2008 年度

2008 年度实验室共发表论文及著作 86 篇，其中 EI 检索 66 篇，SCI 检索 13 篇。论文及著作列表如下。

1. Guoyan Zhang, Shaohui Wang. A Certificateless Signature and Group Signature Schemes against Malicious PKG. The 22nd IEEE International Conference on Advanced Information Networking and Applications (AINA2008), pp. 334-341, 2008. (EI)
2. Guoyan Zhang, Shaohui Wang. Aggregate and Separate of Signatures in Wireless Network. The Fourth International Symposium on Frontiers in Networking with Applications (FINA2008), pp. 428-433, 2008. (EI)
3. Guoyan Zhang. A Generic Model For Proxy-Protected Proxy Cryptography. The NIST Pairing-based Cryptography Workshop, 2008.
4. Baodong Qin, Ming Li, Fanyu Kong, Cryptanalysis of a Type of CRT-Based RSA Algorithms, Journal of Computer Science and Technology, Vol. 23, No. 2, pp. 214-221, 2008. (SCI)
5. Mingqiang Wang, Xiaoyun Wang, Guangwu Xu, Lidong Han. Fast Scalar Multiplication on a Family of Supersingular Curves over F_{2^m}, The 4th International Conferences on Information Security and Cryptology, 2008. (EI)
6. Mingqiang Wang, Qin Jing. A note on a provable secure encryption scheme, ProvSec 2008, J. Shanghai Jiaotong Univ. (Sci.)13(2), pp. 655-658, 2008. (EI)
7. Mingqiang Wang, On the Sum of a Prime the Square of a Prime and the k-th Power of a Prime, Indian J. Pure and Appl. Math, 39(3), pp. 251-271, 2008. (SCI)
8. Meiqin Wang, Xiaoyun Wang, Changhui Hu, New Linear Cryptanalytic Results of Reduced-Round of CAST-128 and CAST-256, SAC 2008, LNCS 5381, pp.231–248, 2008. (EI)
9. Meiqin Wang, Differential Cryptanalysis of Reduced-Round Present, Africa Crypt 2008, LNCS 5023, pp.40-49, 2008. (EI)
10. Xianmeng Meng, Linear Equations with Small Prime and Almost Prime Solutions, Canadian Mathematical Bulletin, 51 (2008), no. 3, pp. 399-405, 2008. (SCI)
11. Xianmeng Meng (with G.S. Lü), On sums of a prime and four prime squares in short intervals, Acta Math. Sin. (Engl. Ser.) 24 (2008), pp. 1291—1302, 2008. (SCI)
12. Xianmeng Meng (with Z. Cui), On Hua's five prime squares theorem with one prime in arithmetic progressions. (Chinese) Acta Math. Sinica (Chin. Ser.) 51 (2008), no. 2, pp. 209—218, 2008
13. Hongbo Yu, Xiaoyun Wang, Nonrandomness of 39-step SHA-256, Eurocrypt 2008 rump session, 2008. (EI)
14. 刘华宁， Mean value of mixed exponential sums, Proceedings of the American Mathematical Society, 2008, 136(4): 1193-1203. (SCI)

15. 刘华宁，张文鹏，Hybrid mean value on the difference between an integer and its reverse modulo q, Arkiv for Matematik, 2008, 46: 337-347. (SCI)
16. 刘华宁，杨存典，On a problem of D. H. Lehmer and pseudorandom binary sequences, Bulletin of the Brazilian Mathematical Society, 2008, 39(3): 387-399. (SCI)
17. Baodong Qin, Ming Li, and Fanyu Kong, Cryptanalysis of a Type of CRT-Based RSA Algorithms, Journal of Computer Science and Technology (计算机科学与技术 英文版), Vol. 23, No. 2, pp.214-221, March 2008. (SCI)
18. 秦宝东，李明，孔凡玉，对 Lee-Hwang-Yang 盲签名体制的密码分析与改进，ChinaCrypt'2008.
19. Jia Yu, Fanyu Kong, Xiangguo Cheng, Rong Hao, Guowen Li, Cryptanalysis of Vo-Kim Forward Secure Signature in ICISC 2005. ProvSec 2008: 176-184. (EI)
20. Jia Yu, Fanyu Kong, Xiangguo Cheng, Rong Hao, Guowen Li, Construction of Yet Another Forward Secure Signature Scheme Using Bilinear Maps, ProvSec 2008: 83-97. (EI)
21. Jia Yu, Fanyu Kong, Rong Hao, Dexiang Zhang, Guowen Li, How to Construct Forward Secure Single-Server, Multi-Server and Threshold-Server Assisted Signature Schemes Using Bellare-Miner Scheme. JCM 3(7): 28-35 (2008). (EI)
22. Jia Yu, Fanyu Kong, Rong Hao, Xuliang Li, Guowen Li, Publicly Verifiable Secret Sharing Member-join Protocol For Threshold Signatures. JCM 3(7): 36-43, (2008). (EI)
23. Jia Yu, Fanyu Kong, Rong Hao, Zhen Cheng, A Publicly Verifiable Dynamic Sharing Protocol for Data Secure Storage. The Ninth International Conference on Web-Age Information Management, WAIM 2008, New York: IEEE Computer Society. pp. 471-472. July 20-22, 2008. (EI)
24. Jia Yu, Fanyu Kong, Rong Hao, Xuliang Li, How to Publicly Verifiably Expand a Member without Changing Old Shares in a Secret Sharing Scheme. Pacific Asia Workshop on Intelligence and Security Informatics (PAISI 2008), ISI Workshops 2008: 138-148, LNCS 5075, Berlin: Springer-Verlag. June 17, 2008. (EI)
25. Jia Yu, Fanyu Kong, Rong Hao, Xuliang Li, Server-Assisted Forward-Secure Threshold Signature. Wuhan University Journal of Natural Sciences. July, 2008. 421-424. (EI)
26. 刘蓬涛，胡程瑜，网格中单点登录技术的研究与方案设计，计算机工程与设计，2008 年 08 期.
27. 于佳，郝蓉，孔凡玉，李绪亮，先动的可公开验证服务器辅助秘密共享，北京邮电大学学报，2008, 31(5): 13-17. (EI)
28. Jianya Liu (with Y. Ye) Correlation of zeros of automorphic L-functions, Sci. China Ser. A, 51 (2008), 1147-1166. (SCI)
29. Jianya Liu (with E. Royer and J. Wu) On a conjeture of Montgomery-Vaughan on extreme values of automorphic L-functions at 1, Centre de Recherches Mathematiques, CRM Proceedings and Lecture Notes, 46 (2008). (SCI)
30. Zhongmin Yan, Qingzhong Li, Yongquan Dong, Yanhui Ding. An Ontology-Based Integration of Web Query Interfaces for House Search (ICIA2008)The IEEE International Conference on Information and Automation June 20 -23, 2008, Zhangjiajie, China 2008. (EI)

31. Lanju Kong and Qingzhong Li. An Investigative Approach on Improving Self Service Capablities Using XML (ICNC2008)Fourth International Conference on Natural Computation Jinan,Shandong,China.18-20 October 2008 2008. (EI)
32. Peng Pan，Qingzhong Li，Yuqing Sun，Zhiyong Chen,Zhongmin Yan,Yongquan Dong Top-K Query Answering for Probabilistic Data Integration Systems in Pervasive Computing Environment (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications October 06-08,2008,Alexandria,Egypt 2008. (EI)
33. 董永权，李庆忠，闫中敏，潘鹏，User Interest Learning in Pervasive Computing Environment. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications October 06-08,2008,Alexandria,Egypt 2008. (EI)
34. Zhongmin Yan, Qingzhong Li, Yongquan Dong, Luhui Cao, Peng Pan, A Deep Web Data Integration Model for Pervasive Computing (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications October 06-08,2008,Alexandria,Egypt 2008. (EI)
35. Guanshi Lv. X.M. Meng. On sums of a prime and four prime squares in short intervals, Acta Math.Sin. (Engl.Ser.), 24(2008), 1291-1302. (SCI)
36. Guanshi Lv, On sums of a prime and four squares of primes in short intervals, Journal of Number theory, 128(2008), 805-819. (SCI)
37. Peng Pan, Qizhong Li, YuQing Sun, Rank Queries in Probabilistic Data Integration Systems for Digital Library Federation (ITME2008)2008 IEEE International Symposium on IT in Medicine and Education December 12-14, Xiamen, China 2008. (EI)
38. Shenhua Li, Chunyan Song, Improved Impossible Differential Cryptanalysis of ARIA. Proceedings of the 2008 International Conference on Information Security and Assurance (ISA 2008), 2008/4/24. (EI)
39. Zhang HaiNa, Lin, Li, Wang XiaoYun, Fast correlation attack on stream cipher ABC v3. SCIENCE IN CHINA SERIES F: INFORMATION SCIENCES, 51(7), pp 936-947, 2008/7. (SCI)
40. Lijiang Zhang, Puwen Wei, Cryptanalysis and Improvement on a Remote User Authentication Scheme Using Bilinear Pairings. International Conference on Convergence and Hybrid Information Technology, pp. 257-261, 2008. (EI)
41. Lijiang Zhang, Puwen Wei, A Modified Remote User Authentication and Key Agreement Scheme Using Smart Cards, ISECS International Colloquium on Computing, Communication, Control, and Management, vol. 1, pp. 419-423, 2008. (EI)
42. 王高丽，王美琴，缩减 RIPEMD-128 分析，软件学报，19(9), pp 2442-2448, 9 月 2008. (EI)
43. 李申华，郑世慧，宋春燕，流密码 Salsa20 的差分研究，计算机工程与应用，44(1), pp 5-13, 2008.
44. 王薇，王小云，对 CLEFIA 算法的饱和度分析，通信学报, 29(10), pp 88-92, 2008/10 (中国期刊网数据库). (EI)
45. 李申华，郑世慧，宋春燕，流密码 Salsa20 的差分研究，计算机工程与应用，44(1), pp 5-13, 2008.

46. Xu Lingling, Mingqiang Wang New id-based signatures without trusted PKG, 2008 Workshop on Knowledge Discovery and Data Mining, 2008, pp. 589 – 593, 2008. (EI)
47. Xiaodong Liu, Yuegong Zhang: Performance Improvement of SOK Key Distribution Scheme. FGCN (1), 2008, pp. 419-422. (EI)
48. Yongquan Dong, Qingzhong Li, Zongmin Shang, Building Web Domain Data Integration System with User Collaboration (CSCWD2008)2008 12th International Conference on Computer Supported Cooperative Work in Design 2008.4.16-18, 西安交通大学. 2008. (EI)
49. Yongquan Dong, Qingzhong Li, Zhongmin Yan, Yanhui Ding. A Generic Web News Extraction Approach (ICIA2008)The IEEE International Conference on Information and Automation June 20 -23, 2008, Zhangjiajie, China. 2008. (EI)
50. 董永权，李庆忠，闫中敏，潘鹏，User Interest Learning in Pervasive Computing Environment. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications October 06-08, 2008, Alexandria,Egypt 2008. (EI)
51. Zhongmin Yan, Qingzhong Li, Yongquan Dong Luhui Cao, Peng Pan. A Deep Web Data Integration Model for Pervasive Computing (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications October 06-08, 2008, Alexandria, Egypt 2008. (EI)
52. Lihong Wang, Qingzhong Li, Li Deng. A Method for Web Data Collection for Pervasive Computing. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications October 06-08, 2008, Alexandria, Egypt 2008. (EI)
53. Na Zhao, Qingzhong Li, Zhongmin Yan. An Increment-Based Random Walk Approach to Sampling Hidden Databases (CSSE2008)2008 International Conference on Computer Science and Software Engineering 12-14 December 2008, Wuhan, Hubei, China 2008. (EI)
54. Shi Bin, Wang Haiyang, Cui Lizhen, Shi Yuliang. Service composition algorithm using semantic constraint to implement user personality. (WISA2008)第五届全国 Web 信息系统及其应用学术会议, Journal of Southeast University (English Edition) Vol.24, No. 3, 东南大学, 365-368, 2008.9. (EI)
55. Liu Jia, Wang Haiyang, Cui Lizhen,Shi Yuliang. Method and supporting framework for business domain-oriented web service discovery. (WISA2008)第五届全国 Web 信息系统及其应用学术会议, Journal of Southeast University (English Edition) Vol.24, No. 3, 3 东南大学, 369-371, 2008.9. (EI)
56. Yan Zhongmin, Li Qingzhong, Cao Luhui, Kong Lanju, Dong Yongquan, Ding Yanhui. Ontology-based schema matching method in web query interface integration. (WISA2008)第五届全国 Web 信息系统及其应用学术会议, Journal of Southeast University (English Edition)Vol.24, No. 3, 东南大学, 385-388, 2008.9. (EI)
57. Zongmin Shang, Haiyang Wang, Liqiang Wang, Hui Li, Yongquan Dong. Running Samrt Process Based on Goals. (CSCWD2008)2008 12th International Conference on Computer Supported Cooperative Work in Design, 西安交

通大学, 427-433, 2008.4.16-18. (EI)

58. Hui Li, Haiyang Wang, Zongmin Shang, Yongquan Dong. Virtual Travel Agency Based on Web Services.(CSCWD2008)2008 12th International Conference on Computer Supported Cooperative Work in Design, 2008.4.16-18, 西安交通大学, 445-451, 2008. (EI)
59. Zhongmin Yan, Qingzhong Li, Yongquan Dong, Yanhui Ding. An Ontology-Based Integration of Web Query Interfaces for House Search.(ICIA2008)The IEEE International Conference on Information and Automation, June 20 -23, 2008, Zhangjiajie, China, 190-194, 2008. (EI)
60. Lanju Kong and Qingzhong Li. An Investigative Approach on Improving Self Service Capablities Using XML. (ICNC2008)Fourth International Conference on Natural Computation, Jinan, Shandong, China. 18-20 October 2008, 463-466, 2008. (EI)
61. Peng Pan, Qingzhong Li, Yuqing Sun, Zhiyong Chen, Zhongmin Yan, Yongquan Dong. Top-K Query Answering for Probabilistic Data Integration Systems in Pervasive Computing Environment. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications, October 06-08, 2008, Alexandria, Egypt, 274-279, 2008. (EI)
62. Feng Zhang, Xiaoguang Hong, Ji Bian. Dynamic Discovery of Incomplete Information in XML Data. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications, October 06-08, 2008, Alexandria, Egypt, 418-423, 2008. (EI)
63. Xinbao Wang, Yongqing Zheng, Chen Luo, Fang Teng. Efficient Computation of Iceberg Quotient Cube by Bounding.(ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications, October 06-08, 2008, Alexandria, Egypt, 424-428, 2008. (EI)
64. Li Deng, Xinjun Wang, Lihong Wang. Indexing Temporal XML Using Semantics-tree Index. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications, October 06-08, 2008, Alexandria, Egypt, 448-451, 2008. (EI)
65. Lei Tan, Xiaoguang Hong, Lei Gao, Hao Wu, Ji Bian. Knowledge Reduction based on Gradular Computing. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications, October 06-08, 2008, Alexandria, Egypt, 452-455, 2008. (EI)
66. Chen Luo, Yongqing Zheng, Xinbao Wang. Mining Double Association Rules on Temporal Dataset. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications, October 06-08, 2008, Alexandria, 543-545, 2008. (EI)
67. Zongmin Shang, Haiyang Wang. Exception Handling in Smart Process-based Applications in Pervasive Computing Environments. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications, October 06-08, 2008, Alexandria, 820-825, 2008. (EI)
68. Xianzhi Huang, Haiyang Wang, Lizhen Cui, Wenjing Cui. A Service-Oriented Business Rule-Based Application Platform in Pervasive Computing Environments.(ICPCA08)2008 3rd International Conference on Pervasive

Computing and Applications, October 06-08, 2008, Alexandria, 906-911, 2008. (EI)

69. Wei He, Haiyang Wang, Lizhen Cui. A True Decentralized Framework for Smart-flow Applications in Pervasive Computing Environments.(ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications, October 06-08, 2008, Alexandria, 927-932, 2008. (EI)
70. Hao Wu, Ming Sun, Ji Bian, Lei Tan. Context-awareness Based Task Deployment and Migration Model in Pervasive Environment. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications, October 06-08, 2008, Alexandria, 985-989, 2008. (EI)
71. Zhi-yong Chen, Hai-yang Wang, Peng Pan. A Framework for QoS-aware Web Service Composition in Pervasive Computing Environments. (ICPCA08)2008 3rd International Conference on Pervasive Computing and Applications, October 06-08, 2008, Alexandria, 1011-1016, 2008. (EI)
72. Lei Zhang, Xiao-guang Hong. Dynamic On-Line Updating Solution for CURE Cubes. (FSKD2008)Fifth International Conference on Fuzzy Systems and Knowledge Discovery, Jinan, Shandong, China. 18-20 October 2008, 396-400, 2008. (EI)
73. Shuai Li, Xin-Jun Wang, Ying Zhang. X-SPA: Spatial Characteristic PSO Clustering Algorithm with Efficient Estimation of the Number of Cluster. (FSKD2008)Fifth International Conference on Fuzzy Systems and Knowledge Discovery, Jinan, Shandong, China. 18-20 October 2008, 533-537, 2008. (EI)
74. Lei Zhang, Xiao-guang Hong, Bao Liang. N-Divided Travel Algorithm for SLCA Problem. (ICICIC 2008)Third International Conference on Innovative Computing, Information and Control, June 18-20, 2008, 大连, p 4603498, 2008. (EI)
75. Liqun Zhang, Haiyang Wang. A block-structured mining approach from audit logs. (ICICIC 2008)Third International Conference on Innovative Computing, Information and Control, June 18-20, 2008, 大连, p 4603267, 2008.(EI)
76. Bao Liang, Xiaoguang Hong, Lei Zhang, Shuai Li. Extended MRI-Cube Algorithm for Mining Multi-Relational Patterns. (ICYCS2008)The 9th International Conference for Young Computer Scientists, Hunan, China - November 18-21, 2008, 1133-1136, 2008. (EI)
77. Wen Huo, Xiaoguang Hong. A Heuristic Knowledge Reduction Algorithm Based on Partition Subdivision and Consistent Degree. IFIP International Federation for Information Processing, Springer Boston, 109-117, 2008.
78. Qing Yao, Jing Zhang, Haiyang Wang. Business Process-Oriented Software Architecture for supporting business process change. (ISECS2008)The International Symposium on Electronic Commerce and Security, Aug 3-5 2008, Guangzhou, China, 690-694, 2008. (EI)
79. GAO Dandan, WANG Xinjun, ZHANG Lihua. Reducing redundancy in XML Keyword Search by Indirect-SLCA. (ITME2008)2008 IEEE International Symposium on IT in Medicine and Education, December 12-14, Xiamen, China, 174-177, 2008. (EI)
80. HUANG Xianzhi, WANG Haiyang, CUI Lizhen. Design of User-Oriented Meta Service-Based Repository for E-Health

Service. (ITME2008)2008 IEEE International Symposium on IT in Medicine and Education, December 12-14, Xiamen, China, 405-408, 2008. (EI)

81. Fei Li, Xiaoguang Hong. A Bitmap Indexing Scheme for Temporal Access Control to XML Documents. (ITME2008)2008 IEEE International Symposium on IT in Medicine and Education, December 12-14, Xiamen, China, 1062-1066, 2008. (EI)
82. Naihui Zheng, Xiaoguang Hong, Ting Gao. Minimization of PTQ under XSCs. (ITME2008)2008 IEEE International Symposium on IT in Medicine and Education, December 12-14, Xiamen, China, 1053-1057, 2008. (EI)
83. Peng Pan, Qizhong Li, YuQing Sun. Rank Queries in Probabilistic Data Integration Systems for Digital Library Federation. (ITME2008)2008 IEEE International Symposium on IT in Medicine and Education, December 12-14, Xiamen, China, 336-342, 2008. (EI)
84. Dandan Gao, Xinjun Wang, Li Deng. Indexing Temporal XML Using Interval-Tree index. (CSSE2008)2008 International Conference on Computer Science and Software Engineering, 12-14 December 2008, Wuhan, Hubei, China, 689-691, 2008. (EI)
85. Na Zhao, Qingzhong Li, Zhongmin Yan. An Increment-Based Random Walk Approach to Sampling Hidden Databases.(CSSE2008)2008 International Conference on Computer Science and Software Engineering,12-14 December 2008,Wuhan,Hubei,China,496-499,2008. (EI)
86. Meng Qingyuan, Wang Haiyang, Xu Chunyang. A New Model for Maintaining Distributed Data Consistence.(CSSE2008)2008 International Conference on Computer Science and Software Engineering, 12-14 December 2008, Wuhan, Hubei, China, 343-346, 2008. (EI)