辽宁省、山西省、河北省、贵州省、云南省、山东省等区域。

公司地址：天津市津南区启迪协信科技园18-2
咨询热线：13164063271（技术）13116114659（业务）

三同步一评估

密评的对象——重要网络与信息系统：法律、法规和国家有关规定要求使用商用密码进行保护的网络与信息系统。

三同步一评估：重要网络与信息系统同步规划、同步建设、同步运行密码保障系统，并定期开展商用密码应用安全性评估。



部分案例

- 天津市商用密码密钥管理中心系统密码测评服务
- 天津市政府电子政务系统密码测评服务
- 天津市国资委信息系统密码测评服务
- 天津市卫生健康委信息系统密码测评服务
- 天津市公安局执法办案监督与问题追溯平台密码测评服务
- 天津市人民检察院第一分院检察工作网密码测评服务
- 宁夏电视台信息系统密码测评服务
- 中国电信天翼云密码测评服务
- 国网天津市电力公司电力监控系统
- 贵州云上遵义密码测评服务
- 曙光政务云密码测评服务

联系电话：022-27607853
企业邮箱：support@tjcstc.com
官方网址：www.tjcstc.com

中互金认证有限公司

中互金认证有限公司隶属于中国互联网金融协会，是协会检测认证工作的实际载体，致力于为各行业客户提供检测认证一体化服务，作为第三方专业机构在支撑服务监管的同时，也在标准认证、安全、合规测评等领域提供相关服务。

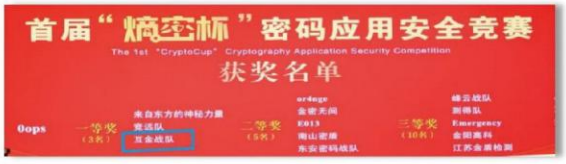
公司拥有商用密码应用安全性评估、金融科技产品检测、信息安全风险评估、服务认证和产品认证等多项资质，可提供商用密码合规测评、数据安全评估、电子银行安全评估、金融科技产品（移动金融客户端 APP、区块链、多方安全计算、商业银行应用程序接口）检测、金融企业标准建设咨询等多项服务。公司服务范围包括金融、政务、公检法、通信、能源等多个行业领域，与 100+家客户建立了合作关系。

公司网址：http://nifc.org.cn/
联系人：李文宝 15201294794
邮箱 ：lwenbao@nifa.org.cn

公司自成立以来始终保持高速发展，坚持自我精进，获得了 CNAS、CMA、信息安全管理体系认证、质量管理体系认证、职业健康安全管理体系认证、环境管理体系认证等多项专业资质，拥有发明专利、软件著作权 30+项，多次荣获中国人民银行及其他监管机构、协会颁发的重要奖项。与此同时，公司积极参与构建以商用密码为支撑的新网络安全体系，作为人民银行科技司推荐、国家密码管理局正式授权的商用密码应用安全性评估试点机构，中互金认证有限公司积极参与并牵头多项国家标准、行业标准及重要团体标准的制定工作，并成为国家密码标准委员会（密标委）测评工作组和应用工作组成员单位。

公司由一支具备丰富行业经验的团队组成，其中技术人员占比 70%，均具备多年信息安全领域的从业经验。核心团队成员曾参与发改委重大专项、核高基专项等重大科研成果研发工作，且多人获得了行业科技特等奖、一等奖等奖项。公司技术团队熟悉密码算法、行业标准，具有丰富的密码测评、信息安全评估经验。

承接数字经济的浪潮，公司未来将恪守客观公正的原则，秉承“科学公正、规范高效、持续创新、客户满意”的服务宗旨，努力成为政府信任、客户信赖、社会需要且与国际接轨的专业测评认证机构，助力金融科技高质量发展，为数字化时代网络安全提供有力支持。



在 2023 年 8 月国内首届“熵密杯”商用密码应用安全竞赛，也是商用密码领域规模最大的一次安全竞赛中，中互金认证有限公司的互金战队在全国 100 多家机构中荣获一等奖。

道普信息

让信息化更规范更安全

山东省计算中心（国家超级计算济南中心）科研成果转化企业
成为第三方信息化风险管控领导者
道普信息技术有限公司

道普信息是一家专注于信息化第三方保障服务的机构，在国内率先提出信息化风险全面第三方保障理念。公司营销总部位于北京，管理总部位于济南，2016年由山东省计算中心所属山东省软件评测中心科研成果转化成立，是国内具备“三保一测一评（等保、分保、关保、软测、密评）”综合能力的领先机构。

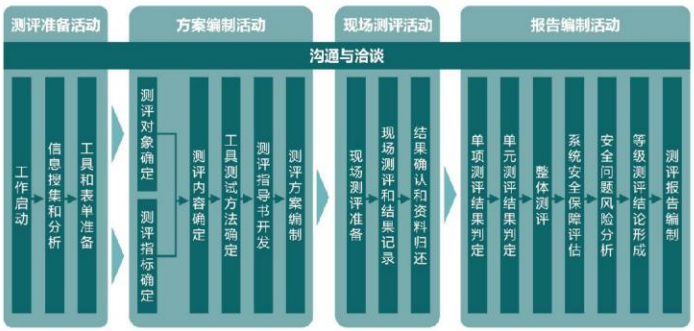
公司坚持“全程以客户为中心”服务理念，面向社会提供商用密码应用安全性评估和网络安全合规管理等服务和综合解决方案，已服务信息工程万余项，覆盖政务、金融、医疗、教育、交通、电力、能源等行业，致力于让客户的信息化更规范更安全，赢得“道普就是靠谱”的良好形象。

荣誉资质

国家密码管理局 商用密码应用安全性评估试点机构
公安部 网络安全等级测评与检测评估机构
中关村华安关键信息基础设施安全保护联盟 会员单位
国家保密局 涉密信息系统集成服务资质（工程监理甲级）
软件工程造价评估机构能力符合性证书
中国电子企业协会 信息系统工程监理服务标准贯标（甲级）
瞪羚企业、专精特新、高新技术、软件企业
承担国家多项科研课题，参与制定多项国家标准
ISO27001\ISO20000\ISO9000\CMMI\ITSS\全过程咨询服务认证
……

商用密码应用安全性评估

依据信息系统密码应用基本要求、商用密玛应用安全性评估测评过程指南、行业密码应用标准和规范、建设指南等，对信息系统密码应用总体要求、密码应用技术、密码应用管理、密钥管理等要求进行测评。出具密码等级测评报告，针对被测系统存在的安全隐患，从系统安全角度提出相应的改进建议。



道普信息技术有限公司

北京总部 13120102970
北京市海淀区翠微路12号
济南总部 0531-86515189
济南市高新区银荷大厦B座4层

天津办事处
18902146600
天津市华苑产业园区
智慧山西塔12层

（扫码关注“道普信息”公众号，回复关键词“密评”，可获得相关服务/解决方案详细介绍）

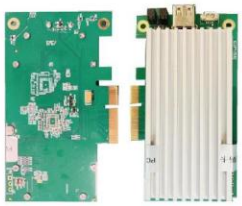
天津商密产品展示

国密运维审计堡垒机

国密运维审计堡垒机是由光电安辰自主研发的高性能商用密码产品，严格遵循密码相关法律法规和标准要求，具备商用密码产品型号认证证书（二级），支持 SM 系列国密算法，可提供运维用户身份认证、国密 SSL 和 IPSec 安全通道建立（包括运维终端和国密堡垒机之间，以及国密堡垒机和核心资产之间）、运维数据机密性和完整性保护等密码应用服务，同时也支持用户管理、访问和权限控制、设备管理、安全运维、报表统计、系统管理等通用运维审计功能，可实现对核心资产的安全运维，可满足等保密评等相关应用要求。

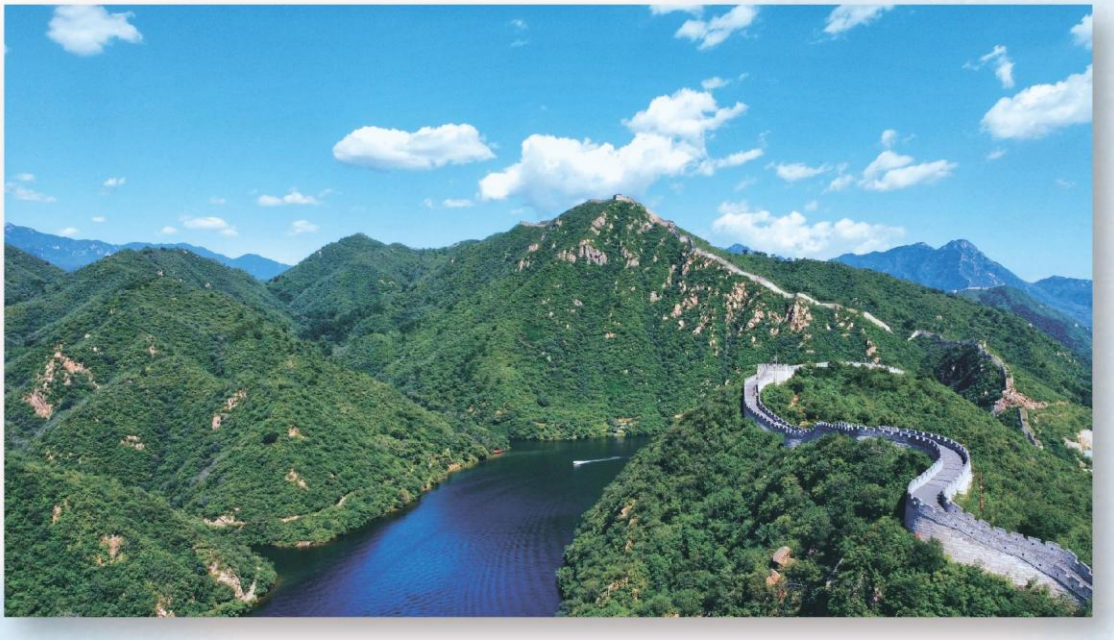
天津光电安辰信息技术股份有限公司
胡双喜 13821024385

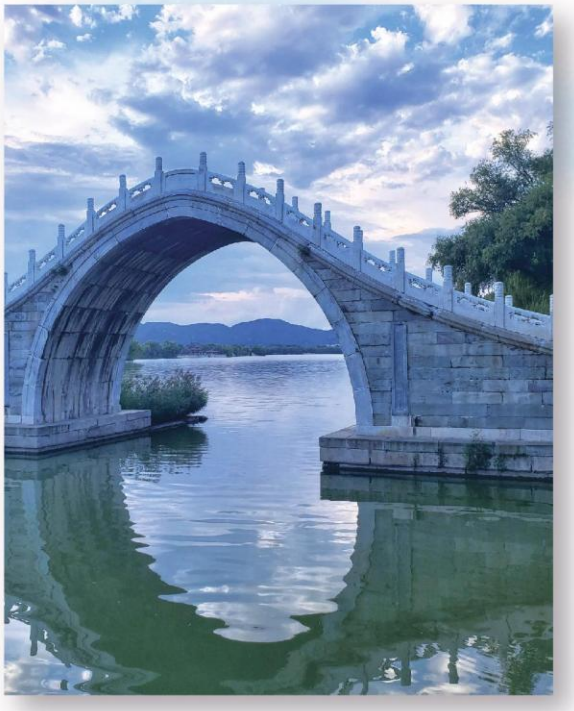
CCUPH2002 PCIE 密码卡



CCUPH2002 PCIE 密码卡产品是基于 C*CORE CCP90X 系列安全芯片设计的一款高速密码卡，遵循国家密码管理局关于 PCI 密码卡的相关技术规范，支持 SM1、SM2、SM3、SM4 等国密算法，能够为可信计算各类安全平台提供多线程、多进程和多卡并行处理的高速密码运算服务，满足其对数字签名 / 验证、非对称 / 对称加解密、数据完整性校验、随机数生成、密钥生成和管理等功能的 要求，保证敏感数据的机密性、真实性、完整性和抗抵赖性，产品支持 Windows、Linux 等主流操作系统。

天津国芯科技有限公司
张培培 15011411157





张文涛

天津光电安辰信息技术股份有限公司

征稿启事

《天津商密》是由天津市商用密码行业协会主办，面向会员单位公开发行的综合性科技期刊。以“引领商密行业发展、促进商密应用推广”为宗旨，集理论性、权威性、时效性、知识性及趣味性于一体。

为进一步丰富杂志内容，现面向社会广泛征集作品，具体事宜说明如下：

一、征稿作品类型：

1、党建园地：会员单位组织党建活动。

2、政策解读：商密相关法律、法规、政策、标准等的解读分析。

3、业界交流：商密相关学术论文、商密知识科普等。

4、密码应用：应用于实际的商密产品、方案等。

5、会员风采：会员单位参加公益类、生活类、企业联动类活动（非党建活动），或员工书画摄影诗词等。

二、征稿作品格式：

1、图文精良，制作规范。

2、文稿为 WORD 格式，会员动态、风采栏目文章字数为 600-800 字，其他栏目文章字数不少于 1000 字。

3、所有图片均为 JPG 格式，分辨率 300DPI。

三、投稿须知：

1、来稿请注明作者真实姓名、职务、单位、联系方式（手机和电子邮件）。

2、来稿署名作者应为合法著作权人，署名无争议。

3、来稿一经采用，将邮件或电话通知作者，赠送当期杂志。

四、投稿方式：

投稿邮箱：tjmmxh2021@163.com 或添加微信：13512981809

《天津商密》长期征稿，欢迎大家踊跃投稿！