2007 年度

2007 年度实验室共发表论文及著作 94 篇，其中 EI 检索 48 篇，SCI 检索 21 篇。论文及著作列表如下。

1. Fanyu Kong, Jia Yu, Zhun Cai, Daxing Li, New Left-to-right Radix-r Signed-digit Recoding Algorithm for Pairing-based Cryptosystems, The 4th Annual Conference on Theory and Applications of Models of Computation, LNCS 4484, pp. 189-198, Springer-Verlag, 2007. (EI)
2. Fanyu Kong, Jia Yu, Baodong Qin, Daxing Li, Cryptanalysis of Server-aided RSA Key Generation Protocols at MADNES 2005, The 4th International Conference on Autonomic and Trusted Computing (ATC-07), LNCS 4610, pp. 52-60, Springer-Verlag, 2007. (EI)
3. Fanyu Kong, Baodong Qin, Jia Yu, Daxing Li, A Note on Short Private Key Attacks on RSA-type Cryptosystems over Conic Curves, ChinaCrypt 2007 (in Chinese), pp.109-115, 2007.
4. Fanyu kong, Jia Yu, Guangqing Zhang, Daxing Li, Cryptanalysis of a Robust Protocol for Generating Shared RSA Parameters, CCWMSN 2007, pp.1085-1088, IET press, 2007.(EI)
5. Meiqin Wang, Lin Li et.al, A Hybrid Approach for Authenticating MPEG-2 Streaming Data, MCAM 2007, LNCS 4577, pp.203-212, 2007. (EI)
6. Xianmeng Meng, A mean value theorem on the binary Goldbach problem and its application. Monatsh. Math. 151 (2007), no. 4, pp. 319-332, 2007. (SCI)
7. Xianmeng Meng (with M. Q. Wang), On additive problems with prime numbers of special type. Demonstratio Math. 40 (2007), no. 2, pp. 271—287, 2007.
8. Xianmeng Meng, The Goldbach problems with prime numbers of special type. (Chinese) Acta Math. Sinica (Chin. Ser.) 50 (2007), no. 2, pp. 255—260, 2007. (SCI)
9. Hongbo Yu, Xiaoyun Wang, Multi-collision Attack on the Compression Functions of MD4 and 3-Pass HAVAL, ICISC 2007, LNCS 4817, pp.206-226,2007. (EI)
10. 刘华宁，张文鹏, General Kloosterman sums and the difference between an integer and its inverse modulo q, Acta Mathematica Sinica English Series, 2007, 23(1): 77-82. (SCI) (博士后)
11. 刘华宁，张文鹏, Hybrid mean value of generalized Bernoulli numbers,general Kloosterman sums and Gauss sums, Journal of the Korean Mathematical Society,2007,44 (1): 11-24. (SCI) (博士后)
12. 刘华宁，张文鹏, Generalized Cochrane sums and Cochrane-Hardy sums, Journal of Number Theory, 2007,

122(2): 415-428. (SCI) (博士后)

13. 刘华宁, A note on local randomness in polynomial random number and random function generators, Applied Mathematics and Computation, 2007, 186: 1360-1366. (SCI) (博士后)
14. 刘华宁，张文鹏, Mean value on the difference between a quadratic residue and its inverse modulo p, Acta Mathematica Sinica English Series, 2007, 23: 915-924. (SCI) (博士后)
15. 刘华宁, New pseudorandom sequences constructed by quadratic residues and Lehmer numbers, Proceedings of the American Mathematical Society, 2007, 135(5): 1309-1318. (SCI) (博士后)
16. 刘华宁, Some generalizations of Knopp's identity, Bulletin of the Brazilian Mathematical Society, 2007, 38: 179-188. (SCI) (博士后)
17. 刘华宁, A note on the upper bound estimate of high-dimensional Cochrane sum, Journal of Number Theory, 2007, 125: 7-13. (SCI) (博士后)
18. 刘华宁，张文鹏, Hybrid mean value results for a generalization on a problem of D.H. Lehmer and Hyper-Kloosterman sums, Osaka Journal of Mathematics, 2007, 44: 615-637. (SCI) (博士后)
19. 刘华宁, On the mean values of the homogeneous Dedekind sums and Cochrane sums in short intervals, Journal of the Korean Mathematical Society, 2007, 44: 1243-1254. (SCI) (博士后)
20. 刘华宁，张文鹏, Hybrid mean value of a generalization on a problem of D. H. Lehmer, Acta Arithmetica, 2007, 130(1): 1-17. (SCI) (博士后)
21. 刘华宁, A family of pseudorandom binary sequences constructed by the multiplicative inverse, Acta Arithmetica, 2007, 130(2): 167-180. (SCI) (博士后)
22. 刘华宁, On a problem of D. H. Lehmer and Hyper-Kloosterman sums, 数学进展, 2007, 36: 245-252. (博士后)
23. 刘华宁，一些新数列的偏差与伪随机性，数学年刊, 2007, 28(3): 319-328. (博士后)
24. 孔凡玉，秦宝东，于佳，李大兴，环 Zn 上圆锥曲线的 RSA 密码的短私钥攻击的注记, ChinaCrypt’2007-第十届中国密码学学术会议论文集, pp.109-115，西南交通大学出版社, 2007.
25. Jianwei Shang, Feng Li, Yanyan Zhang. A Secure Distributed Symmetric Key Generation Scheme. IMECS'2007. pp.375-379. (EI)
26. Jianya Liu, Y. Ye. Perron's formula and the prime number theorem for automor-phic L-functions, Pure Appl. Math. Q., 3 (2007), 481-497. (SCI)
27. Jianya Liu. A large sieve estimate for Dirichlet polynomials and its applications, Ann.Univ. Sci. Budapest., Sect. Comp., 27 (2007), 91-110. (SCI)
28. Jianya Liu. (with T. Zhan) The quadratic Waring-Goldbach problem, J. Shandong Univ.,42(2) (2007), 1-18. (SCI)

29. Guanshi Lv. Y.F. Xu. Hua's theorem with nine almost equal prime variables, Acta Mathematica Hungarica, 116(2007), 309-326. (SCI)
30. Guanshi Lv. Gauss's three squares theorem with almost prime variables, Acta Arith., 128(2007), 391-399. (SCI)
31. Guanshi Lv. (With H.X. Lao) On exponential sums over primes in short intervals, Monatshfte fur Mathematik, 151(2007), 153-164. (SCI)
32. Xiumin ren, K.M. Tsang. Waring-Goldbach problem for unlike powers, Acta. Math. Sinica. , English Series. (2)23(2007), 265-280.
33. Xiumim Ren, K.M. Tsang., Waring-Goldbach problem for unlike powers (II), Acta. Math. Sinica. (Chinese Series) (1)50(2007), 175-182.
34. 李继宝，李庆忠，闫中敏，基于 Deep Web 的地图搜索系统的研究与实现. 山东大学学报(理学版), 2007, Vol.42, No.11.
35. 黎林, MD4 算法分析，山东大学学报(理学版), 42(4), pp 1-5, 2007.4.
36. 张闻宇，张海纳，改进的 7 轮 AES-192 的碰撞攻击，山东大学学报(理学版), 42(4), pp 6-9, 2007.
37. 黎林，三圈 RIPEMD-128 的碰撞攻击，山东大学学报(理学版), 42(3), pp 1-12, 2007.
38. 张闻宇，黎琳, 7 轮 AES-192 的飞去来器攻击，计算机工程与应用, 43(21), pp 16-17, 2007.
39. Gaoli Wang, Related-Key Rectangle Attack on 43-Round SHACAL-2, ISPEC 2007, pp 33-42, 2007/5/7. (EI)
40. Puwen Wei, Mingqiang Wang, Wei Wang, A Note on Shacham and Waters Ring Signatures. Proceedings-2007 International Conference on Computational Intelligence and Security, pp. 652-656, 2007. (EI)
41. 王少辉，郑世慧，张国艳，指定接收人的一次代理签名，计算机工程与应用, 2007 年 22 期, pp.10-12, 2007.
42. 王少辉，张国艳，展涛. Waters 签名方案的研究，通信学报(增刊), 11A, pp. 181-185, 2007.
43. 张国艳，郑世慧，有效的门限签名算法，计算机工程与应用, 2007 年 08 期, pp. 15-17, 2007.
44. Feng Li, Jianwei Shang, Daxing Li, A Proactive Secure Multisecret Sharing Threshold Scheme, SNPD (1)'2007. pp.105-110. (EI)
45. Baodong Qin, Ming Li, Fanyu Kong, Daxing Li. Security Analysis of wrNAF and SPA Resistant Scalar Multiplication", 8th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD 2007), pp. 279-284，New York: IEEE Computer Society, July 2007. (EI)
46. Baodong Qin, Ming Li, Fanyu Kong, Further Cryptanalysis of a Provably Secure CRT-RSA Algorithm, The First International Symposium on Data, Privacy and E-Commerce - ISDPE 2007, pp.327-331, 2007. (EI)
47. 秦宝东,李明,孔凡玉,李大兴. 环 Zn 上圆锥曲线 RSA 型公钥密码体系的小私钥指数攻击[C]，中国信息和

通信安全学术会议(CCICS’2007).

48. Ming Li, Baodong Qin, Fanyu Kong, Daxing Li, Further Cryptanalysis of a CRT-RSA Algorithm at CCS 2003, IFIP International Conference on Network and Parallel Computing Workshops 2007, pp. 72–76, Sept. 2007. (EI)
49. Ming Li, Baodong Qin, Fanyu Kong, Daxing Li, Wide-w-NAF Method for Scalar Multiplication on Koblitz Curves, 8th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing - SNPD 2007, pp. 143-148， New York: IEEE Computer Society, July 2007. (EI)
50. 张光庆，孔凡玉，李大兴. Koblitz 曲线上抵抗简单功耗分析的有效算法，山东大学学报(工学版)，37(3), pp. 78-80, 2007.
51. Chengyu Hu, Daxing Li. An Efficient Threshold Group Signature Scheme. IMECS'2007. pp.338-340. (EI)
52. Chengyu Hu, Daxing Li. A New Type of Proxy Ring Signature Scheme with Revocable Anonymity. SNPD (1)'2007. pp.866-868. (EI)
53. Chengyu Hu, Daxing Li. Ring Blind Signature Scheme. SNPD (1)'2007. pp.869-871. (EI)
54. Guowen Li, Jia Yu, Rupeng Li, Daxing Li. An Approach to Convert Any Threshold Signature into a Threshold Group Signature. SNPD (2)'2007. pp.723-726. (EI)
55. Rupeng Li, Jia Yu, Jin Wang, Guowen Li, Daxing Li. Key-Insulated Group Signature Scheme with Verifier-Local Revocation. SNPD (3)'2007. pp.273-278. (EI)
56. Chengyu Hu, Daxing Li. Forward-Secure Traceable Ring Signature. SNPD (3)'2007. pp.200-204. (EI)
57. Jin Wang, Xi Bai, Jia Yu, Daxing Li. Protecting Against Key Escrow and Key Exposure in Identity-Based Cryptosystem. TAMC'2007. pp.148-158 (EI)
58. Rupeng Li, Xianghua Du, Guowen Li, Jia Yu, Daxing Li. Key-Insulated Group Signature Scheme with Selective Revocation. MUE'2007. pp.1057-1063. (EI)
59. Guowen Li, Jia Yu, Rupeng Li, Daxing Li. Two Threshold Multisignature Schemes from Bilinear Pairings. MUE'2007. pp.1041-1045. (EI)
60. Rupeng Li, Jia Yu, Guowen Li, Daxing Li. A New Identity-Based Blind Signature Scheme with Batch Verifications. MUE'2007. pp.1051-1056. (EI)
61. Chengyu Hu, Pengtao Liu, Daxing Li. A New Type of Proxy Ring Signature Scheme with Revocable Anonymity and No Info Leaked. MCAM'2007. pp.262-266. (EI)
62. Xiaodong Liu, Quan Miao, Daxing Li, A Biometric Identity Based Signature Scheme with Convenient Verification, FGCN (1)’2007. pp.114-117. (EI)
63. Jia Yu, Fanyu Kong, Rong Hao, Publicly Verifiable Secret Sharing with Enrollment Ability. SNPD (3) 2007,

pp.194-199. (EI)

64. 刘晓东，蒋亚丽，李大兴，两种基于生物特征信息的身份签名方案，山东大学学报(理学版), 2007 年 12 期.
65. 王艳，于佳，李大兴，前向安全的基于身份代理签名方案，计算机工程与设计, 2007 年 21 期.
66. 李如鹏，于佳，李国文，李大兴，高效撤消成员的前向安全群签名方案，计算机研究与发展, 2007 年 07 期. (EI)
67. 王洪涛，李大兴，魏传瑾，更为有效的代理数字签名方案，微电子学与计算机, 2007 年 06 期.
68. 李明，秦宝东，李大兴, Koblitz 曲线密码体制中一种可抵抗边带信道攻击的标量乘算法，计算机应用, Journal of Computer Applications, 2007 年 08 期.
69. 解军成，周大水，基于 DSP 的传真数据非实时解调，计算机工程与设计, Computer Engineering and Design, 2007 年 10 期.
70. 由雪梅，李大兴，基于 PKI 的 Web 单点登录系统设计与实现，计算机工程与设计, Computer Engineering and Design, 2007 年 09 期.
71. 李国文，李大兴，一种可验证的门限 RSA 签名方案，计算机应用研究, Application Research of Computers, 2007 年 05 期.
72. 商建伟，李锋，张燕燕，一种入侵容忍的广播通讯 KDC 方案，计算机应用, Journal of Computer Applications, 2007 年 05 期.
73. Yongquan Dong, Qingzhong Li, Yuliang Shi, Research on the Architecture of Ontology-based Context-aware Appliction in Pervasive Environment. (ICPCA07)2007 2nd International Conference on Peervasive Computing and Applications, July26-27, 2007, Birmingham, UK. (EI)
74. Yongquan Dong, Qingzhong Li, Lizhen Cui. Research on the Framework Based on Web Service and Ontology for Sharing Parts Library in Virtual Enterprise. (CSCWD2007)2007 11th International Conference on Computer Supported Cooperative Work in Design. 2007.4.26~28, Melbourne, Australia. (EI)
75. Daolin Du, Qingzhong Li, Tiangang Dong, Exploring Semantic Web Services Selection Method with Effectivity in Collaborative Environment, (CSCWD2007)2007 11th International Conference on Computer Supported Cooperative Work in Design 2007.4.26~28, Melbourne, Australia. (EI)
76. Tiangang Dong, Qingzhong Li, Kangkang Zhang, Lizhen Cui. An Extended Matching Method for Semantic Web Service in Collaboration Environment, (CSCWD2007)2007 11th International Conference on Computer Supported Cooperative Work in Design, 2007.4.26~28, Melbourne, Australia. (EI)
77. Haina zhang, Xiaoyun Wang, Differential Cryptanalysis of T-function Based Stream Cipher TSC-4, ICISC 2007,

LNCS 4817, pp.227-238, 2007. (EI)

78. 张静，王海洋，崔立真，基于 Pi 演算的跨组织工作流建模研究，计算机研究与发展, 2007，第 44 卷，第 7 期, pp1243-1251. (EI)
79. Hui Li, Haiyang Wang, Xiaohuang Hong, Smart Registry, A New Mechanism for Efficient Web Service Discovery, Journal of Computatioal Information Systems, ISSN 1553-9105, Volume 3, Number 5, 2007, pp.1767-1776. (EI)
80. Guozhen Ren, Lin Zhao, Xinjun Wang, Indexing Temporal XML Using N-Dimensional Space, Journal of Computatioal Information Systems, ISSN 1553-9105, Volume 3, Number 5, 2007, pp.2083-2090. (EI)
81. 张立群，王海洋, Process oriented Dynamic Composition of WEB Services in IPVita, Journal of Computatioal Information Systems, ISSN 1553-9105, Vol. 3, Number 3, 2007, pp949-956. (EI)
82. 张立群，王海洋, An Interval_based Method to Discover Process Models From Logs,Journal of Computatioal Information Systems, ISSN 1553-9105, Vol. 3, Number 5, 2007, pp1993-2000. (EI)
83. 何伟，王海洋，林宗楷，普适计算环境中基于群组特性的业务流程管理，软件学报, 2007，第 18 卷增刊. (EI)
84. 林金娇，王海洋, A Rule-based Method for Improving Adaptability in Pervasive Systems, University Press, The Computer Journal, Oxford Journals, Oxford. (SCI)
85. Qing Yao, Lizhen Cui, Haiyang Wang, Toward Cooperative Designing of Customized Business Process in Web Service Environment, (CSCWD2007)2007 11th International Conference on Computer Supported Cooperative Work in Design, 2007 11th International Conference on Computer Supported Cooperative Work in Design. Volume I, 2007.4.26~28, Melbourne, Australia, Swinburne Press, pp258-263. (EI)
86. Hui Li, Haiyang Wang, Lizhen Cui, Automatic Composition of Web Services Composition, (CSCWD2007)2007 11th International Conference on Computer Supported Cooperative Work in Design, 2007 11th International Conference on Computer Supported Cooperative Work in Design. Volume I, 2007.4.26~28, Melbourne, Australia, Swinburne Press, pp258-263. (EI)
87. Wei He, Haiyang Wang, Lizhen Cui, A Groupware-supported Workflow Model and its Applications in Electric Power Enterprise, (CSCWD2007)2007 11th International Conference on Computer Supported Cooperative Work in Design, 2007 11th International Conference on Computer Supported Cooperative Work in Design. Volume I, 2007.4.26~28, Melbourne, Australia, Swinburne Press, pp789-794. (EI)
88. Wenjing Cui, Haiyang Wang, Qi Sui, Lizhen Cui, Towards a Trust Management Model for E-travel, (CSCWD2007)2007 11th International Conference on Computer Supported Cooperative Work in Design, 2007 11th International Conference on Computer Supported Cooperative Work in Design. Volume I, 2007.4.26~28,

Melbourne, Australia, Swinburne Press, pp870-875. (EI)

89. Yongquan Dong, Qingzhong Li, Lizhen Cui, Research on the Framework Based on Web Service and Ontology for Sharing Parts Library in Virtual Enterprise, (CSCWD2007)2007 11th International Conference on Computer Supported Cooperative Work in Design, 2007 11th International Conference on Computer Supported Cooperative Work in Design. Volume I, 2007.4.26~28, Melbourne, Australia, Swinburne Press, pp900-903. (EI)
90. Zongmin Shang, Lizhen Cui, Haiyang Wang, A Collaborative Framework for Exception Handling in Business Process Execution, (CSCWD2007)2007 11th International Conference on Computer Supported Cooperative Work in Design, 2007 11th International Conference on Computer Supported Cooperative Work in Design. Volume I, 2007.4.26~28, Melbourne, Australia, Swinburne Press, pp914-919. (EI)
91. Kun Zhang, Lizhen Cui, Haiyang Wang, Qi Sui, An Improvement of Matrix-based Clustering Method for Grouping Learners in E-Learning, (CSCWD2007)2007 11th International Conference on Computer Supported Cooperative Work in Design, 2007 11th International Conference on Computer Supported Cooperative Work in Design. Volume I,2007.4.26~28, Melbourne, Australia, Swinburne Press, pp1010-1015. (EI)
92. Yongquan Dong, Qingzhong Li, Yuliang Shi, Research on the Architecture of Ontology-based Context-aware Appliction in Pervasive Environment, (ICPCA07)2007 2nd International Conference on Peervasive Computing and Applications, July 26-27, 2007, Birmingham, UK, IEEE PRESS, pp128-132. (EI)
93. Wei He, Haiyang Wang, Zongshui Xiao, Yuliang Shi, A Groupware Supported Workflow Model and its Applications in Pervasive Computing Environments, (ICPCA07)2007 2nd International Conference on Peervasive Computing and Applications, July 26-27, 2007, Birmingham, UK, IEEE PRESS, pp143-148. (EI)
94. Jinjiao Lin, Chengxiang Song, Haiyang Wang, Yuliang Shi, An Approach to Adaptation in Pervasive Systtems, (ICPCA07)2007 2nd International Conference on Peervasive Computing and Applications, July 26-27, 2007, Birmingham, UK, IEEE PRESS, pp496-500. (EI)