2014 年度

2014 年度实验室共发表论文及著作 45 篇，其中 EI 检索 28 篇，SCI 检索 13 篇。

论文及著作列表如下。

1. Liu Jianya and Wu Jie, The number of coefficients of automorphic L-functions for GLm of same signs, J. Number Theory, 148(2015), 429–450. SCI
2. Jiang Yujiao and Lü Guangshi, On the higher mean over arithmetic progressions of Fourier coefficients of cusp forms, Acta Arithmetica, 166(2014), 231-252. SCI
3. Yin Hongbo, Zhang Shunhua*, (2014): The transition matrix between PBW basis and semicanonical basis of $U^+(\mathfrak{sl}_{n}(\mathbb{C})) Science China Mathematics, 57(7) (2014), 1427-1434. （SCI）
4. Pei Genhua, Yin Hongbo, Zhang Shunhua*, (2014): Endomorphism algebras of tilting modules over m-replicated algebras, Linear. Algebra Appl., 448(2014), 292–298. （SCI）
5. Jia Yu, Fanyu Kong, Xiangguo Cheng, Rong Hao, Guowen Li, One forward-secure signature scheme using bilinear maps and its applications, Information Sciences, Vol. 279, pp. 60-76, 2014. (SCI, EI)
6. 于佳, 陈养奎, 郝蓉, 孔凡玉, 程相国, 潘振宽, 无可信中心的可公开验证多秘密共享, 计算机学报, Vol. 37 No. 5, pp. 1030-1038, 2014. (EI)
7. 孔凡玉(参与编写), GM/T 0022-2014 《IPSec VPN 技术规范》 等多项行业标准，中国标准出版社 2014.
8. Mingqiang wang, Haiyang Xue, Tao Zhan, Fault Attacks on Hyperelliptic Curve Discrete Logarithm Problem over Binary Field, Science China Information Sciences，2014, No.3. SCI
9. Puwen Wei, Yuliang Zheng and Wei Wang. Multi-recipient Encryption in Heterogeneous Setting. Information Security Practice and Experience-10th International Conference, ISPEC 2014, LNCS 8434, pp. 462-480, 2014. (EI)
10. Long Wen, Meiqin Wang, Andrey Bogdanov, Huaifeng Chen. General Application of FFT in Cryptanalysis and Improved Attack on CAST-256. Progress in Cryptology--INDOCRYPT 2014, LNCS 8885, pp. 161-176, 2014. (EI)
11. Jingyuan Zhao, Meiqin Wang, Long Wen. Improved Linear Cryptanalysis of CAST-256. Journal of Computer Science and Technology, 29(6), pp.1134-1139, 2014. (SCI)
12. Huaifeng Chen, Long Wen, Meiqin Wang. Linear Cryptanalysis on MULTI2 with FFT Technique. 密码学报, 1(4), pp. 311-320, 2014.
13. Long Wen, Meiqin Wang. Integral Zero-Correlation Distinguisher for ARX Block Cipher, with Application to SHACAL-2. Information Security and Privacy, ACISP 2014, LNCS 8544, pp. 454-461, 2014. (EI)
14. Céline Blondeau, Andrey Bogdanov, Meiqin Wang. On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers. Applied Cryptography and Network Security, ACNS 2014, LNCS 8479, pp. 271-288, 2014. (EI)
15. Long Wen, Meiqin Wang, Andrey Bogdanov, Huaifeng Chen. Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard. Information Processing Letters, 114(6), pp.322–330, 2014. (SCI)
16. Meiqin Wang, Long Wen. Research on Zero-correlation Linear Cryptanalysis. 密码学报, 1(3), pp.296-310, 2014.

17. Long Wen, Meiqin Wang, Andrey Bogdanov. Multidimensional Zero-Correlation Linear Cryptanalysis of E2. Progress in Cryptology – AFRICACRYPT 2014, LNCS 8469, pp.147-164, 2014. (EI)
18. Long Wen, Mei-Qin Wang, Jing-Yuan Zhao. Related-Key Impossible Differential Attack on Reduced-Round LBlock. Journal of Computer Science and Technology, 29(1), pp.165-176, 2014. (SCI)
19. Leibo Li, Keting Jia, Xiaoyun Wang*, Improved Single-Key Attacks on 9-Round AES-192/256, FSE 2014, LNCS 8540, 2015, pp. 1-20.
20. Wei Wei, Chengliang Tian, Xiaoyun Wang*, New Transference Theorems on Lattices Possessing nε-unique Shortest Vectors, Discrete Mathematics 315-316C (2014), pp. 144-155. (SCI)
21. Zongyue Wang, Hongbo Yu, Xiaoyun Wang, Cryptanalysis of GOST R hash function. Inf. Process. Lett. 114(12), 2014, pp. 655-662. (SCI)
22. Mingjie Liu, Xiaoyun Wang*, Guangwu Xu, Xuexin Zheng, A note on BDD problems with λ2-Gap, Inf. Process. Lett. 114(1-2), 2014, pp. 9-12. (SCI)
23. 王新军，闫实，彭朝晖，李庆忠.Extractor：支持查询重构的高效数据库关键词检索系统.电子学报第 42 卷 第 2 期.pp.209-216,2014(EI)
24. Zhu, Yumin; Li, Qingzhong; Yan, Zhongmin.Object distinction based on improved probabilistic latent semantic analysis.(ICIC-ELB)ICIC Express Letters PartB: Applications 第 5 卷 ，第 6 期.pp.1701-1706,2014(EI)
25. Longlong Wang ，Xinjun Wang and Ming Xu.A Method Based on Linear Combination with Dynamic Weight for Event Duplication Detection.(ICIC-ELB)ICIC Express Letters PartB: Applications 第 5 卷，第 6 期,pp.1707-1714,2014(EI)
26. Wei Guo, Kaibo Luo, Xinjun Wang and Lizhen Cui.The Design and Evaluation of a Strategy of Data Placement in Cloud Computing Platform.INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS Vol.7No.1,2014,pp. 13-30,2014(EI)
27. Lanju Kong, Qingzhong Li and Lin Li.Enabling Access Control in Partially Honest Outsourced Databases .International Journal of Database Theory and Application Vol.7, No.3 (2014), pp.63-72,2014(EI)
28. Kong Lanju, Li Qingzhong, Li Lin and Sang Chengliang. Research on Multi-tenant Replication Consistency Based on Quorum NRW System .International Journal of Grid Distribution Computing Vol.7, no.3 ,pp. 13-22, 2014(EI)
29. Chao Yu, Yuliang Shi Game-Theoretic Strategy for Personalized Privacy Protection International Journal of Grid and Distributed Computing Vol.7, no.4 (2014）,pp.123-138 2014(EI)
30. Li Lin1, Li Qingzhong, Kong Lanju and Shi Yuliang. Efficient Query Integrity Protection for Multi-tenant Database.International Journal of Database Theory and Application Vol.7, No.3 ,pp.31-40 ,2014(EI)
31. 张甜甜，崔立真，徐猛.基于 pareto 最优的 Daas 数据布局策略.计算机研究与发展 51(6),pp.1373-1382,2014(EI)
32. Huihui Cai and Lizhen Cui.MultiGranular: An effective Service Composition Infrastructure for Multi-tenant Service Composition. International Journal of Multimedia and Ubiquitous Engineering（IJMUE） Vol.9, No.6 ,pp.171-182,2014(EI)
33. Huihui Cai and Lizhen Cui.Cloud Service Composition Based on Multi-Granularity clustering.Journal of Algorithms&Computational Technology Volume 8,Number2,pp.143-161,2014(EI)
34. Yuanzi Xu ，Qingzhong Li, Zhongmin Yan and Wei Wang.Web Event Topic Analysis by Topic Feature Clustering and Extended. LDA Model JOURNAL OF SOFTWARE VOL. 9, NO. 4,pp. 977-

984 ,2014(EI)

35. Yuanzi Xu , Qingzhong Li, Zhongmin Yan and Wei Wang.Web Reviews and Events Matching Based on Event Feature Segments and Semi-Markov Conditional Random Fields.JOURNAL OF SOFTWARE VOL. 9, NO. 9,pp. 2401-2408,2014(EI)
36. Xu, Yuanzi; Li, Qingzhong; Yan, Zhongmin;Wang, Wei. Event Detection in Multiple Webpages based on Comprehensive Dimension Matching and Co-occurrence Constraint.APPLIED MATHEMATICS & INFORMATION SCIENCES Vol.8, No.3 ,pp.1267-1276 ,2014(SCI)
37. Yali Shao, Yuliang Shi and Hui Li.A Novel Cloud Data Fragmentation Cluster-based Privacy Preserving Mechanism . （IJGDC） International Journal of Grid Distribution Computing Vol.7, No.4,pp.21-32,2014(EI)
38. Lanju KONG*, Lin LI, Qingzhong LI, Yuliang SHI.Composite Authentication Scheme for Data Integrity Protection in SaaS ⋆ .Journal of Computational Information Systems Volume 10 • Number 15,pp.6419–6426, 2014(EI)
39. 史玉良,王捷 .一种多租户云数据存储缓存管理机制.计算机研究与发展 51（11）,pp. 2528-2537,2014(EI)
40. 谷连超,崔立真.一种可伸缩的多租户数据自适应存储方法.计算机研究与发展 51（9）,pp. 2058-2069,2014(EI)
41. Xiaona LI, Qingzhong LI, Lanju KONG, Zhongmin YAN.Research on Multi-tenant Data Placement Strategy for SaaS Application Based on SLA-cost ⋆.Journal of Computational Information Systems Vol.10, No.17 ,pp.7499-7506,2014(EI)
42. Li, Xiaona1; Li, Qingzhong; Kong, Lanju; Yan, Zhongmin; Hou, Dezhi.Research on multi-tenant data placement mechanism for SaaS application based on load optimization⋆. Journal of Computational Information Systems Vol.10, No.22,pp.9641-9648,2014(EI)
43. Guo, Wei ； Wang, Xinjun A framework for workload aware SaaS platform data management Journal of Computational Information Systems Vol.10, No.22 9699-9706 2014(EI)
44. Huihui CAI and Lizhen CUI*.Cloud Service Composition Based on Multi-Granularity Clustering.Journal of Algorithms & Computational Technology Vol. 8 No. 2 ,pp. 143-161, 2014(EI)
45. Meng Xu, Qingzhong Li*, Lizhen Cui. A framework to support flexible application collaboration in cloud computing cloud. computing Information and Computer Technologies 18(11),pp.498-504,2014(EI)