2012 年度

2012 年度实验室共发表论文及著作 71 篇，其中 EI 检索 51 篇，SCI 检索 15 篇。论文及著作列表如下。

1. Liantao Bai, Yuegong Zhang, Guoqiang Yang, SM2 Cryptographic Algorithm Based On Discrete Logarithm Problem And Prospect, The 2nd International Conference on Consumer Electronic, Communications and Networks (CECNet 2012), pp. 837-840, 2012. (EI)
2. Jingguo Bi, Mingjie Liu and Xiaoyun Wang, Cryptanalysis of a Homomorphic Encryption Scheme From ISIT 2008. ISIT2012, pp.2152-2156, 2012. (EI)
3. Jingguo Bi,Qi Cheng, Lower Bounds of Shortest Vector Lengths in Random NTRU Lattices. TAMC 2012: 143-155. 2012 (EI)
4. Andrey Bogdanov,Gregor Leander,Kaisa Nyberg, Meiqin Wang, Integral and Multidimensional Linear Distinguishers with Correlation Zero, ASIACRYPT 2012, LNCS 7658, PP.244-261, 2012. (EI)
5. Andrey Bogdanov, Meiqin Wang, Zero Correlation Linear Cryptanalysis with Reduced Data Complexity, FSE 2012, LNCS 7549, pp.29-48, 2012. (EI)
6. Jiazhe Chen, Meiqin Wang, Bart Preneel, Impossible Differential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT, AFRICACRYPT 2012,LNCS 7374, pp .117-137, 2012. (EI)
7. Jiazhe Chen, Leibo Li, Low Data Complexity Attack on Reduced Camellia-256. ACISP 2012: 101-114. (EI)
8. Cui Lizhen, Xu Meng, A Qos-Aware Hyper-Graph Based Method of Semantic Service Composition, IWEI 2012, pp.81-91. (EI)
9. Lizhen Cui, Jian Li, Yongqing Zheng, A Dynamic Web Service Composition Method Based on Viterbi Algorithm, ICWS2012, pp.267-271. (EI)
10. Qiuyan Huang, Qingzhong Li, Hong Li, Zhongmin Yan, An Approach to Incremental Deep Web Crawling Based on Incremental Harvest Model, Procedia Engineering, Volume 29(part 2), 2012.2, pp.1081-1087. (EI)
11. Qiuyan Huang, Qingzhong Li, Zhongmin Yan, A Novel URL Assignment Model Based on Multi-objective Decision Making Method, WISA 2012, pp.31-34. (EI)
12. Keting Jia, Leibo Li, Christian Rechberger, Jiazhe Chen, Xiaoyun Wang, Improved Cryptanalysis of the Block Cipher KASUMI, SAC 2012, LNCS 7707, pp.222–233, 2012. (EI)

13. Fuzeng Jiao, Guoqing Dong, Qiuyan Li, Jiezhu, OpinMiner, Extracting Feature-Opinion Pairs with Dependency Grammar from Chinese Product Reviews, WISA 2012, pp.217-222. (EI)
14. Lin Li, Qingzhong Li, Yuliang Shi and Kun Zhang, SAPS:A Single Attribute Protection Scheme for SaaS, INFORMATION, Volume 15 Number 1, 2012.1, pp.275-282. (SCI)
15. Jinchai Li, Shidong Zhang, Zhengzheng Liu, Lanju Kong, A Data Rights Control Model for a SaaS Application Delivery Platform*, (AISC)ADVANCES IN INTELLIGENT AND SOFT COMPUTING, AISC146, 2012.3, pp. 139-146. (EI)
16. Chao-Feng Liu, Xiao-Guang Hong, Zhao-Hui Peng, Bo Han, An Entity-Based Method for XML Keyword Search, ACAI2012,pp.3292-3296. (EI)
17. Donglan Liu, Xinjun Wang, Hong Li, Zhongmin Yan, Robust Web Extraction Based on Minimum Cost Script Edit Model, Procedia Engineering, Volume 29(part 2), 2012.2 pp.1119-1125. (EI)
18. Donglan Liu, Xinjun Wang, Zhongmin Yan, Qiuyan Li, Robust Web Data Extraction: A Novel Approach Based on Minimum Cost Script Edit Model, WISM 2012, pp.497-509. (EI)
19. Liu Jianya (with Lau Yuk-Kam and Wu Jie), The first negative coefficients of symmetric square L-functions, Ramanujan J (2012) 27:pp.419–441. (SCI)
20. Liu Jianya, Enlarged Major Arcs in Additive Problems. II, Proceedings of the Steklov Institute of Mathematics, 2012, Vol. 276, pp.176–192.
21. Liu Jianya, Integral points on quadrics with prime coordinates, Monatshefte fur Mathematik, 164(4),pp.439-465, 2011/12. (SCI)
22. Liu Jianya, Qu, Yan, Wu, Jie, Two Linnik-type problems for automorphic L-functions，Mathematical Proceedings of the Cambridge Philosophical Society, Volum 151, pp 219-227, 2011.9. (SCI)
23. Kui Liu and Xiumin Ren, On exponential sums involving Fourier coefficients of cusp forms, Journal of Number Theory, 32(1) (2012) pp.171–181 . (SCI)
24. Ya Liu, Leibo Li, Dawu Gu, Xiaoyun Wang, Zhiqiang Liu, Jiazhe Chen, Wei Li, New Observations on Impossible Differential Cryptanalysis of Reduced-Round Camellia, FSE 2012, LNCS 7549, pp.90–109, 2012. (EI)
25. Xue Liu, Dashui Zhou, Escrow mechanism and monitoring to achieve on IBE, The 3rd International Conference on E-Business and E-Government(ICEE 2012), May-12. (EI)
26. Bingcai Lv, Shidong Zhang, Zhengzheng Liu, Lanju Kong, WFFS: A SaaS-Based Multi-tenant Workflow Engine*, (AISC)ADVANCES IN INTELLIGENT AND SOFT COMPUTING, AISC146,2012.3

pp.77-83. (EI)

27. Guangshi Lv, Jie Wu, Wenguang Zhai, On a divisor problem related to the Epstein zeta-function IV, Acta Arithmetica, 154.3(2012), pp.307-324. (SCI)
28. Guangshi Lv, On general divisor problems involving Hecke eigenvalues, Acta Math. Hungar., 135 (1–2) (2012), pp.148–159. (SCI)
29. Guangshi Lv, Jie Wu, and Wenguang Zhai, On a divisor problem related to the Epstein zeta-function III, Quart. J. Math., 63 (2012), pp.953–963. (SCI)
30. Quan Miao, Dongfeng Yuan, A novel USB key design with online emulation debugging functions, Advanced Manufacturing Technology, Vol.472-475, pp.1484-1487, 2012. (EI)
31. Guozhen Ren, Qingzhong Li, Yuliang Shi, Lizhen Cui, A Confidentiality-Guarantee Mechanism for SaaS, IWEI 2012, pp.71-80. (EI)
32. Chengliang Sang, Qingzhong Li, Zhengzheng Liu, Lanju Kong, VGL: Variable Granularity Lock Mechanism in the Shared Storage Multi-tenant Database, (AISC)ADVANCES IN INTELLIGENT AND SOFT COMPUTING, AISC146, 2012.3, pp.481-487. (EI)
33. Chengliang Sang, Qingzhong Li, Lanju Kong, Tenant Oriented Lock Concurrency Control in the Shared Storage Multi-tenant Database, EDOCW 2012, pp.179-189. (EI)
34. Yue Sun,Meiqin Wang,Shujia Jiang,Qiumei Sun, Differential Cryptanalysis of Reduced-Round ICEBERG, AFRICACRYPT 2012,LNCS 7374, pp.155-171, 2012. (EI)
35. Yue Sun, Meiqin Wang, Linear Cryptanalysis of Reduced-Round ICEBERG. ISPEC 2012: 381-392. (EI)
36. Ming Sun, Huitao Dou, Qingzhong Li, Zhongmin Yan,Quality Estimation of Deep Web Data Sources for Data Fusion, Procedia Engineering, Volume 29(part 4), 2012.2, pp.2347-2354. (EI)
37. Meiqin Wang, Yue Sun, Elmar Tischhauser, Bart Preneel, A Model for Structure Attacks, with Applications to PRESENT and Serpent, FSE 2012, LNCS 7549, PP.49-68, 2012. (EI)
38. Mingqiang Wang, Haiyang Xue, Tao Zhan, Fault Attacks on Hyperelliptic Curve Discrete Logarithm Problem over Finite Fields, China Communications, 2012, 9(11): 150-161. (SCI)
39. Wenyu Wang, Xinjun Wang, Bin Jiang, Jingchang Pan, Data Mining In Massive Spectral Data, INFORMATION, Volume 15 Number 6, 2012.6, pp.2357-2364. (SCI)
40. Zongquan Wang, Guoqing Dong, Jie Zhu, Dual-Kad: Kademlia-Based Query Processing Strategies for P2P Data Integration, WISA 2012, pp.155-158. (EI)
41. Puwen Wei, Xiaoyun Wang and Yuliang Zheng, Public Key Encryption for the Forgetful, Cryptography and Security: From Theory to Applications, David Naccache (Ed.), LNCS 6805,

pp.185-206, 2012. (EI)

42. Puwen Wei, Xiaoyun Wang, Yuliang Zheng, Public Key Encryption without Random Oracle Made Truly Practical (Full Version), Computers and Electrical Engineering, vol.38, no.4, pp.975-985, July 2012. (SCI)
43. Hongchen Wu, Xinjun Wang, Zhaohui Peng, Qingzhong Li, and Lin Lin, PointBurst: Towards a Trust-Relationship Framework for Improved Social Recommendations, APWeb 2012 Workshops, pp.78-88. (EI)
44. Hongchen Wu, Xinjun Wang, Zhaohui Peng, Qiuyan Li, Actively building Collaborative Filtering Recommendation in Clustered Social Data, CSCWD 2012, pp.693-697. (EI)
45. Wu Shengqi, Zhang Shidong, Kong Lanju, Schema Evolution via Multi-Version Metadata in SaaS,Procedia Engineering,Volume 29(part 2), 2012.2, pp. 1107-1112. (EI)
46. Min Song, Yuegong Zhang, An Improved Certificateless Proxy Blind Signature Scheme, 14th International Conference on Communication Technology(ICCT2012), p722-726, Nov. 2012. (EI)
47. Guoqiang Yang, Yuegong Zhang, Liantao Bai, Implementation of Digital Rights Management on the Android Mobile Terminal, The 2nd International Conference on Electric Information and Control Engineering(ICEICE 2012), pp.653-656, 2012. (EI)
48. Hongbo Yin, Shnuhua Zhang, Representation dimensions of triangular matrix algebras. Linear Algebra Appl.,438(2013), 2004-2017. (SCI)
49. Hongbo Yu, Jiazhe Chen, Xiaoyun Wang, The Boomerang Attacks on the Round-Reduced Skein-512, SAC 2012, LNCS. (EI)
50. Jia Yu, Fanyu Kong, Xiangguo Cheng, Rong Hao, Jianxi Fan, Intrusion-Resilient Identity-Based Signature: Security Definition and Construction, Journal of Systems and Software, Vol. 85, Issue 2, 2012, pp.382-391. (SCI/EI)
51. Jia Yu, Fanyu Kong, Huawei Zhao, Xiangguo Cheng, Rong Hao, Non-Interactive Forward-Secure Threshold Signature without Random Oracles, Journal of Information Science and Engineering, Vol. 28, No.3, 2012, pp. 571-586. (SCI/EI)
52. Zhang Chuanyan, Hong Xiaoguang, Peng Zhaohui, An Automatic Approach to Harvesting Temporal Knowledge of Entity Relationships, Procedia Engineering, Volume 29(part 3), 2012.2, pp.1399-1409. (EI)
53. Guoyan Zhang, A General Construction for Multi-authority Attribute-Based Encryption. AICI 2012, pp.333-340.
54. Guoyan Zhang, Lei Liu, Yang Liu, An Attribute-Based Encryption Scheme Secure against

Malicious KGC. TrustCom 2012, pp.1376-1380.

55. Guoyan Zhang, A Multi-Authority Attribute-Based Encryption System Against Malicious KGC, Advanced Engineering Forum.38-44, 2012.
56. Jing Zhang, Xiaoguang Hong, Zhaohui Peng, and Qingzhong Li, NestedCube, Towards online analytical processing on information-enhanced multidimensional network, WAIM 2012 Workshops, pp.128-139. (EI)
57. Kun Zhang, Qingzhong Li, Yuliang Shi, A Novel Non-Deterministic Data Privacy Preservation Mechanism for Software as a Service, (JDCTA)International Journal of Digital Content Technology and its Applications, Volume6, Number7, April 2012, pp.181-189. (EI)
58. La Zhang, Qingzhong Li, Yuliang Shi, Lin Li, and Wenxiao He, An Integrity Verification Scheme for Multiple Replicas in Clouds*,WISM 2012, pp.264-274. (EI)
59. Nuonuo Zhang, Dashui Zhou, Responsibility Certification System Based on Multiple Digital Signatures of EMR System, 2012 International Conference on Computer and Information Science, Safety Engineering, Jun-12. (EI)
60. Zhang Shunhua, Zhang Yuehui, Repetitive cluster-tilted algebras, Acta Mathematica Scientia, 32B(4)(2012), 1449-1454. (SCI)
61. Tiantian Zhang, Yuliang Shi, Meng Xu, Lizhen Cui, A Service Provisioning Strategy Based on SPEA2 for SaaS Applications in Cloud, CGC2012, pp.290-295. (EI)
62. Yongqing Zheng,Chengliang Sang, Xiangxu Meng, Qingzhong Li, Tenant Oriented Lock Granularity Adjustment Strategy in the Shared Storage Multi-tenant Database, (JDCTA)International Journal of Digital Content Technology and its Applications, Volume6, Number19, October 2012, pp.152-161. (EI)
63. Yongqing Zheng, Jinshan Pang, Jian Li, Lizhen Cui, Business Process Oriented Platform-as-a-Service Framework for Process Instances Intensive Applications, IPDPSW 2012, pp.2314-2321. (EI)
64. Yongqing Zheng, Yufang Bian, Xin Du, Hongchen Wu, A Deep Web Database Sampling Method Based on High Correlation Keywords, WISA 2012, pp.9-14. (EI)
65. 崔立真，谷连超，基于平台即服务模式的协同应用动态构建与执行方法，计算机集成制造系统，第 18 卷，第 8 期，2012.8，pp.1667-1674。（EI）
66. 董永权，李庆忠，丁艳辉，彭朝晖，基于约束条件随机场的 Web 数据语义标注，计算机研究与发展，49(2)，2012.2，pp.361-371。（EI）

67. 何伟，崔立真，李保栋，面向实时 ROLAP 应用的并行处理方法，计算机研究与发展，第 49 卷增刊 I ，2012.10，pp.107-113。
68. 李晓娜，李庆忠，孔兰菊，庞成，基于共享模式的 SaaS 多租户数据划分机制研究，通讯学报，第 33 卷第 Z1 期，2012.9，pp.110-120。（EI）
69. 徐猛，崔立真，李庆忠，基于扩展图规划的 Top-K 服务组合方法研究，电子学报，第 40 卷，第 7 期，2012.7，pp.1404-1409。（EI）
70. 张传岩，洪晓光，彭朝晖，李庆忠，基于 SVM 和扩展条件随机场的 Web 实体活动抽取，软件学报，第 23 卷，第 10 期，2012.10，pp.2612-2627。（EI）
71. 张永新，李庆忠，彭朝晖，基于 Markov 逻辑网的两阶段数据冲突解决方法，计算机学报，第 35 卷，第 1 期，2012.1，pp.101-111。(EI)