2009 年度

2009 年度实验室共发表论文及著作 90 篇，其中 EI 检索 62 篇，SCI 检索 21 篇。论文及著作列表如下。

1. Xiaoyun Wang, Hongbo Yu, Wei Wang, Haina Zhang, Tao Zhan, Cryptanalysis on HMAC/NMAC-MD5 and MD5-MAC, Advances in Cryptology, Eurocrypt 2009, LNCS 5479, pp. 121-133, 2009. (EI)
2. Xiaoyun Wang, Wei Wang, Keting Jia, Meiqin Wang, New Distinguishing Attack on MAC using Secret-Prefix Method, FSE 2009, LNCS 5665, pp. 363-374, 2009. (EI)
3. 王薇，王小云，CLEFIA-128/192/256 的不可能差分分析，软件学报，20(9): 2587-2596，2009. (EI)
4. Zheng Yuan, Wei Wang, Keting Jia, Guangwu Xu, and Xiaoyun Wang, New Birthday Attacks on Some MACs Based on Block Ciphers, Crypto 2009, LNCS 5677, pp. 209-230, 2009. (EI)
5. Guoyan Zhang, Xiaoyun Wang. Certificateless Encryption Scheme Secure in the Standard Model. Tsinghua Science and Technology. 14(4), pp. 452-459, 2009. (EI)
6. Guoyan Zhang. Certificateless Threshold Decryption Scheme Secure in the Standard Model. The 2nd International Conference on Computer Science and Information Technology, vol. 2, pp. 414-418, 2009. (EI)
7. Fanyu Kong, Jia Yu, Number-Theoretic Attack on Lyuu-Wu's Multi-proxy Multi-signature Scheme, IAS 2009, Volume 1, pp. 666-668, IEEE Computer Society, 2009. (EI)
8. Mingqiang Wang, Leibo Li. A Note on Twin Diffie-Hellman Problem, CIS 2009, pp. 451-454, 2009. (EI)
9. Mingqiang Wang, Qin Jing, Zhao Huawei. Non-interactive oblivious transfer protocols, Proceedings-2009 International Forum on Information Technology and Applications, IFITA 2009, v 2, pp.120-124, 2009. (EI)
10. Meiqin Wang, Jorge Nakahara Jr, Yue Sun, Cryptanalysis of the full MMB block cipher, SAC 2009, LNCS 5867, pp.231–248, 2009. (EI)
11. Xianmeng Meng, On linear equations with prime variables of special type. Journal of Number Theory 129 (2009), no. 10, pp. 2504-2518, 2009. (SCI)
12. Xianmeng Meng, Jingguo Bi, Weak Keys in RSA With Primes Sharing Least Significant Bits. Inscrypt 2009, LNCS 6151, pp. 278–287, 2009. (EI)
13. Hongbo Yu, Xiaoyun Wang, Near-Collision Attack on the Compression Function of Dynamic SHA2, http://eprint.iacr.org/2009/179.pdf, 2009.
14. Hongbo Yu, Xiaoyun Wang, Full Key-Recovery Attack on the HMAC/NMAC Based on 3 and 4-Pass HAVAL, ISPEC

2009, LNCS 5451, pp.285-297,2009. (EI)

15. Hongbo Yu, Xiaoyun Wang, Distinguishing Attack on the Secret-Prefix MAC Based on the 39-step SHA-256, ACISP 2009, LNCS 5594, pp.185-201,2009. (EI)
16. 刘华宁，On the mean values of Dedekind sums and Hardy sums, Journal of the Korean Mathematical Society, 2009, 46(1): 187-213. (SCI)(博士后)
17. 刘华宁，翟文广，A note on the pseudorandomness of the Liouville function, Acta Arithmetica, 2009, 136(2): 101-121. (SCI)(博士后)
18. 刘华宁，张文鹏，Some applications of certain character sums, Rocky Mountain Journal of Mathematics, 2009, 39(2): 573-589. (SCI)(博士后)
19. 刘华宁，A large family of pseudorandom binary lattices, Proceedings of the American Mathematical Society, 2009, 137(3): 793-803. (SCI）(博士后)
20. 刘华宁，展涛，王小云，On the correlation of pseudorandom binary sequences with composite moduli, Publicationes Mathematicae Debrecen, 2009, 74(1-2): 195-214. (SCI)(博士后)
21. 刘华宁，展涛，王小云，Large families of elliptic curve pseudorandom binary sequences, Acta Arithmetica, 2009, 140(2): 135-144. (SCI)(博士后)
22. 刘华宁，A note on Lehmer k-tuples, International Journal of Number Theory, 2009, 5(7): 1169-1178. (SCI)(博士后)
23. 刘华宁，高静，由椭圆曲线生成的 Z 中的伪随机子集，数学学报，2009, 52(2): 209-216. (博士后)
24. Fanyu Kong, Jia Yu, Number-Theoretic Attack on Lyuu-Wu's Multi-proxy Multi-signature Scheme, The Fifth International Conference on Information Assurance and Security 2009-IAS 2009, Volume 1, Page(s): 666-668, Digital Object Identifier: 10.1109/IAS.2009.130, IEEE Computer Society, August 2009. (EI)
25. Fanyu Kong, Jia Yu, Security Analysis of a Shared Modular Inversion Protocol for RSA Cryptosystem, The Asia-Pacific Conference on Information Processing 2009 - APCIP 2009, Volume 2, Page(s): 553 – 556, Digital Object Identifier: 10.1109/APCIP.2009.272, IEEE Computer Society, July 2009. (EI)
26. Jia Yu, Fanyu Kong, Xiangguo Cheng, Rong Hao: A Forward Secure Threshold Signature Scheme Based on the Structure of Binary Tree. JSW 4(1): 73-80 (2009). (EI)
27. Jianya Liu (with A. V. Kumchev), Sums of primes and squares of primes in short intervals, Monatsh. Math. (2009) 157, 335-363. (SCI)
28. Jianya Liu (with Y. Wang), A theorem on analytic strong multiplicity one, J. Number Theory 129 (2009) No. 8 1874-1882. (SCI)

29. Jianya Liu (with Y. Ye), Functoriality of automorphic L-functions through their zeros, Sci. China Ser. A, 52 (2009), 1-16. (SCI)
30. Yuliang Shi, Shuai Luan, Qingzhong Li, Haiyang Wang, A Multi-Tenant Oriented Business Process Customization System (NISS2009)2009 International Conference on New Trends in Information and Service Science 2009. (EI)
31. Yuliang Shi, Shuai Luan, Qingzhong Li, Haiyang Wang, A Flexible Business Process Customization Framework for SaaS, (ICIE2009)2009 WASE International Conference on Information Engineering Taiyuan, Shanxi, China.10-11 July 2009 2009. (EI)
32. Guanshi Lv, Number of solutions of certain congruences, Acta Arith. , 140.4(2009), 317-328. (SCI)
33. Guanshi Lv, The sixth and eighth moment of Fourier coefficients of cusp forms, Journal of Number Theory, 129.11(2009), 2790-2880. (SCI)
34. Guanshi Lv, On an open problem of Sankaranarayanan, Science in China Series A:Mathematics, 39.8(2009), 1023-1028. (SCI)
35. Guanshi Lv, Uniform estimates for sums of Fourier coefficients of cusp forms, Acta Mathematica Hungarica, 124.1-2(2009), 83-97. (SCI)
36. Guanshi Lv, On sums involving coefficients of automorphic L-functions, Proceedings of the AMS, 137.9(2009), 2879-2887.
37. Guanshi Lv, Average behavior of Fourier coefficients of cusp forms, Proceedings of AMS, 137.6(2009), 1961-1969. (SCI)
38. Guanshi Lv, H.W. Sun, On a generalization of Hua's theorem with five squares primes, Acta Mathematica Hungarica, 122.3(2009), 273-282. (SCI)
39. Guanshi Lv, W.G. Zhai, On the representation of large integers as sums of four almost equal squares of primes, The Ramanujan Journal, 18(2009), 1-10. (SCI)
40. Guanshi Lv, H.W. Sun, Integers represented as the sum of one prime, two squares of primes and powers of 2, Proceedings of AMS, 137.4(2009), 1185-1191. (SCI)
41. Guanshi Lv, The average value of Fourier coefficients of cusp forms in arithmetic progressions, Journal of Number Theory, 129(2009), 488-494. (SCI)
42. Guanshi Lv, Additive functions on arithmetic progressions with large moduli, Journal of Number Theory, 129(2009), 477-487.
43. Jorge Nakahara, Pouyan Sepehrdad, Bingsheng Zhang, Meiqin Wang, Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT. CANS 2009: 58-75. (EI)

44. Lidong Han, Guangwu Xu, Generalization of Some Attacks on RSA with Small Prime Combination and Small Private Exponent, Asia-Pacific Conference on Information Processing 2009(APCIP 2009), 2009.7.19. (EI)
45. Keting Jia, Xiaoyun Wang, Zheng Yuan, Guangwu Xu, Distinguishing and Second-Preimage Attacks on CBC-Like MACs, CANS 2009, LNCS 5888, pp.349–361, Springer, Heidelberg (2009). (EI)
46. Keting Jia, XiaoyunWang, Meaningful Collision Attack on MD4. Journal of Frontiers of Computer Science and Technology, 2009, 4(3):10-21.
47. Siyuan Qiao, Wei Wang, Keting Jia, Distinguishing Attack on Secret Prefix MAC Instantiated with Reduced SHA-1 , ICISC 2009,Seoul, Korea, December 2-4, LNCS 5984. (EI)
48. Lin Yang, Meiqin Wang, Siyuan Qiao, Side Channel Cube Attack on PRESENT. CANS 2009, Springer, 2009, LNCS 5888, pp.379–391. (EI)
49. Shunhua Zhang, Generalizations of a Theorem about the Binomial Coefficient. JP Journal of Algebra, Number Theory and Applications, 14(2), 177-184 (2009).
50. Li Shenhua, Zhang Haina, Wang Xiaoyun, Dedicated Linear Attack on ARIA Version 1.0. Tsinghua Science and Technology, 14(2), pp 212-217, 2009.(EI)
51. Puwen Wei, Guoyan Zhang, Lijiang Zhang, Xiaoyun Wang, Simplified Design for Concurrent Statistical Zero-Knowledge Arguments. Tsinghua Science and Technology, 14(2), pp 255-263, 2009. (EI)
52. Puwen Wei, Xiaoyun Wang, Yuliang Zheng. Public Key Encryption Without Random Oracle Made Truly Practical. ICICS 2009, LNCS 6151, pp. 278–287, 2009.LNCS 5927, pp.107-120, 2009/12/14. (EI)
53. Baodong Qin, Ming Li, Fanyu Kong, Daxing Li, New left-to-right minimal weight signed-digit radix-r representation, Computers & Electrical Engineering, Volume 35, Issue 1, Pages 150-158, 2009. (SCI, EI)
54. Yali Jiang, Xiuling Ju, Lattice-Based CCA-Secure Cryptosystem from IBE System. CIS (2) 2009: 260-264. (EI)
55. Yanhui Ding, Qingzhong Li, Feifei Li, A Novel Method for Evaluating Trustworthiness between Strangers in Large, Dynamic Ad Hoc Networks (WKDD2009)2009 Second International Workshop on Knowledge Discovery and Data Mining Moscow, Russia.23-25 January 2009 2009. (EI)
56. Yanhui Ding, Qingzhong Li, Yongquan Dong, Web Source Evaluation and Selection by Mass Collaboration (WKDD2009)2009 Second International Workshop on Knowledge Discovery and Data Mining Moscow,Russia.23-25 January 2009 2009. (EI)
57. Qing Kong, Qingzhong Li, Object Distinction Based on Decision Tree, (ITCS 2009)2009 International Conference on Information Technology and Computer Science 25-26 July 2009. Kiev, Ukraine 2009. (EI)
58. Junren Wang, Qingzhong Li, Yongquan Dong, A Method of Schema Matching Based on Top-K Mapping and

User Feedback 2009 Fifth International Joint Conference on INC, IMS and IDC 25-27 August 2009.Seoul, Korea 2009. (EI)

59. Kun Zhang, Yuliang Shi, Qingzhong Li, Ji Bian, Data Privacy Preserving Mechanism based on Tenant Customization for SaaS 2009 International Conference on Multimedia Information Networking and Security 17-20 November 2009 Hubei, China, 2009. (EI)
60. Hongbo Li,Yuliang Shi,Qingzhong Li. A Multi-granularity Customization Relationship Model for SaaS* (WISM2009)2009 International Conference on Web Information Systems and Mining 7-8 November 2009 Shanghai,China. 2009 (EI)
61. Xu Cheng, Yuliang Shi, Qingzhong Li. A Multi-tenant Oriented Performance Monitoring, Detecting and Scheduling Architecture Based on SLA* (JCPC2009)The 2009 Joint Conferences on Pervasive Computing December 3-5，2009.Taipei,Taiwan 2009 (EI)
62. Zhang Yongxin,Li Qingzhong,Bian Ji. Enhancing Collective Entity Resolution utilizing Quasi-Clique Similarity Measure (JCPC2009)The 2009 Joint Conferences on Pervasive Computing December 3-5，2009.Taipei,Taiwan 2009 (EI)
63. Gao Ting,Wang Haiyang,Zheng Naihui，Li Fei.An Improved Way to Facilitate Composition-Oriented Semantic Service Discovery.(ICCET 2009)2009 International Conference on Computer Engineering and Technology.Volume Ⅱ.(EI)硕士
64. Lirong Wan,Xinjun Wang,Congcong Chen.A Spiral-Decoding Method for Web Data Extraction.(ETCS2009)The First International Workshop on Education Technology and Computer Science .Volume 1.(EI)硕士
65. Hui Li,Haiyang Wang.An Automatic Configuration Method for Teaching Management Process.(GCIS2009)2009 WRI Global Congress on Intelligent Systems.(EI)
66. Zhao Jiuzhen,Zhang Shidong,Yan Zhongmin.A Novel Method for XML Scheme Matching.(IFITA 2009)国际信息技术与应用论坛 2009 International Forum on Information Technology and Applications.(EI)硕士
67. Baoshi Ding,Yongqing Zheng,Shaoyu Zang.A New Decision Tree Algorithm Based on Rough Set Theory.(APCIP2009)2009 Asia-Pacific Conference on Information Processing.(EI)硕士
68. MA Shao-long,WANG Xin-jun,ZHANG Feng,BIAN Ji.Efficient Processing of XML Twig Pattern Matching based on Extended Region Encoding Labeling Scheme.(ITME2009)The 2009 IEEE International Symposium on IT in Medicine & Education.(EI)硕士
69. Ji Feng,Xiaoguang Hong,Yuanbo Qu.An Instance-based Schema Matching Method with Attributes Ranking and Classification.(FSKD'09)6th International Conference on Fuzzy Systems and Knowledge Discovery .(EI)硕士

70. Lei Liu,Yongqing Zheng,Baoshi Ding,Haiyan Liu.A methodology for clustering XML documents based on labeled tree.(FSKD'09)6th International Conference on Fuzzy Systems and Knowledge Discovery .(EI)硕士
71. Yuanbo Qu,XiaoGuang Hong,Ji Feng.An approach to construct secure view for XML.(MASS2009)2009 International Conference on Management and Service Science.(EI)硕士
72. Fangqiao Xiao,Xiaoguang Hong,Keyong Yuan.Mining Association Rules Using Value Dependence and Pseudo Intension.(MASS2009)2009 International Conference on Management and Service Science.(EI)硕士
73. Jing Wen,Shidong Zhang,Zhongmin Yan.SLCO and DLCO: Two Ontologies for Detecting and Resolving Schema and Data-Level Semantic Conflicts.(ICIA2009)2009 IEEE International Conference on Information and Automation.(EI)硕士
74. Tiankun Zheng,Xinjun Wang,Yingchun Zhou.Indexing Temporal XML Using FIX.(WISM2009)2009 International Conference on Web Information Systems and Mining.(EI)硕士
75. Yuan Ke-yong,Hong Xiao-guang,Xiao Fang-qiao.An Algorithm for Attribute Reduction Based on Database Technology.(AICI2009)2009 International Conference on Artificial Intelligence and Computational Intelligence.(EI)硕士
76. Shuai Luan,Yuliang Shi,Haiyang Wang.A Mechanism of Modeling and Verification for SaaS Customization Based on TLA.(WISM2009)2009 International Conference on Web Information Systems and Mining.硕士
77. Chen Wei-Liang,Zhang Shi-Dong,Gao Xiang.Anchoring the Consistency Dimension of Data Quality Using Ontology.(WISA 2009)2009 Web Information Systems And Applications Conference.(EI)硕士
78. Meng Xu,Lizhen Cui,Haiyang Wang, Yanbing Bi,Ji Bian.A Data-Intensive Workflow Scheduling Algorithm for Grid Computing.(ChinaGrid 2009)2009 Fourth ChinaGrid Annual Conference.(EI)硕士
79. Meng Xu,Lizhen Cui,Haiyang Wang,Yanbing Bi.A Multiple QoS Constrained Scheduling Strategy of Multiple Workflows for Cloud Computing.(ISPA2009)2009 IEEE International Symposium on Parallel and Distributed Processing with Applications.(EI)硕士
80. Hao Guanghao,Zheng Yongqing,Cui Lizhen.Computing Maximum Error and Reduced Threshold of Mining Frequent Patterns in Data Stream.(ICIECS2009)2009 International Conference on Information Engineering and Computer Science .(EI)硕士
81. Shun Han,Haiyang Wang,Lizhen Cui.A User Experience-Oriented Service Discovery Method with Clustering Technology.(ISCID2009)2009 Second International Symposium on Computational Intelligence and Design.(EI)硕士
82. Yingchun Zhou,Guoqing Dong,Lu Chen,Renyou.Research of Clustering Algorithm Based On Data Content for

Heterogeneous Sensor Networks.(WNIS2009)2009 International Conference on Wireless Networks and Information Systems.(EI)硕士

83. Xianzhi Huang,Lizhen Cui,Haiyang Wang,Wenjing Cui.Towards A Decentralized Cooperative BRMS for Service Collaborative Enterprise.(CSCWD2009)2009 13th International Conference on Computer Supported Cooperative Work in Design.(EI)
84. 41.LI Wen-hao,WANG Hai-yang.A Dynamic and Adaptive Scheduling Algorithm for Distributed Student Registration System.(ITME2009)The 2009 IEEE International Symposium on IT in Medicine & Education.(EI)硕士
85. Bing Liu,Yuliang Shi,Haiyang Wang.QoS Oriented Web Service Composition and Optimization in SOA.(JCPC2009)The 2009 Joint Conferences on Pervasive Computing.(EI)硕士
86. Tian JunJie,Cui Lizhen.A Method of Services Intelligent Cooperative Work for Requirements Based on Integrated Planning.(JCPC2009)The 2009 Joint Conferences on Pervasive Computing.(EI)硕士
87. Liu Shiqun,Cui Lizhen.Research on Process-Oriented Component Dynamic Migration and Deployment in Pervasive Environment.(JCPC2009)The 2009 Joint Conferences on Pervasive Computing.(EI)硕士
88. Yuping Zhang,Xinjun Wang,Ying Zhang.A Labeling Scheme for Temporal XML.(WISM2009)2009 International Conference on Web Information Systems and Mining.(EI)硕士
89. 李帅,王华,王新军，石钊.树形变换的 PSO 组播路由算法.小型微型计算机系统.Vol.30 No.8 2009.(EI)硕士
90. 侯金奎，万建成，杨潇，王海洋.构件式体系结构模型映射的形式化语义.计算机研究与发展.46(2),2009.(EI)博士