2011 年度

2011 年度实验室共发表论文及著作 30 篇，其中 EI 检索 9 篇，SCI 检索 11 篇。论文及著作列表如下。

1. Xiaoyun Wang, Mingjie Liu, Chengliang Tian and Jingguo Bi, Improved Nguyen-Vidick Heuristic Sieve Algorithm for Shortest Vector Problem, AISACCS 2011. (EI)
2. Meiqin Wang, Yue Sun, Nicky Mouha, Bart Preneel, Algebraic Techniques in Differential Cryptanalysis Revisited, ACISP 2011, LNCS 6812, pp.120-141. (EI)
3. Hongbo Yu, Xiaoyun Wang. Cryptanalysis of the Compression Function of SIMD, ACISP 2011, LNCS 6812, pp.157-171. (EI)
4. Mingqiang Wang, Xiaoyun Wang, Tao Zhan and Yuliang Zheng, Skew-Frobenius Map on Twisted Edwards Curves, ICIC Express Letter, 5(6), pp.2089-2094, 2011.
5. Jia Yu, Rong Hao, Fanyu Kong, Xiangguo Cheng, Jianxi Fan, Yangkui Chen, Forward-Secure Identity-Based Signature: Security Notions and Construction. Information Sciences. Elsevier Press, Volume 181, Issue 3, February 2011, 648-660. (SCI/EI)
6. Fanyu Kong, Jia Yu, Key Substitution Attack and Malleability of a Short Signature Scheme with Batch Verification, Applied Mechanics and Materials, Vol. 55-57, (2011), pp.1605-1608. (EI)
7. Fanyu Kong, Lei Wu, Jia Yu, Another Attack on Tso's Short Signature Scheme Based on Bilinear Pairings, Applied Mechanics and Materials, Vol. 63-64, (2011), pp.785-788. (EI)
8. Guanhua Ji (Joint with T. Gillespie), Prime number theorems for Rankin-Selberg L-functions over different number fields, Sci. China Ser. A: Math. Vol.54, No.1, pp,35-46,2011. (SCI)
9. Guanshi Lv. J. Wu and W.G. Zhai, On a divisor problem related to the Epstein zeta-function III, to appear in Quart. J. Math. (Oxford).
10. Guanshi Lv. On general divisor problems involving Hecke eigenvalues, to appear in Acta Mathematica Hungarica
11. Guanshi Lv. Y.-K. Lau and J. Wu, Integral power sums of Hecke eigenvalues, to appear Acta Arith..
12. Guanshi Lv. (With Y.-K. Lau), Sums of Fourier coefficients of cusp forms, to appear in Quart. J. Math. (Oxford)
13. Guanshi Lv. (With Z.X. Liu), Density of two squares and powers of 2, International Journal of Number Theory, 5(2011), pp.1317-1329. (SCI)
14. Guanshi Lv., On mean values of some arithmetic functions in number fields, Acta Mathematica Hungarica, 132(2011), pp.1924-1938. (SCI)
15. Guanshi Lv. (With Z.S. Yang), The average behavior of the coefficients of Dedekind zeta functions over square numbers, Journal of Number Theory, 131(2011), pp.1924-1938. (SCI)
16. Guanshi Lv, H.W. Sun, Primes in quadratic progressions on average, Acta Math.Sin.(Engl.Ser.), 27(2011), pp.1187-1194. (SCI)

17. Guanshi Lv. J. Wu and W.G. Zhai, On a divisor problem related to the Epstein zeta-function II, Quart. J. Math. 131(2011), pp.1734-1742. (SCI)
18. Guanshi Lv. Z.X. Liu, On unlike powers of prime and? powers of 2, Acta Mathematica Hungarica, 132(2011), pp.125-139. (SCI)
19. Guanshi Lv. Z.X. Liu, Two results on powers of a in Waring-Goldbach problem, Journal of Number Theory, 131(2011), pp.716-736. (SCI)
20. Guanshi Lv. On higher moments of Fourier coefficients of holomorphic cusp forms, Canadian Journal of Mathematics, 63(2011), pp.634-647. (SCI)
21. Lizhen Cui, Junjie Tian, Haiyang Wang, Qingzhong Li, Service Cooperation in PaaS Platform Based on Planning Method (CSCWD2011)The 2011 15th International Conference on Computer Supported Cooperative Work in Design, June 8-10, 2011, Lausanne Switzerland 2010. (EI)
22. Yue Sun, Meiqin Wang, Qiumei Sun, How to Search Linear Approximations for Large Non-Surjective S-boxes, ASIACCS 2011, pp.459-465, 2011. (EI)
23. Jiazhe Chen, Keting Jia, Hongbo Yu and Xiaoyun Wang, New Impossible Differential Attacks of Reduced-Round Camellia-192 and Camellia-256, ACISP 2011, LNCS 6812, pp.16-33. (EI)
24. An Wang, Zheng Li, Xianwen Yang, and Yanyan Yu, A New Security Proof of Practical Cryptographic Devices Based on Hardware, Software and Protocols. 7th Information Security Practice and Experience Conference (ISPEC 2011), LNCS, vol. 6672, Springer, pp.386-400. (EI)
25. Dong Yongquan, Li Qingzhong, Ding Yanhui, Peng Zhaohui, ETTA-IM: Adeep web query interface matching approach based on evidence theory and task assignment Expert Systems with Applications 2011, Vol.38 No.8 2011. (SCI)
26. Jinshan Pang, Lizhen Cui, Yongqing Zheng, Haiyang Wang, A Workflow-Oriented Cloud Computing Framework and Programming Model for Data Intensive Application, CSCWD2011.
27. Zhongqiu Song, Zongshui Xiao, Fangfang Wu, A Network Services Management Middleware Architecture Model, ICCSIT 2011.
28. Zhang Yong-Xin, Li Qing-Zhong, Sun Tao1, Xu Yuan-Zi, A Novel Method for Linking Reviews with Database Objects, MEC 2011.
29. Wang Xue, Li Qingzhong and Kong Lanju, Multiple Sparse Tables Based On Pivot Table For Multi-Tenant Data Storage In SaaS, ICIA2011.
30. Fangfang Wu, Zongshui Xiao, Zhongqiu Song, A Virtualization Model of Network Services Management, ICCSIT 2011.