亢保元

职称： 教授　　　政治面貌：民盟

办公地点：C601　电子邮箱：baoyuankang@aliyun.com

教学科研简介

教学方面，多年来为本科生、研究生主讲过“离散数学”、“组合数学”、“高等数学”、“高等代数”、“概率论与数理统计”、“抽象代数”、“算法设计与分析”、“计算机密码学”等课程；参加编写《密码学教程》、《线性代数与解析几何》两本教材；参加中南大学和西北工业大学教改项目三项；获得西北工业大学优秀教学成果二等奖一项；获得陕西省第二届青年教师高等数学讲课比赛二等奖。

科研方面，主持完成天津市自然科学基金项目一项；参加完成国防预研基金项目一项；参加完成国家自然科学基金两项；参加完成湖南省自然科学基金两项；在国际、国内期刊及学术会议上发表论文八十余篇，SCI、EI 收录论文二十余篇，应邀为多个国际学术期刊的论文审稿，目前主要研究方向为数字签名、身份认证、电子货币等。

学习经历

（1）1995-09 至 1999-03，西安电子科技大学，密码学专业，博士
（2）1990-09 至 1993-07，山西大学，基础数学专业，硕士
（3）1983-09-至 1987-07，宝鸡师范学院，基础数学专业，学士

工作经历

（1）2009-05 至今，天津工业大学，软件学院，教授
（2）1999-07-2009-05，中南大学，数学科学与计算技术学院，副教授，教授
（期中 2007-03-2008-03，澳大利亚昆士兰科技大学，信息安全学院，国家公派访问学者）
（3）1993-07-1999-07，西北工业大学，应用数学系，助教，讲师

主讲课程

高等数学，线性代数，计算机密码学，离散数学

代表性论文

[1] Baoyuan Kang,Yanbao Han, Kun Qian,Jianqi Du, Analysis and Improvement on an Authentication Protocol for IoT-Enabled Devices in Distributed Cloud Computing

Environment, Mathematical Problems in Engineering, 2020, 2020.

[2] Baoyuan Kang, Jianqi Du, Yanbao Han, and Kun Qian, A Lightweight Anonymous Mobile Payment Scheme for Digital Commodity in Cloud Computing Service, International Journal of Network Security, Vol.22, No.6, 2020, PP.945-953

[3] Baoyuan, Kang, Mu Wang, Dongya, Jing，An Off-Line Payment Scheme for Digital Content via Subliminal Channel，Journal of information science and engineering , vol.34, pp. 171-192 (2018)

[4] Baoyuan Kang, Dongyang Shao and Jiaqiang Wang，A fair electronic payment system for digital content using elliptic curve cryptography，Journal of Algorithms & Computational Technology , vol. 12, no. 1, pp. 13-19, 2018

[5] Baoyuan Kang，Lin Si， Hong Jiang， Chunqing Li， Mingming Xie，ID-Based Public Auditing Protocol for Cloud Data Integrity Checking with Privacy-Preserving and Effective Aggregation Verification ， Security and Communication Networks，Volume 2018, Article ID 3205898, 9 pages，https://doi.org/10.1155/2018/3205898

[6] Baoyuan Kang, Jiaqiang Wang and Dongyang Shao, Certificateless public auditing with privacy preserving for cloud assisted wireless body area networks, Mobile information systems, vol. 2017, Article ID 2925465, 5 pages. https://doi.org/10.1155/2017/2925465

[7] Baoyuan Kang, Jiaqiang Wang and Dongyang Shao, Attack on privacy－reserving public auditing schemes for cloud storage, Mathematical problems in engineering, vol. 2017, Article ID 8062182, https://doi.org/10.1155/2017/8062182

[8] Kang Baoyuan, Wang Mu, Jing Dongya, An efficient certificateless aggregate signature scheme, Wuhan university journal of natural sciences, vol. 22, no. 2, 2017, pp. 165-170.

[9] Kang, Baoyuan, Xu, Danhui, Secure Electronic Cash Scheme with Anonymity Revocation, Mobile Information Systems, vol. 2016, Article ID 2620141 http://dx.doi.org/10.1155/2016/2620141

[10] Baoyuan Kang, Danhui Xu , Perfect-Mail: A secure e-mail protocol with perfect forward secrecy, British Journal of Mathematics and Computer Science, vol.12, no.5, pp. 1-11, 2016

[11] Kang, Baoyuan , Xu, Danhui, A secure certificateless aggregate signature scheme, International Journal of Security and its Applications, vol. 10, no. 3, pp. 55-68, 2016

[12] Kang, Baoyuan , Xu, Danhui, An untraceable off-line electronic cash scheme without merchant frauds, International Journal of Hybrid Information Technology, vol. 9, no. 1, pp. 431-442, 2016

[13] Kang, Baoyuan , Xu, Danhui, A secure multi-receivers e-mail protocol, International Journal of Multimedia and Ubiquitous Engineering, vol. 11, no. 11, pp. 335-342, 2016

[14] Baoyuan Kang, On delegatability of some strong designated verifier signature schemes, Mathematics problems in engineering, Volume 2014, Article ID 761487, 5 pages, doi: 10.1155/2014/761487.

[15] Baoyuan Kang, Colin Boyd, Ed Dawson, A novel identity-based strong designated verifier signature scheme, Journal of Systems and Software, vol. 82, no. 2, February, 2009, pp. 270-273

[16] Baoyuan Kang, Colin Boyd, Ed Dawson, Identity-based strong designated verifier signature schemes: Attacks and new construction. Computers and Electrical Engineering, vol. 35, no. 1, January, 2009, pp. 49-53

[17] Baoyuan Kang, Colin Boyd, Ed Dawson, A novel nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. Computers and Electrical Engineering, vol. 35, no. 1, January, 2009, pp. 9-17

[18] Baoyuan Kang, ID-based aggregate signature scheme with constant pairing computations: attack and new construction, Journal of Computational Information Systems, vol. 8, no. 16, pp. 6611-6618, 2012

[19] Baoyuan Kang, Attacks on One Designated Verifier Proxy Signature Scheme, Journal of applied mathematics, Volume 2012, Article ID 508981, 6 pages, doi: 10.1155/2012/508981

[20] Baoyuan Kang, On the security of some aggregate signature schemes, Journal of applied mathematics, Volume 2012, Article ID 416137, 10 pages, doi: 10.1155/2012/416137

教学科研项目

（1）天津市自然科学基金，面上项目（编号：15JCYBJC15900），信息安全中强安全聚合签名的研究，2015/04-2018/03，10 万，主持。

（2）国家自然科学基金（编号：61202099），车载自组织网络数据安全聚合机理与方法研究。参加

获奖情况