曹正军

姓名	曹正军
职称/职务	副教授
电话/传真	021-66132414
电子邮箱	caozhj@shu.edu.cn
个人主页	
学科/专业	应用数学
主要研究领域	密码学
学术/社会兼职	美国数学评论评论员
主要获奖	中国科学院研究生院首届中澳BHBP奖学金, 黑龙江省第三届优秀硕士论文奖
主要课程教学	信息论, 编码理论, 高等数学
主要学术成果	(1)首次提出数字签名模型分类问题,并给出了迄今最好的分类结果. (2) 证明若干量子密钥分享协议不是真正的密钥分享而是密钥协商. (3) 证明广为人知的Gottesman-Chaung量子数字签名方案中没有真正的量子态公钥. (4) 提出一个用来优化公钥密码协议的基本准则--较少参数原理. (5) 首次提出在Shor大数分解算法中引入第三个量子寄存器, 预见该算法依赖于一种全新的宏观量子纠缠现象.
代表性论著	(1) ZJ Cao, ML Liu: Classification of Signature-only Signature Models, Science in China Series F-Information Sciences, Vol.51(8),pp.1083-1095 (2008) (2) ZJ Cao, O. Markowitch: A note on an arbitrated quantum signature scheme, Int. J. Quantum Information. Vol.7(6),Sep.2009,pp.1205-1209 (2009) (3) ZJ Cao, O. Markowitch: A note on some quantum secret sharing schemes, Int. J. Quantum Information. Vol.8(3),2010,pp.451-456 (2010) (4) LH Liu, ZJ Cao: On computing $Ord_N(2)$ and its application,Information and Computation,204,pp.1173-1178 (2006) (5) ZJ Cao: Analysis of One Popular Group Signature Scheme, AsiaCrypt2006, LNCS 4284, pp. 460-466 (2006) (6) ZJ Cao, LH Liu: On the Complexity of Shor's Algorithm for Factorization, Second International Symposium on Information Science and Engineering (ISISE), pp.164-168 (2009) (7) ZJ Cao, X Fan: Extension of Barreto-Voloch Root Extraction Method, 13th International Conference on Information and Communications Security, ICICS2011, LNCS,7043, pp.184-189 (2011) (8) ZJ Cao: A Note On Gottesman-Chuang Quantum Signature Scheme. IACR Cryptology ePrint Archive 2010: 317 (2010) (9) ZJ Cao: A Principle for Cryptographic Protocols Beyond Security, Less Parameters. IACR Cryptology ePrint Archive 2010: 51 (2010) (10)曹正军,刘木兰:数字签名方案中的孤悬因子及冗余数据,计算机学报,2006(2),pp.249-255 (11)曹正军,刘木兰:一个基于强 RSA签名方案的改进,计算机学报,2006(9)pp.1617-1621 (12)曹正军,刘丽华:两个指定验证人签名方案的安全性分析,软件学报,Vol.19(7),pp.1753-1757 (2008)