**电子取证与保密技术攻防体系关键技术研究**

**一、融合山大优势的保密攻防对抗体系建设**

山东大学作为国内网络安全研究的核心力量，依托丰富的技术积累和实践经验，在保密攻防对抗体系建设中取得了显著成果。2004年至2006年，王小云院士团队攻克了国际通用的SHA-1与MD5哈希算法，在国际密码学界引起广泛关注。此后，王小云院士主持设计的SM3哈希算法成为我国首个商用哈希算法标准，并成功入选ISO/IEC国际标准。

在教学与人才培养方面，我校注重网络安全的系统化教育布局，开设了《网络工程与防御实践》等多个攻防对抗类课程，帮助学生在分析、实践、知识运用和独立解决问题等方面全面提升。此外，山东大学积极承担中央网信办委托的网络空间安全教材体系规划、网络空间安全课程体系建设以及网络空间安全教材编写指南三大课题，旨在完善我国网络空间安全人才培养的体系化建设。在此基础上，我校编写了《网络工程与防御实践》等有关网络安全、对抗攻防领域的教材，且《网络工程与防御实践》已通过CNAS认证。

在科研与教学平台建设方面，我校与鹏城靶场合作建设了分布式靶场项目，充分利用其动态模拟网络环境的技术优势，通过快速重构和虚拟化技术，为演练提供与真实环境高度一致的模拟条件。靶场系统架构完善、功能齐全。靶场建设基于一个建设标准、两大科学问题、三类主要应用、四种攻防模式、五方核心角色、六步业务流程及七层体系架构的理念，涵盖WEB渗透、逆向分析、加解密、隐写术、移动安全、工控安全、智能家居安全等网络空间安全领域的典型竞赛真题和模拟练习题；此外，还提供丰富的课程资源，包括各类教学文档、教学视频和模拟实验，以支持系统化教学。通过此平台，我校师生能够获得深度的实战模拟体验，有效提升攻防对抗的科研水平和技术能力，为网络空间安全研究与人才培养提供了高质量的支撑。

**二、融合山大优势的保密违法违规数据取证技术体系建设**

在建设保密违法违规数据取证技术体系的过程中，山东大学网络空间安全学院的Sigma实验室作为荣获青岛市委机要保密局颁发的“密码与保密技术实验室”称号的团队，发挥重要作用，实验室在先进数据加密与解密技术上拥有核心优势，可实现复杂数据环境下的高效解析和取证。基于加密检测和破解工具，Sigma实验室能够快速识别可疑数据流，并对其进行解密分析，提升取证过程的时效性。同时，实验室的密钥管理技术确保在数据提取与分析过程中的密钥安全，构建了安全可靠的密钥存储与管理机制，保护数据完整性。此外，Sigma实验室还在多层次数据流加密保护上做出技术突破，涵盖数据取证过程中的各个环节，为保密数据提供全方位的安全保障。通过加密传输和存储方案，数据在取证过程中的安全性得以提升。

此外，Sigma实验室还配备了FL-2000取证航母一体化智能取证工作站，这款设备集成了计算机技术、数据存储技术和人工智能等多项先进技术，是一款适用于多种数据类型和取证需求的高效智能化工作站。FL-2000采用模块化设计，灵活支持多种取证任务，能够单台设备满足日常数据取证的多种需求，显著提升了数据取证的效率和准确性。FL-2000工作站的设计将并行加速、触控操作与人工智能技术高度融合，极大提高了操作的简便性和取证速度。其智能化操作模式，使得即便是没有专业技术背景的人员也能快速上手。借助一键式操作，用户可以在接入存储介质后，迅速完成介质预检、数据固定、取证分析、报告生成等全过程，确保取证工作的高效与严谨。这款设备支持多种取证功能，包括多路硬盘复制、仿真系统、计算机取证、手机取证以及数据融合分析等。多路硬盘复制功能能够同时处理多个硬盘数据，减少取证时间；仿真系统功能可模拟目标计算机系统环境，进行有效的取证分析；手机取证功能支持从不同类型的移动设备中提取数据，包括SIM卡、内存和存储等；融合分析则结合多种数据源和信息，进行深度挖掘和整合分析，提供更为全面的证据支持

目前国内经过CNAS认证，支持电子取证的高校主要集中在政法类院校和公安类院校，能够支持电子取证的综合类大学几乎没有，而山东大学网络空间安全学院Sigma实验室具有支持电子取证的条件，且具有多项产研成果，比如敏感数据泄密检查与取证系统[SIGMA-DBS]V1.0. 证书号：软著登字第13397634号、密码信息服务管理系统V1.0. 证书号: 软著登字第3897721号，正在申请通过CNAS认证。

**三、数据安全与网络对抗与保密取证人才培养建设**

课程建设方面，山东大学网络空间安全学院开设《网络安全法》、《网络工程与防御实践》、《计算机取证学》、《安全多方计算》等多项保密技术与攻防体系课程，其中《网络安全法》课程多次邀请公安三所、青岛市纪要保密局、青岛市大数据局等送课入校；《网络工程与防御实践》取证分析模块，多次邀请电子六所、360以及苏州龙信等授课。此外，还在暑期开展海外师资课程“隐私计算前沿讲习”，于2023 年暑期开始联合Hong-Sheng Zhou 教授、Mark Manulis 教授（德国慕尼黑联邦国防军大学）、Willy Susilo 教授（澳大利亚卧龙岗大学）开展隐私计算前沿讲习暑期课程，是国内首次开设的与隐私计算直接相关的海外师资课程。本项目拟从理论到实践方面对隐私计算进行全面介绍。首先，介绍隐私的定义、分类和相关法律法规，如《数据安全法》等，帮助学生了解隐私保护的背景和重要性。接着，探讨现实世界中隐私保护面临的各种威胁和挑战，包括数据泄露、数据滥用、隐私侵犯等，以及与隐私相关的伦理和社会问题。然后，深入研究隐私计算的协议和算法，如安全多方计算（Secure Multi-Party Computation，简称MPC）和同态加密（Homomorphic Encryption），以及基于这些协议的隐私计算应用。最后，探讨在不同领域中的隐私计算应用案例，如医疗保健、金融服务、智能城市等，以帮助学生了解隐私计算在实际场景中的应用和挑战。

教材建设方面，自编《网络工程与防御实践》（陆军院士作序、电子工业出版社），这本书从多个维度深入探讨了网络攻防技术。书中依据漏洞型、攻防型、应急响应型、CTF型等多种类型的靶场进行编写，强调以实战化的网络攻防为核心，力求让读者通过模拟环境深入理解并掌握实际操作技能。在编写过程中，专注于提供可操作的案例与实战训练，全面覆盖了从入门到进阶的网络攻防知识。此外，书中特别新增了入门篇、进阶篇和竞赛篇等攻防实践篇章，为不同层次的读者提供了更具针对性的学习路径，帮助读者逐步提高在复杂环境中应对网络攻击的能力。书籍内容不仅结合当前网络安全的热点技术，还涵盖了应急响应、攻击防御对抗等实战技巧，旨在培养能够应对各种网络安全威胁的高素质网络安全人才。计划编著《计算机取证学实践》一书，专注于计算机取证领域的实践应用，结合现代取证技术和实际操作需求，详细介绍计算机取证的基本原理、方法和技巧。

自编《同态加密与安全多方计算》教材，是一本结合现代密码学前沿技术的专业教材，专注于同态加密（Homomorphic Encryption, HE）和安全多方计算（Secure Multi-Party Computation, MPC）领域。该教材不仅深入探讨了同态加密和多方计算的基本理论、数学基础和算法设计，还特别强调它们在隐私保护、数据安全和云计算等实际应用中的重要作用。书中结合大量实际案例与最新的研究成果，详细介绍了同态加密和MPC的基本原理、实现方法、性能优化技术以及如何解决在实际部署中遇到的挑战。同时，教材还涵盖了这些技术在隐私保护计算、区块链、安全数据共享等新兴领域中的应用，帮助读者建立从理论到实践的全面认知。为了更好地支持学术研究和实践应用，实验室自建了Sigma-MPC密码学隐私增强计算教研平台。该平台是一个集成了同态加密、安全多方计算等密码学技术的创新平台，旨在为研究人员、开发者和学者提供一个便捷、高效的实验环境，用于开发和测试各种隐私增强计算方案。平台支持多种同态加密算法和多方计算协议的实现，并提供易于使用的开发工具和接口，使得学生能够高效地进行隐私保护计算的设计与实验

**四、团队优势（详情见上述内容）**

1 自编《网络工程与防御实践》教材（并已联系电子工业出版社出版），具有自主知识产权的自建Sigma-Range网络攻防靶场，并通过了CNAS认证；

2 自编《同态加密与安全多方计算》教材，自建Sigma-MPC密码学隐私增强计算教研平台；

3 具有自主知识产权的关键字保密查询设备，正在申请通过CNAS认证；

4 建有鹏城靶场山东大学分靶场，并在此基础上搭建了密码分析平台；采购美亚柏科FL2000取证一体机，手机取证塔等设备；