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: 022-58685358
Email: baoyuankang@aliyun.com

近几年以第一作者发表的主要论文：

[1] Baoyuan Kang, Colin Boyd, Ed Dawson, A novel identity-based strong designated verifier signature scheme, Journal of Systems and Software, v 82, n 2, February, 2009, pp 270-273.

[2] Baoyuan Kang, Colin Boyd, Ed Dawson, Identity-based strong designated verifier signature schemes: Attacks and new construction，Computers and Electrical Engineer ing, v35, n1, January, 2009, pp 49-53.

[3] Baoyuan Kang, Colin Boyd, Ed Dawson, A novel non-repudiable threshold multi-proxy mult i-signature scheme with shared verification, Computers and Electrical Engineering, v 35,n 1, January, 2009, pp 9-17.

[4] 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.

[5] Baoyuan Kang, ID-based aggregate signature scheme with constant pairing computations:attack and new construction, Journal of Computational Information Systems, v 8, n 16, p6611-6618, 2012.

[6] Baoyuan Kang, Attacks on One Designated Ver ifier Proxy Signature Scheme, Journal of applied mathemat ics, Volume 2012, Article ID **508981**

[7] Baoyuan Kang, On the security of some aggregate signature schemes, Journal of

applied mathematics, Volume 2012, Article ID 416137

[8] Baoyuan Kang, New types of verifiably encrypted signature schemes， Advanced Materials Research, v 490-495, p 914-918, 2012, Mechatronics and Intelligent Mater ials II.

[9] Baoyuan Kang, Danhui Xu , Secure Electronic Cash Scheme with Anonymity Revocation, Mobile Information Systems ,Volume 2016 (2016), Article ID 2620141, 10 pages.

[10] Kang, Baoyuan , Xu, Danhui, An untraceable off-line electronic cash scheme without merchant frauds, International Journal of Hybrid Information Technology, v 9, n 1, p 431-442, 2016

[11] Kang, Baoyuan , Xu, Danhui, A secure certificateless aggregate signature scheme, International Journal of Security and its Applications, v 10, n 3, p 55-68, 2016

[12] Baoyuan Kang, Danhui Xu , Perfect-Mail: A secure e-mail protocol with perfect forward secrecy, British Journal of Mathematics and Computer Science, 12(5): 1-11,2016.

[13] Baoyuan Kang, Verifiably encrypted signature schemes: attacks and general constructions, Advances in information science and service sciences, v 5, n 7, 2013, pp 573-580.

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

[15] 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.

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

[17] Baoyuan Kang, Tong Lu，Cryptanalysis and Improvement on Key-Insulated SignatureScheme， 2010 1nd International Conference on Computer and Automation Engineer， December. 2010, pp 149-151.

[18] Baoyuan Kang, Jinguang Han and Qingju Wang， An Improvement on Conference Key Agreement Protocol with User Anonymity， 2010 2nd International Conference on Computer Engineering and Technology. Vol.1, April, 2010, pp 58-61.

[19] Baoyuan Kang, Jinguang Han and Qingju Wang，Cryptanalysis and Improvement on an IC-card-based Remote Login Mechanism， 2010 2nd International Conference on Computer Engineering and Technology. Vol.1, April, 2010, pp 65-68.

[20] Baoyuan Kang, Jinguang Han, Cryptanalysis and improvement on three-party protocols for password authenticated key exchange, 2010 2nd International Conference on Education Technology and Computer, vol. 5, 2010, pp5197-5201.