亢保元，男，教授，博士，硕士生导师。1987 年毕业于宝鸡师范学院数学系，获得基础数学专业学士学位；1993 年毕业于山西大学数学系，获得基础数学专业硕士学位；1999年毕业于西安电子科技大学通信工程学院，获得密码学专业博士学位。2007 年3 月至2008年3 月在澳大利亚昆士兰科技大学信息安全学院留学访问。1993 年7 月至1999年7 月在西北工业大学应用数学系任教；1999 年7 月至2009年7 月在中南大学数学科学与计算技术学院任教；2009 年7 月调到天津工业大学计算机科学与软件学院工作。

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”、“编码学”、“密码学”、“数字签名技术”、“信息安全”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，目前主持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一项；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七十余篇，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。

主要研究方向：（1）数字签名
（2）身份认证与密钥共识
（3）安全电子商务协议

联系方式：Tel: 022-83956358
Email: baoyuankang@aliyun.com

近几年以第一作者发表的主要论文：

[1] 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)

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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.

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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.

[13] 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

[14] 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

[15] 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

[16] 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

[17] Baoyuan Kang, Dongyang Shao, Jiaqiang Wang，Improved Incentive-Based Electronic Payment Scheme for Digital Content，International Journal of Engineering Research And Management (IJERM), vol.4, no. 9, September 2017

[18] 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

[19] 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

[20] Baoyuan Kang, New types of verifiably encrypted signature schemes，Advanced Materials Research, vol. 490-495, pp. 914-918, 2012, Mechatronics

and Intelligent Materials II

[21] Baoyuan Kang, Jinguang Han and Qingju Wang, A new threshold multi-proxy multi-signature scheme, Journal of electronics (china), no.4, 2006, pp. 560-563

[22] Baoyuan Kang, Improvement on Lin-Wu(t,n)-threshold verifiable mult-secret sharing scheme, Chinese Journal of Engineering Mathematics，2006（5）,pp 881-885.

[23] Baoyuan Kang，Cryptanalysis on an e-voting scheme over computer network, International Conference on Computer Science and Software Engineering, vol. 3, December, 2008, pp. 826-829.

[24] Baoyuan Kang, Jinguang Han， On the Security of Blind Signature and Partially Blind Signature，2010 2nd International Conference on Education Technology and Computer. vol.5. June, 2010, pp. 206-208

[25] Baoyuan Kang, Jinguang Han， A More Practical and Efficient Threshold Proxy Signature Scheme，2010 2nd International Conference on Education Technology and Computer. vol.5, June, 2010, pp. 202-205

[26] Baoyuan Kang, Jinguang Han and Qingju Wang，On the Security of Proxy Blind Multi-signature Scheme without a Secure Channel，2010 2nd International Conference on Computer Engineering and Technology. April, 2010, vol.1, pp. 62-64

[27] Baoyuan Kang, Tong Lu，Cryptanalysis and Improvement on Key-Insulated Signature Scheme，2010 1nd International Conference on Computer and Automation Engineering. December, 2010, pp. 149-151