

2022 年度教育部高等学校科学研究优秀成果奖公示表 (自然科学奖)

项目名称	物理层认证的基础理论与扩展应用
提名单位 (专家)	广东省教育厅
项目简介	<p>物理层认证方法由于其高安全性、低复杂性和高兼容性，近年来受到了广泛关注和重视。然而，物理层认证方法在复杂通信环境下难以满足实际系统性能要求，已成为制约构建新一代网路空间安全体系的瓶颈。该团队在国家自然科学基金和科技部 973 等项目支持下，针对物理层认证方法基础理论和扩展应用领域的关键科学问题，开展了近十年的探索研究，为物理层认证方法的设计、分析、评价与应用奠定了重要的理论基础。主要科学发现为：</p> <p>发现点 1：建立复杂通信环境下物理层认证的理论方法。现有方法在复杂通信环境下性能会急剧恶化。发现发射信号相邻符号之间存在函数关系，设计了盲物理层认证方法。新方法不仅可以克服时变信道和多径信道带来的不利影响，而且对未知用户具有很好的隐蔽性、对干扰信号具有很好的鲁棒性、对敌对用户具有很好的安全性。</p> <p>发现点 2：建立小样本场景下物理层认证的理论方法。现有方法在小样本场景下性能会急剧下降，并需要复杂的预处理操作等。发现对发射信号随机分组并对其发射功率进行微调，可以实现小样本场景下可靠认证。新方法的优势：1) 低复杂性：无需信道估计，无需解调，无需解码；2) 高鲁棒性：性能不受信道估算误差影响；3) 高可靠性：对观测样本长度依赖较少。</p> <p>发现点 3：构建通用物理层认证方法的安全理论模型。物理层认证方法性能分析需要考虑 3 个属性：隐蔽性、安全性和鲁棒性。然而，现有方法中这 3 个属性是分别分析，对参数优化和性能比较带来诸多不便。发现通过分析接收机的认证概率和攻击者的探测概率，可以将上述 3 个属性进行综合考虑，构建通用物理层认证方法的安全理论模型。基于安全理论模型，不仅可以系统地优化物理层认证方法参数，还可以系统地评估不同物理层认证方法的性能。</p> <p>发现点 4：创建物理层认证方法在媒体通信领域应用的理论方法。物理层认证方法不仅能提高无线通信安全，也能提高媒体通信安全，比如二维码。发现非法复制攻击对打印-扫描信道的改变，可以设计出基于物理层认证的低复杂性抗复制攻击二维码。新方法的优势：1) 复杂性低：无需使用复杂的加密算法；2) 成本低：无需使用专用设备；3) 应用广：手机端也可使用。</p> <p>本项目 5 篇代表性论文都发表在通信与安全领域的顶级期刊上，包括 IEEE JSAC、IEEE TIFS、IEEE TDSC 和 IEEE TIP，所有期刊都是中科院一区，TOP 期刊，CCF A 类。论文受到多位院士和多位 IEEE Fellow 的积极评价。基于该项目的研究成果，第一完成人获评广东省高等学校优秀青年教师和 IET Fellow。第二完成人获评广东省特支计划青年拔尖人才和深圳市鹏城学者特聘教授，并是物理层网络编码理论创始人。该项目的科学发现不仅引起学术界的关注，也引起了产业界的高度关注，第一完成人现在正在华为公司 2012 实验室任高级顾问（兼职），尝试将物理层认证技术引入到下一代无线通信标准中。与产业界的深入合作，保证了本项目的研究具有很好应用前景。</p>

主要完成人情况表	<p>(包括：排名、姓名、技术职称、工作单位、完成单位、对本项目重要科学发现的贡献)</p> <p>1. 谢宁，深圳大学教授、博导，广东省高等学校优秀青年教师，华为公司高级顾问（兼职）。近5年以第一作者在权威学术期刊上发表IEEE期刊长文18篇；获得3项美国和30多项中国发明专利授权，有9项发明专利已成功转让；主持国家和省部级以上科研项目20多项。主要贡献：对该项目的所有创新点均有实质性贡献。提出快速衰落信道的盲物理层认证方法，显著提升时变信道和多径信道下的认证性能；提出适用于小样本场景的，斜率物理层认证方法，使认证性能不依赖于信道的相干时间；提出物理层认证的安全模型，不仅可以系统地优化某个物理层认证方法参数，还可以系统地、方便地比较不同物理层认证方法的性能。是代表性论文1, 2, 4的第一作者。</p> <p>2. 张胜利，深圳大学教授、博导，获得广东省特支计划青年拔尖人才，深圳市鹏城学者特聘教授。主要研究方向包括：物理层网络编码、无线通信和区块链技术等。主要研究成果有：首次提出并发展了物理层网络编码理论，首次提出并发展了已知干扰消除理论，首次提出并开发了许可公链系统。共发表中科院二区以上论文30余篇，承担了国家自然科学基金，科技部青年973以及重点研发计划等项目与课题。主要贡献：承担了与该项目密切相关的国家自然科学基金项目和国家973青年科学家项目，在该项目的支持下，提出了基于置信传递算法提出了盲已知干扰消除方法，并参与设计了快速衰落信道的盲物理层认证方法。是代表性论文3的第一作者，代表性论文1的通讯作者。</p> <p>3. 陈昌盛，深圳大学副教授，深圳市海外深圳市高端人才。主要研究信息安全，在二维码和文档图像安全方向做出了重要贡献。近五年在IEEE Trans. 汇刊中发表顶级论文12篇。在工作提出了业界首创的图像二维码、高通用性的防复制二维码、及首次发现以深度网络模型可完成高质量的文档图像篡改。其科研成果获得2021年深圳市科协“优秀自然科学学术论文”奖、2021年第二届中国媒体取证与安全大会“阿里巴巴-最佳报告”奖。主要贡献：提出新的二维码图像嵌入方法，在图像质量和解码鲁棒性之间建立了更好均衡性，并参与设计了斜率物理层认证方法。是代表性论文5的第一作者，代表性论文2的通讯作者。</p> <p>4. 缪伟豪，香港科技大学教授。主要研究领域为：显示-拍摄信道通信、无线通信、编码和信息理论，开创了解决信号检测问题的格检测方法（例如球体解码和复数格约化辅助检测），并统一了广泛应用于前导码和雷达信号的完美单位根序列的所有已知数学建构。迄今为止已出版了2本书，并共同撰写200多份技术出版物，其中以唯一作者发表超过40篇论文。曾担任多份杂志的编辑，包括IEEE Transactions on Wireless Communications, Advances in Mathematics of Communications, 及Cryptography and Communications。先后承担资助科研项目30多项，参编IEEE国际标准2项，已累计获授权发明专利30余项。主要贡献：参与设计了新的二维码图像嵌入方法，在图像质量和解码鲁棒性之间建立了更好均衡性。是代表性论文5的通讯作者。</p> <p>5. 王晖，深圳信息职业技术学院校长、教授、博导，担任广东省大规模移动计算与智能网联工程技术研究中心和深圳大学区块链技术研究中心主任。王晖教授多年来一直从事无线网络与无线通信的理论研究与应用研究。在IEEE JSAC、IEEE TWC, 《电子学报》、《电子科学学刊》等国内外知名刊物和会议发表论文60余篇，授权/申请发明专利20余项。在美国Springer出版社、CRC出版社出版学术专著（章节）两部。近年，在分布式学习、安全有效的区块链共识算法和可信计算等领域展开研究工作，设计并实现了安全、可信的联邦学习参数聚合以及隐私保护智能电网能源调度方案，并搭建了大规模区块链仿真实验验证系统。主要贡献：参与设计了基于置信传递算法提出了盲已知干扰消除方法，在快速衰落信道下能达到最大后验概率最优接收的近似性能。是代表性论文3的通讯作者。</p>			
	主要完成单位	深圳大学 香港科技大学		
	代表性论文（专著）目录			
	序号	论文（专著）名称	刊名	所有作者
	1	Blind Authentication at the Physical Layer under Time-Varying Fading Channels	IEEE Journal on Selected Areas in Communications (IEEE JSAC)	谢宁，张胜利

2	Slope Authentication at the Physical Layer	IEEE Transactions on Information Forensics and Security (IEEE TIFS)	谢宁, 陈昌盛
3	Blind Known Interference Cancellation	IEEE Journal on Selected Areas in Communications (IEEE JSAC)	张胜利, 刘紹强, 王晖
4	Security Model of Authentication at the Physical Layer and Performance Analysis over Fading Channels	IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)	谢宁, 陈昌盛, 明仲
5	PiCode: A New Picture-Embedding 2D Barcode	IEEE Transactions on Image Processing (IEEE TIP)	陈昌盛, 黄文坚, 周保健, 刘辰辰, 繆伟豪