

姓 名：邓伦治

职 称：三级教授

邮 箱：denglunzhi@163.com



基本情况

邓伦治，男，贵州桐梓人，1979年8月生，理学博士，现为贵州师范大学科学与技术处副处长，三级教授，博士生导师，贵州“省政府特殊津贴”专家。

研究方向

密码学，信息安全、隐私保护

开设课程

抽象代数、密码学基础、密码协议

教育经历

1. 2009-09 至 2012-06，厦门大学，数学科学学院，博士
2. 2005-09 至 2008-06，贵州师范大学，数学与计算机科学学院，硕士
3. 1998-09 至 2002-06，贵州师范大学，数学与应用数学，学士

工作经历

1. 2013-12 至今，贵州师范大学，数学科学学院，教授
2. 2011-12 至 2013-12，贵州师范大学，数学与计算机科学学院，副教授
3. 2007-12 至 2011-12，贵州师范大学，数学与计算机科学学院，讲师
4. 2002-07 至 2007-12，贵州师范大学，数学与计算机科学学院，助教

科研成果

近 5 年发表的 SCI 期刊论文（第一作者）

- [1]. **Lunzhi Deng**, Jianxin Shao, Zhenyu Hu: Identity based two-party authenticated key agreement scheme for vehicular ad hoc networks. Peer-to-Peer Networking and Applications, vol.14, pp.2236–2247, 2021 (SCI期刊, 中科院3区)
- [2]. **Lunzhi Deng**, Yixian Yang, Ronghai Gao: Certificateless designated verifier anonymous aggregate signature scheme for healthcare wireless sensor network. IEEE Internet of Thing Journal, vol.8, Issue.11, pp.8897- 8909, 2021. (SCI期刊, 中科院1区)
- [3]. **Lunzhi Deng**, Ronghai Gao: Certificateless two-party authenticated key agreement scheme for smart grid. Information Sciences, vol.543, pp.143–156, 2021. (SCI期刊, 中科院1区)
- [4]. **Lunzhi Deng**, Xiuru He, Tian Xia: Secure identity-based blind signature scheme for online transactions. Wireless Personal Communications, vol.116, pp.1525-1537, 2021. (SCI期刊, 中科院4区)
- [5]. **Lunzhi Deng**, Benjuan Yang, Xiangbin Wang: A lightweight identity-based remote data auditing scheme for cloud storage, IEEE Access, vol.8, pp. 206396-206405, 2020. (SCI期刊, 中科院2区)
- [6]. **Lunzhi Deng**, Bingqin Ning, Yuhong Jiang: A lightweight certificateless aggregation signature scheme with provably security in the standard model. IEEE Systems Journal, vol.14, no.3, pp.4242-4251, 2020. (SCI期刊, 中科院2区)
- [7]. **Lunzhi Deng**: Anonymous aggregate encryption scheme for industrial internet of things. IEEE Systems Journal, vol.14, no.3, pp.3999-4006, 2020. (SCI期刊, 中科院2区)
- [8]. **Lunzhi Deng**: An improved certificateless two-party authenticated key agreement protocol for wireless sensor networks. International Journal Ad Hoc and Ubiquitous Computing, vol.34, no. 4, pp.208-215, 2020. (SCI期刊, 中科院4区)
- [9]. **Lunzhi Deng**, Tian Xia, Xiuru He: Provably secure certificateless encryption scheme in the standard model. KSII Transactions on Internet and Information, vol.14.no.6, pp.2534-2553, 2020. (SCI期刊, 中科院4区)
- [10]. **Lunzhi Deng**, Siwei Li, Huawei Huang, Yuhong Jiang, Bingqin Ning: Certificateless ring signature scheme from elliptic curve group. Journal of Internet Technology, vol. 2, no.3, pp.715-723, 2020. (SCI期刊, 中科院4区)
- [11]. **Lunzhi Deng**, Hongyu Shi, Yan Gao: Certificateless Linkable Ring Signature Scheme. IEEE Access, vol.8, pp. 54641-54651, 2020. (SCI期刊, 中科院2区)
- [12]. **Lunzhi Deng**: Anonymous certificateless multi-receiver encryption scheme for smart community management systems. Soft Computing, vol.24, pp.281–292, 2020. (SCI期刊, 中科院3区)
- [13]. **Lunzhi Deng**; Yuhong Jiang; Yuling Chen: Identity-Based Linkable Ring Signature Scheme. IEEE Access, vol.7, pp. 153969-153976, 2019. (SCI期刊, 中科院2区)

院2区)

- [14]. **Lunzhi Deng**; Yixian Yang; Yuling Chen; Certificateless short aggregate signature scheme for mobile devices. *IEEE Access*, vol.7, pp. 87162-87168, 2019. (SCI, 中科院2区)
- [15]. **Lunzhi Deng**; Yixian Yang; Yuling Chen; Xiong Wang: Aggregate signature without pairing from certificateless cryptography, *Journal of Internet Technology*, vol.19, no.5, pp.1479-1486, 2018. (SCI期刊, 中科院4区)
- [16]. **Lunzhi Deng**; Yixian Yang; Ronghai Gao; Yuling Chen: Certificateless short signature scheme from pairing in the standard model, *International Journal of Communication Systems*, vol.31, no.17, pp.1-8, 2018. (SCI期刊, 中科院4区)
- [17]. **Lunzhi Deng**, Jiwen Zeng, Huawei Huang: ID-based multi-signer universal designated multi-verifier signature based on discrete logarithm, *Chiang Mai Journal of Science*, vol.45, no.1, pp. 617-624, 2018. (SCI期刊, 中科院4区)
- [18]. **Lunzhi Deng**, Yixian Yang, Yuling Chen: Certificateless multi-signer universal designated multi-verifier signature from elliptic curve group, *KSII Transactions on Internet and Information Systems*, vol.11, no.11, pp.5625-5641, 2017. (SCI期刊, 中科院4区)
- [19]. **Lunzhi Deng**: An improved certificateless encryption scheme for telecare medicine information systems, *Journal of Internet Technology*, vol.18, no.2, pp. 223-227, 2017. (SCI期刊, 中科院4区)

科研项目

1. 多用户情境下两类公钥加密方案的理论研究, 国家自然科学基金项目(61962011), 2020-01-01 至 2023-12-31, 经费: 40 万元, 主持。
2. 可证明安全理论下两类公钥签名方案的设计与应用研究, 国家自然科学基金项目(61562012), 2016-11-01 至 2019-12-31, 经费: 41.2 万元, 主持。
3. 云储存数据完整性审计机制的理论与应用研究, 贵州省科技计划重点项目(黔科合基础[2019]1434 号), 2019.01.01 至 2022.12.31, 经费: 30 万元, 主持。
4. 公钥体制下云存储数据完整性检验机制的设计理论及其应用研究, 贵州省教育厅创新群体重大研究项目(黔教合 KY 字[2016]026), 2016-11-01 至 2020-10-31, 经费: 20 万元, 主持。
5. 半群及基于半群理论的密码方案的设计, 贵州师范大学博士科研基金项目

[2013], 2012-12-20 至 2016-06-30, 经费: 10 万元, 主持。

6. 半群及其在公钥密码中的应用, 贵州省科学技术基金项目 (黔科合 J 字 LKS [2013]02), 2014-01-01 至 2016-12-31, 经费: 3.4 万元, 主持。

7. 与等价关系和序关系相关联半群的刻画, 贵州省科学技术基金项目 (黔科合 J 字 LKS [2010]02), 2010-12-01 至 2012-12-31, 经费: 3 万元, 主持。

获奖情况

1. 2020 年, 被评为贵州“省政府特殊津贴”专家。