2010 年度

2010 年度实验室共发表论文及著作 87 篇，其中 EI 检索 46 篇，SCI 检索 17 篇。论文及著作列表如下。

1. Guoyan Zhang, Practical One Time Proxy Signature Scheme, The Sixth International Symposium on Frontiers in Networking with Applications (FINA2010), 2010. (EI)
2. Guoyan Zhang, Certificateless Encryption Scheme With Non-Black-Box Technology, The 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp.454-459, 2010. (EI)
3. Fanyu Kong, Jia Yu, Two efficient algorithms against power attacks for elliptic curve cryptosystems, ICSPS 2010, Volume 2, pp.V2-148-V2-152, IEEE Computer Society, 2010. (EI)
4. Mingqiang Wang, Haifeng Zhang, A new method of constructing a lattice basis and its applications to cryptanalyse short exponent RSA, Mathematical problems in engineering, pp.1-11, 2010. (SCI)
5. Mingqiang Wang, Cai Jie, Constructing pairing friendly curves with small , PACIIA 2010, pp.130-133, 2010. (EI)
6. Meiqin WANG, Xiaoyun WANG, Kam Pui CHOW, Lucas Chi Kwong HUI, New Differential Cryptanalytic Results for Reduced-Round CAST-128, Journal of IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, pp.2744-2754, 2010. (EI)
7. Meiqin Wang, Xiaoyun Wang, Hui Lucas C.K, Differential-Algebraic Cryptanalysis of Reduced-Round of Serpent-256, SCIENCE IN CHINA SERIES F-INFORMATION SCIENCES, pp.546-556, 2010. (SCI)
8. Xianmeng Meng, Cryptanalysis of RSA with Small Prime Combination, ICISC 2010. (EI)
9. Xianmeng Meng (with Q. Cheng, C. Sun and J.Z. Chen), Bounding the Sum of Square Roots via Lattice Reduction, Mathematics of Computation, vol. 79, no. 270, pp.1109-1122. 2010. (SCI)
10. Alex Dent and Yuliang Zheng, Practical Signcryption, a volume in Information Security and Cryptography, Springer-Verlag, Berlin, November 2010. (ISBN: 978-3-540-89409-4)
11. Hongbo Yu, Xiaoyun Wang, Cryptanalysis of the Compression Function of SIMD , http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/Aug2010/documents/Program_SHA3_Aug2010.pdf, 2010. (EI)
12. Fanyu Kong, Jia Yu, Security analysis of a provably secure identity-based signature scheme using bilinear parings, The 2nd International Conference on Industrial and Information Systems 2010 - IIS 2010, Volume 2, Page(s): 160-163, Digital Object Identifier: 10.1109/INDUSIS.2010.5565652, IEEE Computer Society, July 2010.

(EI)

13. Fanyu Kong, Jia Yu, Key Substitution Attack on an Improved Short Signature Scheme without Random Oracles, The Second Asia-Pacific Conference on Information Processing 2010 - APCIP 2010, Page(s): 288 – 291, IEEE, September 2010. (EI)
14. Fanyu Kong, Jia Yu, Key Substitution Attacks on Two Short Signature Schemes from Bilinear Pairings, The 4th International Conference on Intelligent Information Technology Application - IITA 2010, Volume 3, Page(s): 262-264, IEEE, November 2010. (EI)
15. 于佳，孔凡玉，程相国，郝蓉，Guo Xiangfa，可证安全的入侵容忍签名方案，软件学报，2010, 21(9): 2352-2366. (EI)
16. 于佳，孔凡玉，郝蓉，李大兴，一个基于双线性映射的前向安全门限签名方案的标注，计算机研究与发展，2010, 47(4): 605-612. (EI)
17. Jia Yu, Rong Hao, Fanyu Kong, Xiangguo Cheng, Huawei Zhao, Yangkui Chen, Cryptanalysis of a Type of Forward Secure Signatures and Multi-signatures, International Journal of Computers and Applications, ACTA Press, Vol. 32, No. 4, 2010. (EI)
18. Jia Yu, Fanyu Kong, Xiangguo Cheng, Rong Hao, Yangkui Chen, Guowen Li, Forward-Secure Multisignature, Threshold Signature and Blind Signature Schemes, Journal of Networks. Academy Publisher, Volume 5, issue 6, 2010, pp.634-641. (EI).
19. Jia Yu, Rong Hao, Fanyu Kong, Xiangguo Cheng, Huawei Zhao, Yangkui Chen, Identity-Based Forward Secure Threshold Signature Scheme Based on Mediated RSA, International Journal of Computers and Applications, ACTA Press, Vol. 32, No. 4, 2010. (EI)
20. Jianya Liu, Enlarged Major Arcs in Additive Problems, Mathematical Notes, 88 (2010), pp.395-401. (SCI)
21. Jianya Liu, Integral points on quadrics with prime coordinates, Monatshefte für Mathematik DOI: 10.1007/s00605-010-0253-5. (SCI)
22. Jianya Liu (with P. Sarnak), Integral points on quadrics in three variables whose coordinates have few prime factors, Israel J. of math., 178 (2010), 393–426. (SCI)
23. Jianya Liu (with Lau Yuk-Kam and Wu Jie), Coefficients of symmetric square L-functions, Sci. China Math, 2010, 53, doi: 10.1007/s11425-010-4046-z.[54]
24. Jianya Liu (with J. Brudern, R. Dietmann and T. D. Wooley), A Birch–Goldbach theorem, Arch. Math. 94 (2010), 53–58. (SCI)
25. 孔兰菊，李庆忠，史玉良，王学，面向 saas 应用基于键值对模式的多租户索引研究，计算机学报 T

2010，第 33 卷 第 12 期，2010。（EI）

26. 闫中敏，李庆忠，彭朝晖，董永权，丁艳辉，张永新，徐秀星，DWDIS：面向分析的 Deep Web 数据集成系统，计算机研究与发展增刊 2010，第 47 卷 增刊Ⅰ，2010 年 10 月。
27. 史玉良，栾帅，李庆忠，董晋利，刘方方，基于 TLA 的 SaaS 业务流程定制及验证机制研究，计算机学报 2010，第 37 卷 第 11 期 2010。（EI）
28. 史玉良，栾帅，李庆忠，董晋利，基于 TLA 的 SaaS 业务流程定制及验证机制研究（CCF NCSC 2010）第一届全国服务计算学术会议，2010 年 8 月 10-11 日，中国.哈尔滨 2010。（EI）
29. KONG Lanju, LI Qingzhong, ZHENG Xuxu, CHEN Weiliang, A Metadata-driven Platform for Delivery of SaaS Application (FCC 2010) 2010 Second International Conference on Future Computer and Communication Shanghai, China, September 28-29, 2010. (EI)
30. Lanju Kong, Qingzhong Li, Xuxu Zheng, A Novel Model Supporting Customization Sharing in SaaS Applications (MINES 2010) 2010 International Conference on Multimedia Information Networking and Security Nanjing, Jiangsu, China.4-6 November 2010 2010. (EI)
31. 闫中敏，李庆忠，张世栋，彭朝晖，董永权，丁艳辉，张永新，徐秀星，MI-WDIS: Web Data Integration System for Market Intelligence, (CIKM2010) The 19th International Conference on Information & Knowledge Management and Co-Located Workshops Canada, Toronto, Ontario, October-26-30, 2010 2010. (EI)
32. Yuliang Shi, Kun Zhang, and Qingzhong Li, A New Data Integrity Verification Mechanism for SaaS (WISM2010) 2010. (EI)
33. Xiumin ren, Y.B. Ye. Resonance between automorphic forms and exponential functions, Science China Mathematics 2010, (9) 53, 2463-2472. (SCI)
34. Guanshi Lv, Z.X. Liu, Eight cubes of primes and powers of 2, Acta Arith. , 145(2010), 171-192. (SCI)
35. Guanshi Lv, Y. H. Wang, Note on the number of integral ideals in Galois extensions, Science China: Mathematics, 53(2010), 2417-2424. (SCI)
36. Guanshi Lv, H.G. Xia, Note on divisor function for quaternion algebras, Journal of number theory, 130(2010), 2147-2156. (SCI)
37. Guanshi Lv, On a divisor problem related to the Epstein zeta-function, Bulletin of the London Mathematical Society, 42(2010), 267-274. (SCI)
38. Guanshi Lv, H.C. Tang, On some results of Hua in short intervals, Lithuanian Mathematical Journal, 50(2010), 54-70. (SCI)

39. Guanshi Lv, H.W. Sun, On fractional power moments of L-functions associated to certain cusp forms, Acta Appl Math., 109(2010), 653-667. (SCI)
40. Lidong Han, Xiaoyun Wang, Gusangwu Xu, On an Attack on RSA with Small CRT-Exponents, Science China Information Sciences,vol.53, No.8, 2010.8. (SCI)
41. Jiazhe Chen, Keting Jia, Improved Related-Key Boomerang Attacks on Round-Reduced Threefish-512, ISPEC 2010, pp.1-18. (EI)
42. Jingguo Bi, Xianmeng Meng, Lidong Han, Cryptanalysis of two knapsack-type public-key cryptosystems, ICCASM 2010, pp.623-626. (EI)
43. 韩立东，刘明洁，毕经国，两种背包型公钥密码算法的安全性分析，电子与信息学报，pp.1485-1488. (EI)
44. Keting Jia, Yvo Desmedt, Lidong Han, Xiaoyun Wang, Practical Pseudo-Cryptanalysis of Luffa. Inscrypt 2010. (EI)
45. 贾珂婷，改进的 44 轮 SHACAL-2 的相关密钥攻击，山东大学学报(理学版)，45(4):12-16.
46. 乔思远，贾珂婷, SHA-0-MAC 的部分密钥恢复攻击,山大学报（理学版），2010 年，第 45 卷第 4 期，第 6-11 页
47. 杨林，王美琴，约减轮的 MIBS 算法的差分分析，山东大学学报（理学版），第 45 卷第 4 期 7-11 页。
48. Shunhua Zhang, Goldbach Conjecture and the Least Prime Number in an Arithmetic Progression, Comptes Rendus Mathematique, Acadmemie des Sciences, Paris 348 (2010). (SCI)
49. Shunhua Zhang, On fixed points of order k of RSA, Journal of Mathematics, 30(3), 551-553, 2010.
50. Chenghang Du, Jiazhe Chen, Impossible Differential Cryptanalysis of ARIA Reduced to 7 Rounds, CANS 2010, LNCS 6467, Springer, Heidelberg, 2010, pp.20-30. (EI)
51. Chenghang Du, Jiazhe Chen, Novel Impossible Differential Cryptanalysis of ARIA. ISAI 2010, IEEE, 2010, vol. 3, pp.63-67.
52. Chenghang Du, Jiazhe Chen, Improved Meet-in-the-Middle Attacks on ARIA. ISAI 2010, IEEE, 2010, vol. 3, pp.306-310.
53. Yue Sun, Meiqin Wang, Zhenli Dai, Breaking the Block Cipher PUFFIN for RFID Tags, 2010 International Conference on Information Security and Artificial Intelligence (ISAI 2010), pp.196-201.
54. Yue Sun, Meiqin Wang, Zhenli Dai, Breaking the Block Cipher PUFFIN for RFID Tags, The 6th Workshop on RFID Security, Poster Papers, 2010.
55. An Wang, Zheng Li, Xianwen Yang, Research on a New Security Problem of USB: Monitoring Cable Attack,

Countermeasures, and Applications, 3rd International Conference on Computer and Electrical Engineering(ICCEE 2010), vol. 4, pp.110-114.

56. An Wang, Maoning Wang, Zheng Li, Xianwen Yang, Improved Alternatives of Barrel Shifter Used in Reconfigurable Design of Block Cipher Algorithms, 2010 International Conference on Future Information Technology (ICFIT 2010), vol. 1, pp.63-66.
57. An Wang, Zheng Li, Xianwen Yang, Yanyan Yu, Maoning Wang, A Practical Key Management Scheme in Software Layer and Its Applications, 2010 International Conference on Management Science and Information Engineering (ICMSIE 2010), vol. 3, pp.72-75.
58. He Shang, Mingqiang Wang, Some New Optimal Pairings. 2010 International Conference on Computational Intelligence and Security, cis, pp.390-393. (2010) (EI)
59. Yali Jiang, Xiuling Ju, Feng Shi, New Lattice-Based Public-Key Cryptosystem, IITSI 2010, pp.387-389. (EI)
60. 丁艳辉，李庆忠，董永权，彭朝晖. 基于集成学习和二维关联边条件随机场的 Web 数据语义标注方法，计算机学报 T 2010, Vol.33 No.2 2010. (EI)
61. Qingzhong Li, Yanhui Ding, An Feng, Yongquan Dong, A Novel Method for Extracting Information from Web Pages with Multiple Presentation Templates, Journal Of Software 2010,Volume5 Number5 2010. (EI)
62. 董永权，李庆忠，丁艳辉，彭朝晖，A Query Interface Matching Approach Based on Extended Evidence Theory for Deep Web, JOURNAL OF COMPUTER SCIENCE & TECHNOLOGY（计算机科学技术学报英文版 JCST）T 2010,Vol.25 No.3 2010. (EI)
63. Yan-hui Ding, Qing-zhong Li, Yongquan Dong, Zhao-hui Peng. 2D Correlative-Chain Conditional Random Fields for Semantic Annotation of Web Objects JOURNAL OF COMPUTER SCIENCE & TECHNOLOGY（计算机科学技术学报英文版 JCST）2010, Vol.25 No.4 2010 EI
64. 张坤，李庆忠，史玉良，面向 SaaS 应用的数据组合隐私保护机制研究，计算机学报，2010，第 37 卷第 11 期 2010. (EI)
65. Yongquan Dong, Qingzhong Li, Yongqing Zheng, Xiaoyang Xu, Yongxin Zhang. Semantic Annotation of Web Objects Using Constrained Conditional Random Fields (WAIM 2010)The 11th International Conference on Web-Age Information Management July 15-17, Sichuan, China 2010. (EI)
66. Zheng Xuxu, Li Qingzhong, Kong Lanju. A Data Storage Architecture Supporting Multi-Level Customization for SaaS, (WISA 2010) 2010 Seventh Web Information Systems and Applications Conference Hohhot, China, 20-22 August 2010 2010. (EI)
67. Xiuxing Xu, Qingzhong Li, Yongquan Dong, Yanhui Ding. Dynamically Constructing a Global Schema for Web

Entities (WISA 2010) 2010 Seventh Web Information Systems and Applications Conference Hohhot, China, 20-22 August 2010 2010. (EI)

68. Huitao Dou, Qingzhong Li, Yongxin Zhang. Find Answers from Web Search Results (WISA 2010) 2010 Seventh Web Information Systems and Applications Conference Hohhot, China, 20-22 August 2010 2010. (EI)
69. Yang Bo, Zheng Yongqing, The improved on-line analysis mining for multi-dimension data based on association rules, CAR 2010. (EI)
70. Xiujuan Zhang, Guoqing Dong, A New Architecture of Online Trading Platform Based on Cloud Computing, APWCS2010. (EI)
71. Niu Na, Dong Guoqing, A New Labeling Scheme for XML Trees Based on Mesh Partition, The 2010 International Conference on Future Computer and Communication. (EI)
72. Jinli Dong, Shidong Zhang, Yong Shi, Xiaoyang Xu, Wenjuan Guo, Process Customization Based on Dependent Topology in Software as a Service Model, SEDM 2010. (EI)
73. Chen Weiliang, Zhang Shidong, Kong Lanju, A Multiple Sparse Tables Approach for Multi-tenant Data Storage in SaaS, IIS2010. (EI)
74. Zhongyan Liu, Xiaoguang Hong, Ye Hu, XML-twig Approximate Matching Twig Join Algorithm Based on DTD, IIS2010. (EI)
75. Jing Li, Xinjun Wang, Zhaohui Peng, A Preprocessing Technique for Keyword-Driven Analytical Processing, DCABES 2010. (EI)
76. Hu Ye, Liu Weihua, Hong Xiaoguang, TwigFilter, An Efficient Holistic Approach of XML Twig Pattern Matching, WISA 2010.(EI)
77. Yuanhui Sun, Zongshui Xiao, Dongmei Bao, Jie Zhao, An Architecture Model of Management and Monitoring on Cloud Services Resources, ICACTE 2010. (EI)
78. Dongmei Bao, Zongshui Xiao, Yuanhui Sun, Jie Zhao, A Method and Framework for Quality of Cloud Services Measurement, ICACTE 2010. (EI)
79. Song Ran, Hong Xiaoguang, Yang Shanyong, A New Twig Query Evaluation for XML Based on Region Encoding, BMEI 2010.
80. Wu Shengqi, Zhang Shidong, Kong Lanju, A Dynamic Data Storage Architecture for SaaS, MINES 2010. (EI)
81. Yang Shan-yong, Wang Xin-jun, Song Ran, Peng Zhao-hui, XML Keyword Query Algorithm On SLCA, ICCEE 2010.
82. Xin Du, Yongqing Zheng, Zhongmin Yan, Automate Discovery of Deep Web Interfaces, ICISE2010.

83. Jie Zhao, Zongshui Xiao, Dongmei Bao, Communication Framework of Main Station and Protocol Parsing Model for Electricity Information Acquisition, ICISE2010.
84. Guangyao Li, Xinjun Wang, Zhaohui Peng, Keyword Query Preprocessing, ICCEE 2010.
85. Ping Zhang, Guoqing Dong, A New Labeling Scheme using Vectors Based on Polar coordinate system for Dynamic XML Data, PACCS 2010. (EI)
86. Wei He, Haiyang Wang, Business process management in pervasive environments, WIRELESS COMMUNICATIONS AND MOBILE COMPUTING. (SCI)
87. 周智增，王新军，XML 概率数据库中空值处理方法研究，计算机科学，ISSN 1002-137X CN50-1075/TP