项目名称：开放网络环境下隐私保护与计算效率的协同优化

提名者：湖北省教育厅

提名等级:自然科学二等奖

提名意见：本项目围绕开放网络环境中隐私计算的高效性和安全性的协同优化挑战，取得了一系列原创性理论突破和技术创新，为数据要素的安全流通与高效利用提供了关键支撑，具有重要的科学价值和社会意义。在理论创新方面，项目首创了基于SIMD的多维空间统一编码模型，显著提升了复杂数据密态处理效率，解决了传统隐私计算的性能瓶颈问题；提出了抗泄漏的新型密码学工具AB-HPS，在格密码中实现抗量子攻击的泄漏平滑性安全，并突破密钥膨胀约束，提升了开放式网络环境的安全性；构建了基于有限状态自动机的任务隐匿模型，首次实现动态任务的语义安全执行，为隐私计算的可组合性提供了理论基础。在技术应用方面，研究成果已成功应用于金融、医疗、政务等领域的数据安全共享，推动数据要素“可用不可见”的实践落地。

5篇代表性论文发表于IEEE Transactions on Information Forensics and Security、计算机学报等国内外顶级期刊，1篇入选ESI高被引论文，3篇英文代表作谷歌学术引用634次、SCI他引329次;5篇代表作受到鹏城实验室网络空间安全研究中心、贵州大学公共大数据重点实验室、蚂蚁集团安全协作智能实验室、工业和信息化部安全关键软件重点实验室、公共大数据国家重点实验室、曼彻斯特大学、加拿大滑铁卢大学、南洋理工大学、伦敦大学、乔治·华盛顿大学、不列颠哥伦比亚大学、史蒂文斯理工学院、伊利诺伊大学芝加哥分校等142家知名机构的持续关注

和跟踪研究，引文作者包括 6 位 IEEE Fellow。此外，项目团队获国际会议最佳论文奖 3 项，授权发明专利 15 项，成果转化 3 项，体现了极高的学术影响力与产业价值；成员包括全球高被引科学家和世界前 2%顶尖科学家，成果获国际同行广泛引用与认可。

对照自然科学奖授奖条件，决定提名该项目为 2025 年度湖北省自然科学二等奖。

项目简介：

随着国家数据要素市场化进程加速，隐私计算成为平衡数据安全与价值释放的核心技术。然而，开放网络环境中隐私计算面临性能瓶颈、恶意攻击威胁及任务隐匿性不足三大挑战，严重制约数据要素的安全流通与高效利用。本项目以推动数据要素安全流通与数字经济发展为目标，聚焦开放网络环境的隐私保护与计算效率协同优化问题，突破传统隐私计算理论的局限性，通过“高效密态数据处理→抗泄露安全基座→任务逻辑保护”的研究路线，构建下一代隐私计算的理论框架。

(1) 复杂数据密态处理的多维编码理论。首创基于 SIMD（单指令多数据流）的多维空间统一编码模型，突破传统同态加密、联邦学习等技术的性能瓶颈。通过密态数据压缩与多维计算优化，支持海量高维数据（如自动驾驶实时决策、超大规模协同计算）的高效隐私处理，为复杂业务场景提供理论支撑。

(2) 抗泄漏新型密码学工具。提出有界泄漏模型下的基于属性的哈希证明系统（AB-HPS），首次在格密码中实现抗量子攻击

的泄漏平滑性安全；构建弹性泄漏场景的亚线性密钥膨胀技术，突破“密钥长度与泄漏容量正相关”的传统约束，密钥管理效率提升 50%。该理论为开放式网络抵御侧信道攻击、量子算法破解等威胁提供了可证安全的核心工具。

(3) 任务隐匿的隐私计算自动机模型。提出基于有限状态自动机的形式化任务隐匿模型，通过状态混淆与负载转换技术，消除外包任务的语义泄露风险，防止计算逻辑暴露。模型支持图灵完备的动态任务（如迭代算法、交互协议）隐匿执行，为构建可组合隐私计算系统奠定理论基石。

三项主要成果互为补充：成果(1)的多维编码依赖成果(2)的抗泄漏密码提供底层安全支撑，尤其在量子攻击场景下，格密码的泄漏平滑性可保障编码模型的安全性；成果(3)的任务隐匿需成果(1)的高效密态计算支持，否则动态任务的隐匿执行将因性能问题难以落地；成果(2)的亚线性密钥膨胀技术为成果(3)的自动机模型提供轻量级密钥管理方案，降低状态混淆的通信开销。三项主要成果均通过数学模型重构打破传统约束。成果(1)用 SIMD 多维编码替代传统同态加密的线性计算；成果(2)用 AB-HPS 和亚线性密钥突破泄漏-密钥长度正比关系；成果 3 用自动机状态混淆替代静态任务隐藏。三项主要成果分别从数据、密钥、任务三个层次构建隐私计算的完整技术链，形成“数据安全处理→密钥安全→任务隐匿”的递进防护体系。

5 篇代表作他引 344 次(WOS&CNKI)，1 篇入选 ESI 高被引论文、2 篇发表在信息安全领域国际顶级期刊、2 篇发表在权威中文期刊；5 篇代表作受到鹏城实验室网络空间安全研究中心、贵

州大学公共大数据重点实验室、蚂蚁集团安全协作智能实验室、安徽省工业智能数据安全重点实验室、北京可信计算重点实验室、中国通信安全科学技术实验室、工业和信息化部安全关键软件重点实验室、北京密码学国家重点实验室、公共大数据国家重点实验室、曼彻斯特大学、加拿大滑铁卢大学、南洋理工大学、伦敦大学、萨里大学、乔治·华盛顿大学、不列颠哥伦比亚大学、史蒂文斯理工学院、伊利诺伊大学芝加哥分校、仁川国立大学、伊朗 MAPNA 公司 ICT 项目管理部等 142 家知名机构的持续关注和跟踪研究，引文作者包括 6 位 IEEE Fellow。此外，项目团队获国际会议最佳论文奖 3 项，授权发明专利 15 项，成果转化 3 项；成员包括全球高被引科学家和世界前 2%顶尖科学家，成果获国际同行广泛引用与认可。

代表性论文专著目录（适用于自然科学奖）：

序号	论文（专著）名称/刊名/作者	年、卷、页码	发表时间（年月日）	通讯作者（含共同）	第一作者（含共同）	国内作者	他引总次数	检索数据库	论文署名单位是否包含国外单位	是否国内期刊，如是请填写CN号
1	Efficient Privacy-Preserving Cube-Data Aggregation Scheme for Smart Grids / IEEE Transactions on Information Forensics and Security / Hua Shen, Mingwu Zhang, Jian Shen	2017, 12(6): 1369-1381.	2017-06-01	Mingwu Zhang	Hua Shen	沈华,张明武,沈剑	105	WOS	否	否

2	Efficient Public Key Encryption With Equality Test Supporting Flexible Authorization / IEEE Transactions on Information Forensics and Security / Sha Ma, Qiong Huang, Mingwu Zhang, Bo Yang	2015, 10(3): 458-470.	2014-12-04	Sha Ma	Sha Ma	马莎,黄琼,张明武,杨波	118	WOS	否	否
3	PPO-CPQ: A Privacy-Preserving Optimization of Clinical Pathway Query for E-Healthcare Systems / IEEE Internet of Things Journal / Mingwu Zhang, Yu Chen, Willy Susilo	2020, 7(10): 10660-10672.	2020-10-28	Mingwu Zhang	Mingwu Zhang	张明武,陈誉	106	WOS	是	否
4	隐私保护的推理机策略函数加密及应用 / 计算机学报 / 张明武, 杨波, 王春枝, Tsuyoshi Takagi	2015, 38(4): 897-908.	2014-12-02	张明武	张明武	张明武,杨波,王春枝	6	CNKI	是	11-1826/TP
5	高效弹性泄漏下CCA2安全公钥加密体制 / 计算机学报 / 张明武,陈泌文, 何德彪,杨波	2016, 39(3): 492-502.	2015-07-23	张明武	张明武	张明武,陈泌文,何德彪,杨波	9	CNKI	否	11-1826/TP

主要完成人（单位）：张明武、沈华、马莎

主要完成单位：湖北工业大学、华南农业大学