2013年论文列表

发布时间：2016-03-10 【字号： 小 中 大 】

序号	论文类型	论文名称	刊物名称	论文所在期刊的卷、期、页	论文收录类型	论文作者
1	国外重要刊物	Relative Network Entropy based Clustering Algorithm for Intrusion Detection	International Journal of Network Security	Vol. 15, No. 1, 2013, pp. 16-22	SCI收录	X. B. Chen, X. X. Niu, X. J. Zhou, and Y. X. Yang
2	国外重要刊物	Multi-party quantum secret sharing with the single-particle quantum state to encode the information	Quantum Information Processing	12 (1): 365-380 (2013)	SCI收录	X. B. Chen, X. X. Niu, X. J. Zhou, and Y. X. Yang
3	国外重要刊物	High-dimensional deterministic multiparty quantum secret sharing without unitary operations	Quantum Information Processing	12 (2): 785-792 (2013)	SCI收录	M. M. Wang, X. B. Chen, and Y. X. Yang
4	国外重要刊物	Attack on the Improved Quantum Blind Signature Protocol	International Journal of Theoretical Physics	52 (2): 331-335 (2013)	SCI收录	M. Zhang, G. A. Xu, X. B. Chen, S. Yang, and Y. X. Yang
5	国外重要刊物	The faithful remote preparation of general quantum states	Quantum Information Processing	12 (1): 279-294 (2013)	SCI收录	M. X. Luo, X. B. Chen, Y. X. Yang, and X. X. Niu
6	国内重要刊物	A new key-stream generation scheme based on chaotic systems	Journal of Central South University of Technology	Vol. 20 No. 7 July,1904-1909,2013	SCI收录	Huang Fang-jun, Zhao Yu-qian
7	国外重要刊物	Quantum private communication with an anonymous sender	International Journal of Theoretical Physics	2013, 52(2): 411-419	SCI收录	Xiao-Qiu Cai, Hui-Fang Niu

8	国外重要刊物	Cryptanalysis of dynamic quantum secret sharing	Quantum Information Processing	doi:10.1007/s11128-012-0508-2	SCI收录	Tian-Yin Wang, Yan-Ping Li
9	国外重要刊物	A robust blind color image watermarking in quaternion Fourier transform domain	Journal of Systems and Software	2013, 86(2): 255-277	SCI收录	Xiang-yang Wang, Chun-peng Wang, Hong-ying Yang, Pan-pan Niu
10	国外重要刊物	An efficient certificateless aggregate signature with constant pairing computations	Information Sciences	19(10): 225-235, 2013, Elsevier Press	SCI收录	Hu Xiong*, Zhi Guan, Zhong Chen, Fagen Li
11	国外重要刊物	Efficient Public Key Cryptosystem Resilient to Key Leakage Chosen Ciphertext Attacks	CT-RSA 2013, Springer, Heidelberg, San Francisco, Feb 25 - Mar. 1, 2013	LNCS 7779, pp. 84--100	EI收录	Shengli Liu, Jian Weng, Yulei Zhao
12	国外重要刊物	On the linear complexity of binary threshold sequences derived from Fermat quotients. Designs	Codes and Cryptogr	67 (3), 317-323	SCI收录	Zhixiong Chen and Xiaoni Du
13	国外重要刊物	An ID-based three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments	Arabian Journal for Science and Engineering	August 2013, Volume 38, Issue 8, pp 2055-2061	SCI收录	Deibao He, Yitao Chen, Jianhua Chen
14	国内重要刊物	一种基于FPGA的可信平台模块攻击方法	北京工业大学学报	期1，2013	其他收录	李健俊、方娟、季琦、刘鹏、毛军捷、林莉、姜伟
15	国内重要刊物	一种高效的(k, p)进制转换算法	应用科学学报	2013 Vol. 31 (6): 569-578	EI收录	陈嘉勇, 张卫明, 胡金龙,祝跃飞
16	国内重要刊物	高效自适应图像隐写术	自动化学报	2013 Vol. 39 (10): 1594-1601	EI收录	陈嘉勇, 张卫明, 韩涛,祝跃飞
17	国外重要刊物	Grid-based Data Stream Clustering for Intrusion Detection	International Journal of Network Security	Vol. 15, No. 1, 2013, pp. 1-8	其他收录	Qian Quan, Chao-Jie Xiao, and Rui Zhang
18	国外重要	Relative Network Entropy based Clustering Algorithm for Intrusion	International Journal of Network Security	Vol. 15, No. 1, 2013, pp. 16-22	其他收	Quan Qian, Tianhong Wang,

	刊物	Detection			录	and Rui Zhan
19	国内重要刊物	基于随机数同步更新的RFID安全协议	计算机工程	2013 Vol. 39 (8): 9-14	其他收录	钱权, 贾彦龙, 张瑞
20	国内重要刊物	基于主机攻击图的攻击识别	上海大学学报	2013 Vol. 19 (3): 271-279	其他收录	钱权, 朱伟, 赖岩岩, 张瑞
21	国外重要刊物	Generalized ptychography with diverse probes	Optical Engineering	2013, 30 (5): 054203	SCI收录	Y. Shi*, Y. Wang and S. Zhang
22	国内重要刊物	对完整轮数ARIRANG加密模式的新的相关密钥矩形攻击	计算机科学	2013,40(8):109-114	其他收录	刘青，卫宏儒
23	国外重要刊物	A recursive construction of resilient Boolean function with high nonlinearity	Information Science	DOI:10.1016/j.ins.2013.10.015, 2013	SCI收录	Shaojing Fu, Chao Li, Longjiang Qu.
24	国外重要刊物	Improved Construction of Boolean Function with Maximum Algebraic Immunity using Univariate Polynomial Representation	IEICE Transactions on Fundamentals 96-A(1	pp360-362,2013	SCI收录	Shaojing Fu, Chao Li, Longjiang Qu
25	国内重要刊物	缩减轮数PRESENT算法的Biclique分析	计算机学报	2013 (6)	EI收录	龚征，刘树生，温雅敏，唐韶华
26	国外重要刊物	Comparative Study of Multicast Authentication Schemes with Application to Wide-Area Measurement System	ACM AsiaCCS 2013, Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communication	pp. 287-298, 2013	EI收录	Yee Wei Law, Zheng Gong, Tie Luo, Slaven Marusic and Marimuthu Palaniswami
27	国外重要刊物	Power Analysis Attacks against Hardware Implementation of KLEIN	Journal of Computational Information Systems	8: 1 (2013)	EI收录	Weijian Li, Shaohua Tang and Zheng Gong
28	国外重要刊物	Differential Fault Analysis on the MD5 Compression Function	Journal of Computers	8(11), pp. 2888–2296，2013	EI收录	W. Li, Z. Tao, D. Gu, Y. Wang, Z. Liu, Y. Liu

29	外重要刊物	Post-quantum strongly unforgeable identity-based signature scheme from lattices without random oracles	5th International Conference on Intelligent Networking and Collaborative Systems –INCoS2013	IEEE, 2013, pp. 578-585	EI收录	Zhenhua Liu*, Xiangsong Zhang, Tsuyoshi Takagi
30	国内重要刊物	标准模型下高效的强不可伪造短签名方案	江苏大学学报（自然科学版）	2013,34（3）：309-313	其他收录	刘振华，胡予濮，张襄松
31	国外重要刊物	Steganalysis of a PVD-based Content Adaptive Image Steganography	Signal Processing, 2013	93(9): 2529-2538	SCI收录	Xiaolong Li, Bin Li, Xiangyang Luo, Bin Yang, Ruihui Zhu
32	国外重要刊物	Steganalysis of F5-like Steganography Based on Selection of Joint Distribution Features	Proceedings of the 5th ACM International Conference on Internet Multimedia Computing and Service (ICIMCS)	2013, pp.71-75.	EI收录	Yuan Liu, Xiangyang Luo, Jicang Lu, Daofu Gong.
33	国外重要刊物	Fusion of Two Tpyical Quantitative Steganalysis Based on SVR	Journal of Software	2013, 8(3): 731-736	EI收录	Chunfang Yang, Fenlin Liu, Xiangyang Luo, Ying Zeng
34	国外重要刊物	Model of Domain Based RBAC and Supporting Technologies.	Journal of Computers	2013, 8(5): 1220-1229	EI收录	Zan Yang, Lin Yang, Xiangyang Luo, Linru Ma, Baosheng Kou, Kun Zhang
35	国外重要刊物	A System for Extracting and Ranking Name Aliases in Emails	Journal of Software	2013, 8(3): 737-745	EI收录	Meijuan Yin, Xiaonan Liu, Junyong Luo, Xiangyang Luo
36	国外重要刊物	On the privacy of Khanet al.'s dynamic ID-basedremote authentication scheme with user anonymity	Cryptologia	37(4) (2013) 345-355	SCI收录	Da-Zhi Sun*(孙达志) and Zhen-Fu Cao
37	国外重要刊物	A comment on "An efficient common-multiplicand-multiplication method to the Montgomery algorithm for speeding up exponentiation"	Information Sciences	223 (2013) 331-334	SCI收录	Da-Zhi Sun*(孙达志), Jin-Peng Huai, and Zhen-Fu Cao
38	国外重要刊物	A Trust-aware Access Control Policy for Cloud Data Protection	Applied Mechanics and Materials	2013, 411-414: 40-44	EI收录	Xiao Yong Tang, Jin Wei Li, Gui Ping Liao
39	国内重要	基于可编程hash 函数的短签名	中国科学: 信息科学	2013, 43: 335-342, doi: 10.1360/112011-	其他收	王志伟

	刊物			874	录	
40	国外重要刊物	Slight homomorphic signature for Access Controlling in Cloud Computing[J]	Wireless Personal Communications	2013, 73:51-61	SCI收录	Zhiwei Wang, Kewei Sha, Wei Lv
41	国外重要刊物	A New Definition of Homomorphic Signature for Identity Management in Cloud Computing[J]	Journal of Computer and System Sciences, Accepted	Available online 3 July 2013	SCI收录	Zhiwei Wang, Guozi Sun and Danwei Chen
42	国外重要刊物	A Query Conversion Scheme for Encrypted Cloud Databases	ITA2013,CPS出版	2013	EI收录	Hequn Xian, Jing Li, and Xiuqing Lu
43	国外重要刊物	Dynamic Constraint Definition Method in Cloud Databases	CCIS 2013		EI收录	Hequn Xian, Jing Li, and Xiuqing Lu
44	国内重要刊物	标准模型下可证明安全的入侵容忍公钥加密方案	软件学报	2013,24(2)：266-278	EI收录	于佳*，程相国，李发根, 潘振宽, 孔凡玉, 郝蓉
45	国外重要刊物	Security analysis and improvement of two verifiable multi-secret sharing schemes	Int. J. Security and Networks, Inderscience Publishers	Vol. 8, No. 4, 2013.200-206	EI收录	Jia Yu*, Rong Hao, Xiangguo Cheng
46	国外重要刊物	Short (t,N) Key-Insulated Aggregate Signature With Specified Verifier	CECNet 2013	IEEE Press, 2013	EI收录	Huiyan Zhao, Jia Yu*, Tiantian Xun, Shaoxia Duan
47	国外重要刊物	Constructions of balanced Boolean functions with high nonlinearity and high algebraic degree	International Journal of Computer Mathematics	vol. 90, no. 9, pp. 1832-1839, 2013	SCI收录	Yujuan Sun*, Luyang Li, Bo Yang
48	国外重要刊物	The autocorrelation distribution of balanced Boolean function	Frontiers of Computer Science	vol. 7, no. 2, pp. 272-278, 2013.	SCI收录	Yu Zhou*, Weiguo Zhang, Juan Li, Xinfeng Dong, Guozhen Xiao
49	国内重要刊物	Differential Fault analysis and meet in the middle attack on the block cipher katan32	上海交通大学学报(英文版)	18(2),pp147-152,2013.	EI收录	Zhang Wenying, Liu Feng
	国					

50	内重要刊物	特征为2的有限域上的一类差分4一致函数	数学进展	http://advmath.pku.edu.cn/CN/10.11845/sxjz.2012149b	其他收录	肖理，张习勇
51	国外重要刊物	OAKE: a new family of implicitly authenticated diffie-hellman protocols	ACM Conference on Computer and Communications Security	2013: 1113-1128	其他收录	Andrew Chi-Chih Yao, Yunlei Zhao*
52	国外重要刊物	Online/Offline Signatures for Low-Power Devices.	IEEE Transactions on Information Forensics and Security	8(2): 283-294 (2013)	EI收录	Andrew Chi-Chih Yao, Yunlei Zhao*:
53	国外重要刊物	Privacy Preserving Authenticated Key Exchange Over Internet	IEEE Transactions on Information Forensics and Security	Volume: PP ， Issue: 99	EI收录	Andrew Chi-Chih Yao, Yunlei Zhao*:
54	国外重要刊物	Efficient Public Key Cryptosystem Resilient to Key Leakage Chosen Ciphertext Attacks	CT-RSA	2013: 84-100	其他收录	Shengli Liu, Jian Weng, Yunlei Zhao*:
55	国外重要刊物	Privacy-preserving smart metering with regional statistics and personal enquiry services	ASIACCS 2013	369-380	其他收录	Cheng-Kang Chu, Joseph K. Liu, Jun Wen Wong, Yunlei Zhao, Jianying Zhou
56	国外重要刊物	Accountable Authority Identity-Based Encryption with Public Traceability	CT-RSA	2013: 326-342	其他收录	Junzuo Lai, Robert H. Deng, Yunlei Zhao, Jian Weng
57	国外重要刊物	Cryptanalysis of the Quantum State Sharing Protocol Using Four Sets of W-class State	International Journal of Quantum Information	11 (1): 11 (2013)	SCI收录	X. B. Chen, S. Yang, G. Xu, Y. Su, and Y. X. Yang.
58	国外重要刊物	Schemes for Remotely Preparing a Six-Particle Entangled Cluster-Type State	International Journal of Theoretical Physics	52 (3): 968-979 (2013)	SCI收录	S. Y. Ma, P. Tang, X. B. Chen, and Y. X. Yang
59	国外重要刊物	Quantum Teleportation and State Sharing via a Generalized Seven-Qubit Brown State	International Journal of Theoretical Physics	52 (10): 3413-3431 (2013)	SCI收录	S. Y. Kang, X. B. Chen, and Y. X. Yang
60	国外重要刊	A Novel Quantum Covert Channel Protocol Based on Any Quantum Secure Direct Communication Scheme	Communications in Theoretical Physics	59 (5): 547-553 (2013)	SCI收录	S. J. Xu, X. B. Chen, X. X. Niu, and Y. X. Yang

	物						
61	国内重要刊物	Steganalysis and improvement of a quantum steganography protocol via a GHZ(4) state	Chinese Physics B	22 (6): 4 (2013)	SCI收录	S. J. Xu, X. B. Chen, X. X. Niu, and Y. X. Yang
62	国内重要刊物	High-efficiency quantum steganography based on the tensor product of Bell states	Science China-Physics Mechanics & Astronomy	56 (9): 1745-1754 (2013)	SCI收录	S. J. Xu, X. B. Chen, X. X. Niu, and Y. X. Yang
63	国外重要刊物	Comment on "High-dimensional deterministic multiparty quantum secret sharing without unitary operations"	Quantum Information Processing	12 (2): 785-792 (2013)	SCI收录	M. M. Wang, X. B. Chen, and Y. X. Yang
64	国外重要刊物	Deterministic Joint Remote Preparation of an Arbitrary Two-Qubit State Using the Cluster State.	Communications in Theoretical Physics	59 (5): 568-572 (2013)	SCI收录	M. M. Wang, X. B. Chen, and Y. X. Yang
65	国内重要刊物	A blind quantum signature protocol using the GHZ states	Science China-Physics Mechanics & Astronomy	56 (9): 1636-1641 (2013)	SCI收录	M. M. Wang, X. B. Chen, and Y. X. Yang
66	国外重要刊物	Optical color image hiding scheme based on chaotic mapping and Hartley transform	Optics and Lasers in Engineering	51(8): 967-972 (2013)	SCI收录	Zhengjun Liu*, Yu Zhang, Wei Liu, Fanyi Meng, Qun Wu, Shutian Liu
67	国外重要刊物	A mixed scrambling operation for hiding image	Optik	124(22): 5391-5396 (2013)	SCI收录	Zhengjun Liu*, Yu Zhang, Wei Liu, Fanyi Meng, Qun Wu, Shutian Liu
68	国外重要刊物	The power of qutrit logic for quantum computation	International Journal of Theoretical Physics	52(2013)2959-2965	SCI收录	罗明星*, Song-Ya Ma, Xiu-Bo Chen, Yi-Xian Yang
69	国外重要刊物	The rational approximations of the unitary groups	Quantum Information Processing	12(2013) 3149-3166	SCI收录	罗明星*, Yun Deng, Xiubo Chen, Yixian Yang
70	国外重要刊物	Random quantum evolution	Quantum Information Processing	12(2013) 3353-3367	SCI收录	罗明星*, Yun Deng, Song-Ya Ma, Xiu-Bo Chen, and Zhi-Guo Qu
	国						

71	外重要刊物	Efficient Shellcode Detection on Commodity Hardware [J]	IEICE Transactions on Information and Systems	2013, Vol.E96-D,No.10	SCI收录	Donghai Tian, Mo Chen, Hu Changzhen, Xuanya Li
72	国内重要刊物	OPKH: A Lightweight Online Approach to Protecting Kernel Hooks in Kernel Modules [J]	China Communications	2013, 10(11): 15-23	SCI收录	Tian Donghai, Li Xuanya, Hu Changzhen, et al
73	国外重要刊物	Insecurity of 'Improved Anonymous Multi-Receiver Identity-Based Encryption'	The Computer Journal	doi: 10.1093/comjnl/bxt052	SCI收录	Huaqun Wang
74	国外重要刊物	Signer-admissible strong designated verifier signature from bilinear pairings	Security and Communication Networks	DOI: 10.1002/sec.805	SCI收录	Huaqun Wang
75	国外重要刊物	Cryptanalysis and Improvement of the Controlled Quantum Secure Direct Communication by Using Four Particle Cluster States	Int. J. Theor. Phys	DOI 10.1007/s10773-013-1949-9	SCI收录	ZhenChao Zhu, AiQun Hu and AnMin Fu
76	国外重要刊物	An Efficient Quantum Secure Dialogue Scheme without Information Leakage by Using Single Photons	2013 6th International Congress on Image and Signal Processing	(CISP 2013)	EI收录	ZhenChao Zhu, AiQun Hu and AnMin Fu
77	国内重要刊物	Permutation polynomials with low differential uniformity over finite fields of odd characteristic	Science China Mathematics	Vol. 56, No. 7, pp. 1429-1440, July 2013	EI收录	Wenjie Jia, Xiangyong Zeng*, Chunlei Li, Tor Helleseth, Lei Hu
78	国外重要刊物	A new construction of zero-difference balanced functions and its applications	IEEE Transactions on Information Theory	Vol.59, No.8, pp. 5008-5015, August 2013	SCI收录	Han Cai, Xiangyong Zeng*, Tor Helleseth, Xiaohu Tang, Yang Yang
79	国外重要刊物	Ancestor Excludable Hierarchical ID-Based Encryption Revisited. Network and System Security	Lecture Notes in Computer Science Volume 7873	2013, pp 663-670	EI收录	Fan Zhang, Hua Guo*, Zhoujun Li
80	国外重要刊物	Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks	Multimedia Systems	DOI: 10.1007/s00530-013-0346-9	SCI收录	Debiao He, Neeraj Kumar, Jianhua Chen, Cheng-Chi Lee, Naveen Chilamkurti, Seng-Soo Yeo
81	国外重要	Cryptanalysis and improvement of an anonymous authentication protocol for wireless access	Wireless Personal Communications	DOI: 10.1007/s11277-	SCI收	Debiao He, Yuanyuan Zhang, Jianhua

	刊物	networks		013-1282-x	录	Chen
82	国外重要刊物	Mixed Strategy Nash Equilibrium in the Camera Source Identification Game	in Proc. of 20th IEEE International Conference on Image Processing 2013 (ICIP2013), Melbourne, Australia, Sept. 2013	(ICIP2013)	EI收录	Hui Zeng, Xiangui Kang*, Jiwu Huang
83	国外重要刊物	Game Theoretic Analysis of Camera Source Identification	in Proc. of Asian-Pacific Signal and Information Processing Association Annual Submit Conference (APSIPA ASC) 2013, Taibei, Nov. 2013.	(APSIPA ASC) 2013	EI收录	Hui Zeng, Yunwen Jiang, Xiangui Kang*, Li Liu
84	国外重要刊物	The Game of Countering JPEG Anti-forensics Based on the Noise Level Estimation	in Proc. of Asian-Pacific Signal and Information Processing Association Annual Submit Conference (APSIPA ASC) 2013, Taibei, Nov. 2013.	(APSIPA ASC) 2013	EI收录	Yunwen Jiang, Hui Zeng, Xiangui Kang*, Li Liu
85	国外重要刊物	Performing Scalable Lossy Compression on Pixel Encrypted Images	The EURASIP Journal on Image and Video Processing	vol. 2013, pp.32-1~6, May 2013.	SCI收录	Xiangui Kang, Anjie Peng and Xianyu Xu, Xiaochun Cao,
86	国外重要刊物	Camera Source Identification Game with incomplete information	in Proc. of International Workshop on Digital-forensics and Watermarking	IWDW 2013, 2013/10/01-2013/10/03, Auckland, New Zealand, 2013	EI收录	Hui Zeng, Xiangui Kang
87	国内重要刊物	双素数Sidel'nikov序列的自相关函数	电子与信息学报	2013 Vol. 35 (11): 2602-2607	EI收录	岳 塑*，高军涛，谢 佳
88	国外重要刊物	Optical image encryption via ptychography	Opt. Lett	Vol. 38, Issue 9, pp. 1425-1427 (2013)	SCI收录	Y. Shi*, T. Li, Y. Wang, Q. Gao, S. Zhang, H. Li
89	国内重要刊物	Generalized ptchography with diverse probes	Chin. Phy. Lett	30(5): 054203 (2013)	SCI收录	Y. Shi*, Y. Wang, S. Zhang
90	国内重要刊物	Ptychographical Imaging Algorithm with a Single Random Phase Encoding	Chin. Phy. Lett	30(7): 074203 (2013).	SCI收录	Y. Shi*, Y. Wang, T. Li, Q. Gao, H. Wan, S. Zhang, Z. Wu
	国					

91	外重要刊物	Application of diffractive optical elements for controlling the light beam in ptychography	Opt. Eng	52(9): 091720 (2013)	SCI收录	Y. Wang, T. Li, Q. Gao, Y. Shi*
92	国内重要刊物	可见光域叠层成像中照明光束的关键参量研究	物理学报	62(6):064206 (2013)	SCI收录	王雅丽，史祎诗*，李拓，高乾坤，肖俊，张三国
93	国外重要刊物	Collision Attack on the Full Extended MD4 and Pseudo-preimage Attack on RIPEMD	Journal of Computer Science and Technology	28(1), pp. 129-143, 2013	SCI收录	Gaoli Wang *
94	国外重要刊物	Preimage and pseudo-collision attacks on step-reduced SM3 hash function	Information Processing Letters	113 (8), pp. 301-306, 2013	SCI收录	Gaoli Wang*, Yanzhao Shen
95	国外重要刊物	Pixel Group Trace Model-Based Quantitative Steganalysis of Multiple Least Significant Bits Steganography	IEEE Transactions on Information Forensics and Security	2013, 8(1): 216-228	SCI收录	Chunfang Yang, Fenlin Liu, Xiangyang Luo, Ying Zeng
96	国内重要刊物	一种基于图像边缘的鲁棒水印算法	中国科学: 信息科学	2013, 43(11): 1410-1430	其他收录	巩道福, 刘粉林, 罗向阳
97	国外重要刊物	Fusion of Two Tpyical Quantitative Steganalysis Based on SVR	Journal of Software	8(3): 731-736, 2013	EI收录	Chunfang Yang, Fenlin Liu, Xiangyang Luo, Ying Zeng
98	国外重要刊物	Embedding Change Rate Estimation Based on Ensemble Learning	Proceedings of the ACM Workshop on Information Hiding and Multimedia Security	2013, pp.77-83	EI收录	Zhenyu Li, Zongyung Hu, Xiangyang Luo, Bin Lu
99	国外重要刊物	A System for Extracting and Ranking Name Aliases in Emails	Journal of Software	2013, 8(3): 737-745	EI收录	Meijuan Yin, Xiaonan Liu, Junyong Luo, Xiangyang Luo
##	国外重要刊物	The weight enumerators of three families of cyclic codes	IEEE Trans. Inform. Theory	vol.59, no.9, Sept. 2013, pp. 6002-6009	SCI收录	Z.C. Zhou*, C. Ding, J. Luo, and A.X. Zhang
##	国外重要刊	Seven classes of three-weight cyclic codes	IEEE Transactions on Communications	Vol. 61, No.10, Oct. 2013, pp. 4120-4126	SCI收录	Z.C. Zhou* and C. Ding

	物					
##	国外重要刊物	New classes of optimal frequency hopping sequences with low hit zone	Adv. Math. Communi	vol. 7, no. 2, 2013	SCI收录	X. Niu, D.Y. Peng, and Z.C. Zhou
##	国外重要刊物	Five Families of Three-Weight Ternary Cyclic Codes and Their Duals	IEEE Transactions on Information	Vol: 59 , Issue: 122013 , Page(s): 7940 - 7946	SCI收录	C. Ding*, Y. Gao, and,Z.C. Zhou
##	国内重要刊物	Formulations of Some Bit Switching Functions in DES	Wuhan University Journal of Natural Sciences	Vol.18, No.5, 2013	SCI收录	YOU Lin, YANG Yilin, WEN Wanli
##	国内重要刊物	IK-CPA security implies IE-CCA security in the random oracle model	SCIENCE CHINA Information Sciences	2013,56(3):1-11	SCI收录	Rui Xue（薛锐）
##	国外重要刊物	iBigTable:Practical Data Integrity for BigTable in Public	Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy	2013,341-352	EI收录	Wei Wei,Ting Yu、Rui Xue（薛锐）
##	国外重要刊物	Role-based and time-bound access and management of EHR data	Security and Communication Networks	2013,6(12)	其他收录	章睿,Liu Ling（2）薛锐（3）
##	国外重要刊物	Zero Knowledge Proofs from Ring-LWE	CANS 2013	LNCS 8257:57-73,2013	其他收录	谢翔,薛锐（2）王敏倩（3）
##	国内重要刊物	Reflections on the security proofs of Boneh-Franklin identity-based encryption scheme	SCIENCE CHINA MATHEMATICS	2013,56 (7):1385-1401	SCI收录	陈宇,Liqun Chen(陈利群) Dongdai Lin(林东岱)
##	国外重要刊物	Real time cryptanalysis of Bluetooth encryption with condition masking	Crypto2013,Springer verlag	LNCS vol.8042:165-182,2013	EI收录	张斌，徐超,冯登国（3）
##	国外重要刊物	A New Model for Error-Tolerant Side-Channel Cube Attacks	Workshop on Cryptographic Hardware and Embedded Systems 2013-CHES' 2013	LNCS，vol. 8086:453-470,2013	其他收录	李振琦,张斌,范俊峰（3）Ingrid Verbauwhede（4）
	国					

##	外重要刊物	Cryptanalysis of Helix and Phelix revisited	18th Australasian Conference on Information Security and Privacy-ACISP'2013	LNCS vol. 7959:27-40,2013	EI收录	石振青,张斌冯登国（3）
##	国外重要刊物	An Improved Twisted Ate Pairing over KSS Curves with $k=18$	Pairing-Based Cryptography – Pairing 2012	LNCS 7708:35–45 2013	其他收录	陈珊,王鲲鹏（2）林东岱（3）
##	国外重要刊物	Stronger Security Model for Public-Key Encryption with Equality Test	Pairing-Based Cryptography – Pairing 2013	2013,7708:65-82	其他收录	卢尧,张锐（2）林东岱（3）
##	国外重要刊物	Factoring RSA Modulus with Known Bits from Both p and q: A Lattice Method	Network and System Security - 6th International Conference	2013,7873:393–404	EI收录	卢尧,张锐（2）林东岱（4）
##	国外重要刊物	Factoring Multi-Power RSA Modulus N = prq with Partial Known Bits	18th Australasian Conference on Information Security and Privacy	2013,7959:57–71	EI收录	卢尧,张锐（2）林东岱（5）
##	国外重要刊物	Improved Bounds for The Implicit Factorization Problem	Advances in Mathematics of Communications	2013,7(3):243-251	SCI收录	卢尧,张锐（2）林东岱（6）
##	国外重要刊物	A New Method for Solving Polynomial Systems with Noise over F_2 and Its Applications in Cold Boot Key Recovery	SAC 2012, Revised Selected Papers	LNCS 7707:16-33,2013	EI收录	黄震宇,林东岱
##	国外重要刊物	A new algorithmic scheme for computing characteristic sets	Journal of Symbolic Computation,J SYMB COMPUT	2013,50:431–449	SCI收录	金萌,李晓亮（2）王东明（3）
##	国外重要刊物	Construction of Resilient and Nonlinear Boolean Functions with Almost Perfect Immunity to Algebraic and Fast Algebraic Attacks	Lecture Notes in Computer Science	2013,7763:276-293	EI收录	王天择,刘美成（2）林东岱（3）
##	国外重要刊物	Comments on "A design of Boolean functions resistant to (fast) algebraic cryptanalysis with efficient implementation"	Cryptography and Communications	2013,5(1):1-6	其他收录	王文浩、刘美成（2）张寅（3）
##	国外重要刊	On the immunity of rotation symmetric Boolean functions against fast algebraic attacks	Discrete Applied Mathematics	2013,162:17-27	EI收录	张寅,刘美成（2）林东岱（3）

	物						
##	国外重要刊物	Threshold visual secret sharing by random grids with improved contrast	Journal of Systems and Software ,J Syst Software	2013(86):2094–2109	SCI收录		郭腾,Feng Liu (刘峰), ChuanKun Wu (武传坤)
##	国外重要刊物	A method for counting the number of polynomial equivalence classes	Journal of Mathematical Cryptology	2013,7(1):69-95	其他收录		王天择,Dongdai Lin（林东岱）
##	国外重要刊物	Defending return-oriented programming based on virtualization techniques	SECURITY AND COMMUNICATION NETWORKS	2013,6(10):1236-1249	SCI收录		贾晓启,Rui Wang,Jun Jiang，Shengzhi Zhang， Peng Liu
##	国外重要刊物	Analysis of Multiple Checkpoints in Non-perfect and Perfect Rainbow Tradeoff Revisited	ICICS 2013,Springer论文集	8233LNCS:288-301,2013	其他收录		王文浩,林东岱
##	国内重要刊物	Making a Higher Hit Ratio Cryptanalytic Time-Memory Trade-Off Attack on Passwords	Chinese Journal of Electronics	2013,22(4):671-676	SCI收录		邹静（1）林东岱（2）郝春辉（3）李振奇（4）王文浩（5）卢尧（6）
##	国外重要刊物	View invariant action recognition using weighted fundamental ratios	Computer Vision and Image Understanding	2013,117(6):587-602	SCI收录		Nazim Ashraf,Yuping Shen（沈玉萍），Xiaochun Cao（操晓春）,Hassan Foroosh
##	国外重要刊物	Unified Dictionary Learning and Region Tagging with Hierarchical Sparse Representation	Computer Vision and Image Understanding	2013,117(8):934-946	SCI收录		Xiaochun Cao (操晓春）,Xingxing Wei（韦星星），Yahong Han（韩亚洪）, Yi Yang（杨毅）, Nicu Sebe, Alexander Hauptmann
##	国外重要刊物	Performing scalable lossy compression on pixel encrypted images	EURASIP JOURNAL ON IMAGE AND VIDEO PROCESSING	2013,32	SCI收录		Xiangui Kang（康先贵）,Anjie Peng（彭安杰），Xianyu Xu（徐先宇）, Xiaochun Cao（操晓春）
##	国外重要刊物	Geometric attack resistant image watermarking based on MSER	FRONTIERS OF COMPUTER SCIENCE	2013,7(1):145-156	SCI收录		Xuejuan Zhang（张雪娟）,Xiaochun Cao（操晓春），Jingjie Li（李靓蕾）

##	国外重要刊物	Lip segmentation and tracking under MAP-MRF framework with unknown segment number	NEUROCOMPUTING	2013,104(15):155-169	SCI收录	Yiu-ming Cheung（陈玉明）,Meng Li（李萌）, Xiaochun Cao（操晓春）
##	国外重要刊物	Video Editing with Temporal, Spatial and Appearance Consistency	Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition	2013:2283-2290	EI收录	Xiaojie Guo(郭晓杰）,Xiaochun Cao（操晓春）, Xiaowu Chen（陈小武）,Yi Ma（马毅）
##	国外重要刊物	Visual Saliency Detection Based on Photographic Composition	ACM International Conference Proceeding Series	2013:13-16	EI收录	Jingjing Chen（陈静静）,Handong Zhao（赵汉东）, Yahong Han（韩亚洪）, Xiaochun Cao（操晓春）
##	国外重要刊物	Horizon matters: Image re-targeting using horizon cues	Proceedings - IEEE International Conference on Multimedia and Expo	2013:1-6	EI收录	Xiaochun Cao (操晓春）,Feng Jiang（江峰）, Siyuan Li（李思远）, Xiaojie Guo（郭晓杰）
##	国外重要刊物	Saliency map fusion based on rank-one constraint	Proceedings - IEEE International Conference on Multimedia and Expo	2013:1-7	EI收录	Xiaochun Cao (操晓春）,Zhiqiang Tao（陶志强）, Bao Zhang（张宝）, Huazhu Fu（付华柱）, Xuewei Li（李雪威）
##	国外重要刊物	Robust Tensor Clustering with Non-Greedy Maximization	Proceedings of the Twenty-Third international joint conference on Artificial Intelligence	2013:1254-1259	其他收录	Xiaochun Cao (操晓春）,Xingxing Wei（韦星星）, Yahong Han（韩亚洪）,YiYang（杨毅）, Dongdai Lin（林东岱）
##	国外重要刊物	Object coding on the semantic graph for scene classification	MM 2013 - Proceedings of the 2013 ACM Multimedia Conference	2013:493-496	EI收录	Jingjing Chen（陈静静）,Yahong Han（韩亚洪）, Xiaochun Cao（操晓春）, Qi Tian（田琦）
##	国外重要刊物	Motion Matters: A Novel Framework for Compressing Surveillance Videos	MM 2013 - Proceedings of the 2013 ACM Multimedia Conference	2013:549-552	EI收录	Xiaojie Guo(郭晓杰）,Siyuan Li（李思远）, Xiaochun Cao（操晓春）
	国外					

##	重要刊物	The non-existence of permutations EA-equivalent to certain AB functions	IEEE Transactions on Information Theory	2013,59(1):672-679	SCI收录	李永强
##	国内重要刊物	Constructing Differentially 4 Uniform Permutations from Known Ones	Chinese Journal of Electronics	2013,22(3):495-499	SCI收录	Yuyin Yu (余玉银),MMingsheng Wang (王明生)，Yongqiang Li (李永强)
##	国外重要刊物	Permutation polynomials and their differential properties over residue class rings	Discrete Applied Mathematics	2013,161 (18):3104-3108	EI收录	Yuyin Yu (余玉银),MMingsheng Wang (王明生)，Yongqiang Li (李永强)
##	国内重要刊物	On Annihilators in Fewer Variables: Basic Theory and Applications	Chinese Journal of Electronics	2013,22(3):489-494	SCI收录	Lin Jiao (矫琳),Yongqiang Li (李永强), Meicheng Liu (刘美成)
##	国外重要刊物	Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions	Lecture Notes in Computer Science	7707 LNCS:355-371,2013	EI收录	Shengbao Wu (吴生宝),Wenling Wu (吴文玲)
##	国外重要刊物	Integral Attacks on Reduced-Round PRESENT	Lecture Notes in Computer Science	8233 LNCS:331–345	其他收录	Shengbao Wu (吴生宝)
##	国外重要刊物	Leaked-State-Forgery Attack Against The Authenticated Encryption Algorithm ALE	Lecture Notes in Computer Science	8269 LNCS:377-404,2013	其他收录	Shengbao Wu (吴生宝),Hongjun Wu, Tao Huang, Mingsheng Wang (王明生), Wenling Wu (吴文玲)
##	国外重要刊物	An improved time-memory-data trade-off attack against irregularly clocked and filtered keystream generators	Lecture Notes in Computer Science	7763 LNCS:294-310,2013	EI收录	Lin Jiao (矫琳),Mingsheng Wang (王明生), Bin Zhang (张斌), Yongqiang Li (李永强)
##	国外重要刊物	A Generic Framework for Anonymous Authentication in Mobile Networks	Journal of Computer Science and Technology ,J Comput Sci Technol	2013,28(4):732-742	SCI收录	徐静,Wentao Zhu（朱文涛）
##	国外重要刊物	Efficient identity-based strong designated verifier signature schemes	Security and Communication Networks	2013,6(7):902-911	SCI收录	段美娇,徐静（2）冯登国（3）
##	国内重要	Design and Implementation of a Context-based Android Mobile Terminal Trusted Running Control	北京交通大学学报：自然科学版	2013,37(5):100-104	其他收	曲海鹏,敖赢戈，晏敏，于

	刊物	System			录	爱民，赵保华
##	国外重要刊物	ChainDroid：Safe and Flexible Access to Protected Android Resources Based on Call Chain	The 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications	2013:156-162	其他收录	周启惠（1）汪丹（2）
##	国外重要刊物	An efficient method for computing comprehensive Gröbner bases	Journal of Symbolic Computation	2013,52:124-142	SCI收录	Deepak Kapur,Dingkang Wang（王定康）
##	国外重要刊物	An efficient algorithm for computing a comprehensive Groebner system of a parametric polynomial system	Journal of Symbolic Computation	2013,56(6):1155-1168	SCI收录	Deepak Kapur,Dingkang Wang（王定康）
##	国内重要刊物	A signature-based algorithm for computing Grobner basis in solvable polynomial algebras	Science China, Mathematics	2013:351-358	EI收录	孙瑶
##	国外重要刊物	A new proof for the correctness of the F5 algorithm	International Symposium on Symbolic and Algebraic Computation	2013,56(4):745-756	SCI收录	孙瑶,Dingkang Wang（王定康）
##	国外重要刊物	Video steganography with multi-path motion estimation	SPIE Conf. Electronic Imaging -- Media Watermarking, security, and Forensics	2013:8665	EI收录	曹纭,X.ZHAO（赵险峰）、F.LI（李凤华）、N.YU（俞能海）
##	国内重要刊物	基于拟合盲隐写分析结果的隐写隐蔽性组合测评方法	第十一届全国信息隐藏暨多媒体信息安全学术大会	2013:358-364	其他收录	Bingbing Xia(夏冰冰),Xianfeng Zhao(赵险峰)、Hong Zhang(张弘)
##	国内重要刊物	基于特征融合聚类的JPEG盲隐写分析	计算机应用与软件	2013,30(3):7–9	其他收录	周楠,赵险峰, 黄炜, 盛任农
##	国内重要刊物	基于组合线性最小二乘回归的盲定量隐写分析	计算机应用与软件	2013,30(8):7–9	其他收录	张纪宇 ,赵险峰, 黄炜, 盛任农
##	国内重要刊物	基于改变率自适应分类的多类隐写分析	计算机应用与软件	2013,30(6):7–9	其他收录	安宁钰 ,赵险峰, 黄炜, 盛任农
	国					CHEN Kai（陈

##	外重要刊物	Vulnerability-based Backdoors: Threats From Two-steps Trojans	The 7th International Conference on Software Security and Reliability	2013:169 - 177	EI收录	恺）,ZHANG Yingjun（张颖君）, LIAN Yifeng（连一峰）
##	国外重要刊物	VulLocator: Automatically locating vulnerable code in binary programs	9th International Conference on Information Security Practice and Experience	2013:295-308	EI收录	ZHANG Yingjun,CHEN Kai（陈恺）, LIAN Yifeng
##	国外重要刊物	Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption	Information Forensics and Security, IEEE Transactions on	2013,8(3):553 - 562	SCI收录	Ma, K.,Weiming Zhang; Xianfeng Zhao（赵险峰） ; Nenghai Yu; Fenghua Li（李凤华）
##	国外重要刊物	Fast Estimation of Optimal Marked-Signal Distribution for Reversible Data Hiding	Information Forensics and Security, IEEE Transactions on	2013,8(5):779 - 788	SCI收录	Xiaocheng Hu,Weiming Zhang ; Xuexian Hu ; Nenghai Yu ; Xianfeng Zhao（赵险峰） ; Fenghua Li（李凤华）
##	国外重要刊物	Improving the Embedding Efficiency of Steganography with Reduced Covering Set	The Second Cross-Straits Conference on Information Security	2013:1-6	其他收录	bingbing Xia(夏冰冰),赵险峰
##	国外重要刊物	Blackdroid: A black-box way for Android plaintext and ciphertext privacy leaks detecting and guarding	International Conference on Consumer Electronics, Communications and Networks	2013	其他收录	张妍,Ruoding Zhang, Qihui Zhou,Yazhe Wang,Dan Wang
##	国外重要刊物	Keystroke Timing Analysis of on-the-fly Web Apps.	ACNS 2013	Applied Cryptography and Network Security Lecture Notes in Computer Science Volume 7954:405-413	EI收录	Chee Meng Tey,Payas Gupta, Debin Gao, Yan Zhang.
##	国外重要刊物	Forgeability of Wang-Zhu-Feng-Yao's Attribute-Based Signature with Policy-and-Endorsement Mechanism	Journal of Computer Science and Technology	2013,28(4):743-748	其他收录	Aijun Ge (葛爱军),Xin-Yi Huang (黄欣沂), Cheng Chen (陈成), Rui Zhang (张锐)
##	国外重要刊物	A Collusion-Resistant Conditional Access System for Flexible-Pay-Per-Channel Pay-TV Broadcasting	IEEE Transactions on Multimedia	2013,15(6):1353-1364	SCI收录	Zhiguo Wan,Jun Liu, Rui Zhang, Robert H. Deng
##	国外重要刊物	Security Analysis of a Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption Scheme	IEEE Transactions on Parallel and Distributed Systems	2013,24(11):2319-2321	SCI收录	Aijun Ge,Jiang Zhang, Rui Zhang, Chuangui Ma, Zhenfeng Zhang

##	国外重要刊物	EMD-Based Denoising for Side-Channel Attacks and Relationships between the Noises Extracted with Different Denoising Methods	ICICS 2013	LNCS 8233:259–274	其他收录	Mingliang Feng1（冯明亮）,Zhenmei Yu
##	国外重要刊物	Systematic Construction and Comprehensive Evaluation of Kolmogorov-Smirnov Test Based Side-Channel Distinguishers	ISPEC 2013	LNCS 7863:336–352	EI收录	Hui Zhao（赵辉）,François-Xavier Standaert, Hailong Zhang
##	国外重要刊物	Security and Improvement of an Authenticated Group Key Transfer Protocol Based on Secret Sharing	Applied Mathematics & Information Sciences	2013,7(5):1943-1949	SCI收录	袁巍,胡亮，李宏图，初剑峰
##	国外重要刊物	A Topology Hidden Anonymous Multicast Routing for Ad Hoc Networks	globecom2013	2013	其他收录	袁巍,胡亮，杨鲲
##	国外重要刊物	Efficient Deterministic Anchor Deployment for Sensor Network Positioning	International Journal of Distributed Sensor Networks	Vol.2013	SCI收录	陈永乐,陈祠（2）朱红松（3）孙利民（4）
##	国外重要刊物	Amortized Fairness for Drive-Thru Internet	International Journal of Distributed Sensor Networks	Vol.2013	SCI收录	李志（1）孙利民（2）周新运（3）
##	国外重要刊物	Mo-Fi: Discovering Human Presence Activity with Smartphones Using Non-intrusive Wi-Fi Monitors	the 6th IEEE International Conference on Cyber, Physical and Social Computing	Vol.2013	其他收录	秦伟俊,朱红松（2）张佳棣（3）李波（4）
##	国外重要刊物	Context-aware Handoff on Smartphones	MASS2013,IEEE 论文集	2013:470 - 478	其他收录	李强（1）韩琪（2）孙利民（3）
##	国外重要刊物	Domino of the Smart Grid: An Empirical Study of System Behaviors in the Interdependent Network Architecture	SmartGridComm2013 论文集	2013:612-617	其他收录	芦翔（1）,王文野（2）马建峰（3）孙利民（4）
##	国外重要刊物	Adaptive Computing Resource Allocation for Mobile Cloud Computing	International Journal of Distributed Sensor Networks	2013	EI收录	Hongbin Liang (1),Tianyi Xing (2)Lin Cai（3） Dijiang Huang（4） Daiyuan Peng（5）
##	国内重要	基于SMDP的无线多媒体服务自适应信道优化分配	第七届中国传感器网络学术会议	2013	其他收	梁宏斌(1) ,彭代渊

	刊物				录	
##	国内重要刊物	a line of sight fingerprint localization algorithm resisting multipath and shadow	计算机研究与发展	2013,50(3):524-531	EI收录	陈永乐,朱红松（2）孙利民(3)
##	国外重要刊物	MERPL:A More Memory-efficient Storing Mode in RPL	IEEE ICON 2013	2013	其他收录	甘伟（1）,石志强，孙利民，Dan Ionescu
##	国内重要刊物	Adaptive TDMA Slot Assignment Protocol for Vehicular Ad Hoc Networks	中国邮电高校学报（英文版	2013,20(1):11-18	EI收录	杨卫东,李攀，刘燕，朱红松
##	国内重要刊物	车载自组网节点轨迹隐私攻防博弈模型	通信学报	2013,34(z1):240-245	其他收录	杨卫东,何云华，孙利民 朱红松
##	国内重要刊物	An efficient algorithm for factoring polynomials over algebraic extension field	Science China, Mathematics	2013,56(6):1155-1168	SCI收录	Yao Sun (孙瑶）
##	国内重要刊物	细粒度超媒体描述模型及其使用机制	通信学报	2013, 08, 34(z1): 223-229	EI收录	苏铓, 李凤华, 史国振, 申莹, 黄琼, 王苗苗
##	国内重要刊物	基于行为的结构化文档多级访问控制	计算机研究与发展	2013, 07, 50(7): 1399-1408	EI收录	熊金波, 姚志强, 马建峰, 李凤华, 李琦
##	国外重要刊物	Certificateless public auditing for data integrity in the cloud	IEEE Conference on Communications and Network Security (CNS 2013),National Harbor, MD, USA.	2013.10. 136 - 144	EI收录	Boyang Wang, Baochun Li, Hui Li, Fenghua Li
##	国外重要刊物	FDR-ABE: Attribute-Based Encryption with Flexible and Direct Revocation	In Proceedings of the 5th International Conference on Intelligent Networking and Collaborative Systems. Xi’an, China	2013.09. 38-45	EI收录	Yinghui Zhang, Xiaofeng Chen, Jin Li, Hui Li, Fenghua Li
##	国外重要刊物	Improving the Message-Ciphertext Rate of Lewko’s Fully Secure IBE Scheme	ISPEC2013	LNCS 7863:105-116	EI收录	贾仃仃,李宝，刘亚敏、梅其祥
	国					

##	外重要刊物	RKA Secure PKE Based on the DDH and HR Assumptions	PROVSEC2013	LNCS 8209:271-287	EI收录	贾仃仃,路献辉、李宝、梅其祥
##	国外重要刊物	RSA-OAEP is RKA Secure	Inscrypt 2013	2013	EI收录	贾仃仃,李宝、路献辉、刘亚敏
##	国外重要刊物	Cryptanalysis of three Authenticated Encryption Schemes for Wireless Sensor Networks	Inscrypt 2013	INSCRYPT2013 论文集	EI收录	李晓千,王鹏、李宝、孙哲蕾
##	国外重要刊物	First Multidimensional Cryptanalysis on Reduced-Round PRINCEcore	ICISC2013	ICISC2013论文集	EI收录	李晓千,李宝、吴文玲、于晓丽、郝荣林、马冰珂
##	国外重要刊物	Efficient lossy trapdoor function based on subgroup membership assumptions	CANS2013	LNCS 8257:235-250	EI收录	薛海洋
##	国外重要刊物	How to Remove the Exponent GCD in HK09	PROVSEC2013	LNCS 8209:239-248	EI收录	路献辉,李宝、刘亚敏
##	国外重要刊物	About hash into Montgomery form elliptic curves	ISPEC 2013	Springer Verlag,LNCS 7863 :147-159	EI收录	于伟,王鲲鹏、李宝、田松
##	国外重要刊物	Joint triple-base number system for multi-scalar multiplication	ISPEC 2013	Springer Verlag,LNCS 7863 :160-173	EI收录	于伟,王鲲鹏、李宝、田松
##	国外重要刊物	On the expansion length of triple-base number systems	AFRICACRYPT 2013	Springer Verlag,LNCS 7918 :424-432	EI收录	于伟,王鲲鹏、李宝、田松
##	国外重要刊物	Triple-base number system for scalar multiplication	AFRICACRYPT 2013	Springer Verlag,LNCS 7918 :433-451	EI收录	于伟,王鲲鹏、李宝、田松
##	国内重要刊	基于部分信息泄露的Hensel提升计算问题	计算机工程 国内	2013,39(8):38-43	其他收录	臧统政

	物					
##	国外重要刊物	New Results on the Hardness of ElGamal and RSA Bits Basing on Binary Expansions	CSAE 2013	Proceedings of 2013 IEEE International Conference on Computer Science and Automation Engineering :518-522	EI收录	康镇麒
##	国内重要刊物	类背包DH问题的比特安全性研究	第28次计算机安全学术交流会 国内会议	信息网络安全,(10):121-123	其他收录	李伟
##	国外重要刊物	The Hidden Number Problem of Least Significant Bits	ICCT2013	WIT Transactions on Information and Communication Technologies	EI收录	康镇麒
##	国内重要刊物	谈谈隐藏数问题	中国密码学会通讯	(2):18-23	EI收录	吕克伟
##	国外重要刊物	Security concerns in popular cloud storage services	IEEE PERVASIVE COMPUTING 国际	2013,12(4):50-57	SCI收录	Chu, Cheng-Kang,朱文涛、Han,Jin、Liu,Joseph K、Xu,Jia、Zhou,Jianying
##	国外重要刊物	Preserving user privacy in the smart grid by hiding appliance load characteristics	CSS2013	LNCS 8300:67-80	EI收录	葛宝生,朱文涛
##	国外重要刊物	Towards secure and communication-efficient broadcast encryption systems	JOURNAL OF NETWORK AND COMPUTER APPLICATIONS 国际	2013,36(1):178-186	SCI收录	朱文涛
##	国外重要刊物	Cryptanalysis of the OKH Authenticated Encryption Scheme	ISPEC 2013	LNCS 7863:353-360	EI收录	王鹏,Wenling Wu, Liting Zhang
##	国外重要刊物	Collision Attacks on Variant of OCB Mode and Its Series	Inscrypt 2012	LNCS 7763:216-224	EI收录	孙哲蕾,Peng Wang, Liting Zhang
##	国外重要刊物	Public Verification of Outsourced Computation of Polynomial Functions	TrustCom2013	2013,776-780	EI收录	李佩丽

##	国外重要刊物	Homomorphic Signatures for Correct Computation of Group Elements	EIDWT2013	2013,66-71	EI收录	李佩丽
##	国内重要刊物	Instance-Dependent Commitment and Its Non-Malleability	Chinese Journal of Electronics 国际	2013,22(1):181-186	SCI收录	景文盼,李宝
##	国内重要刊物	Statistically Binding Non-Interactive Non-Malleable Commitment	中国科学院研究生院学报 国内	2013,30(2):264-271	其他收录	黄桂芳,胡磊
##	国内重要刊物	基于动态密钥的Android 短信加密方案	中国科学院研究生院学报 国内	2013,30(2):272-277	其他收录	李昭,王跃武，雷灵光，张中文
##	国外重要刊物	MJBlocker: A Lightweight and Run-time Malicious JavaScript Extensions Blocker	SERE2013	119-128	EI收录	王平建,向继，刘鹏，高能，荆继武
##	国外重要刊物	A High-Throughput SHA-1 Implementation on FPGA	ICCT2013		其他收录	王平建,潘无穷，向继
##	国外重要刊物	High Radix Montgomery Modular Multiplier on Modern FPGA	TrustCom2013		其他收录	王平建,刘宗斌，高能
##	国外重要刊物	Optimizing the Performance of Machine Learning Based Traffic Classification	Advanced Materials Research 国际	756-759:3506-3510	EI收录	王秋晨,向继
##	国内重要刊物	基于RFID的移动存储设备安全管控方案	第二十八次全国计算机安全学术交流会 国内会议	信息网络安全,(10):65-68	其他收录	王秋晨,王雷，夏鲁宁
##	国外重要刊物	Time Evolving Graphical Password for Securing Mobile Devices	ASIACCS 2013	347-352	EI收录	王展,荆继武、李亮
##	国外重要	Verification of Data Redundancy in Cloud Storage	Cloud Computing 2013	41961	EI收	王展,Kun Sun, Sushil Jajodia,荆

	刊物				录	继武
##	国外重要刊物	TerraCheck: Verification of Dedicated Cloud Storage	DBSec 2013	LNCS 7964:113-127	EI收录	王展,Kun Sun, Sushil Jajodia，荆继武
##	国外重要刊物	Reducing Attack Surface with VM-based Phantom Server	MILCOM 2013	1429-1434	其他收录	Li Wang,Kun Sun, Sushil Jajodia
##	国外重要刊物	A High-Speed Elliptic Curve Cryptographic Processor for Generic Curves over GF(p)	SAC2013	2013	EI收录	马原,刘宗斌，潘无穷，荆继武
##	国外重要刊物	Leakage-resilient zero knowledge proofs of knowledge for NP	NSS2013	LNCS 7873:365-380	EI收录	李红达,牛其华、梁蓓
##	国外重要刊物	Leakage-resilient proxy signatures	INCoS2013	IEEE Computer Society:495-502	EI收录	唐飞,李红达、牛其华、梁蓓
##	国外重要刊物	ID-Based signcryption with restrictive unsigncryption	INCoS2013	IEEE Computer Society:485-489	EI收录	唐飞,林昌露、李红达
##	国外重要刊物	A Threat to Mobile Cyber-physical Systems: Sensor-based Privacy Theft Attacks on Android Smartphones	TrustCom2013	126-133	EI收录	雷灵光,周健、查达仁、张中文
##	国外重要刊物	Formal Analysis of Dynamic Domain Establishment Protocol in Cloud Logging Service	EWDC2013	LNCS 7869:24-38	EI收录	胡伟
##	国内重要刊物	基于信息流模型的TCB完整性策略分析方法与工具	《武汉大学学报》(自然科学版) 国内	2013,59(7): 431-437	其他收录	胡伟
##	国外重要刊物	From Mini House Game to Hobby-driven Behavioral Biometrics-based Password	TrustCom2013	712-719	EI收录	江伟玉,,向继，刘丽敏，查达仁，王雷 刘丽敏 管乐 荆继武
	国内				其	

##	重要刊物	面向云存储的访问控制服务研究	第二十八次全国计算机安全学术交流会 国内会议	2013, (10):1671-1121	他收录	江伟玉,,刘丽敏查达仁
##	国外重要刊物	Fingerprint Embedding: A Proactive Strategy of Detecting Timing Channels	ICICS2013	LNCS8233:229-244	EI收录	汪婧,刘鹏刘丽敏管乐荆继武
##	国外重要刊物	A New Group Key Agreement Protocol with Anonymous	ICCAAE 2013	380-384:595-600	EI收录	姚刚,郭丽
##	国外重要刊物	Protocols for Message Authentication from a Weak Secret	ICCAAE 2013	380-384:590-594	EI收录	郭丽,姚刚
##	国外重要刊物	Full quantum treatment of Rabi oscillation driven by a pulse train and its application in ion-trap quantum computation	IEEE Journal of Quantum Electronics 国际	2013,49(8):641-651	SCI收录	杨理,杨碧瑶、陈玉福
##	国内重要刊物	Quantum probabilistic encryption scheme based on conjugate coding	China Communication 国际	2013,10(2):19-26	SCI收录	杨理,向憧、李宝
##	国内重要刊物	On a class of quantum Turing machine halting deterministically	Sci China-phys Merch Astron	2013,56(5):941-946	SCI收录	梁敏
##	国内重要刊物	联合调制量子密钥分配系统	物理学报 国内	2013,63 (13):130303-1—130303-7	SCI收录	郭邦红,向憧、关翀、吴令安、刘颂豪
##	国内重要刊物	量子动态口令认证方案	中国科学院研究生院学报 国内	2013,30(1):131-136	其他收录	李昭,周瑞瑞
##	国外重要刊物	Impossibility of finding any third family of server protocols integrating Byzantine quorum systems with threshold signature schemes	SECURITY AND COMMUNICATION NETWORKS 国际	2013,6(5):612-630	SCI收录	林璟锵,Peng Liu，荆继武，王琼霄
##	国外重要刊物	Automatic Security Evaluation of Block Ciphers with S-bP Structures against Related-key Differential Attacks	Inscrypt 2013	LNCS	EI收录	孙思维,胡磊、宋凌、解永宏、王鹏

##	国外重要刊物	Differential Fault Attack on the PRINCE Block Cipher	LightSec 2013	LNCS 8162 :43-54	EI收录	宋凌,胡磊
##	国外重要刊物	Improved algebraic and differential fault attacks on the KATAN block cipher	ISPEC 2013	LNCS 7863 :372-386	EI收录	宋凌,胡磊
##	国外重要刊物	Analysis of two knapsack public key cryptosystems	IET Communications 国际	2013,7(5):1638-1643	SCI收录	彭力强,胡磊、许军、解永宏
##	国外重要刊物	New Optimal Frequency Hopping Sequence Sets from Balanced Nested Difference Packings of Partition-Type	International Journal of Foundations of Computer Science 国际	2013,24(4):533-545	SCI收录	Han Cai, 曾祥勇、唐小虎、胡磊
##	国内重要刊物	Periods of Polynomials over a Galois Ring	SCIENCE CHINA-MATHEMATICS 国际	2013,56(9):1761-1772	SCI收录	张晓磊,胡磊
##	国内重要刊物	Galois 环上极大周期序列的平移等价	应用数学学报 国内	2013,36(4):646-655	其他收录	张晓磊,胡磊
##	国外重要刊物	A rational secret sharing protocol with unconditional security in the synchronous setting	18th Australasian Conference on Information Security and Privacy 国际会议	LNCS 7959:403－418	EI收录	俞扬,周展飞
##	国外重要刊物	Rational Secret Sharing Information-Theoretically Secure against Adaptive Adversaries	12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) 国际会议	249-256	EI收录	俞扬,周展飞
##	国外重要刊物	Rational Secret Sharing Eliminates Incredible Threat in Standard Communication Network	2nd International Conference on Computer Science and Network Technology 国际会议	358-362	SCI收录	孙富玲,周展飞
##	国内重要刊物	Rational secret sharing protocol in the context of extensive game with imperfect information	中国科学院大学学报 国内	2013,30(4):539-546	其他收录	孙富玲,周展飞、俞扬
##	国内重	Security Analysis and Improvement of an Authentication	第28次全国计算机安全学术交流会 国内会	信息网络安	其他	秦文仙,王琼霄、高能、王

	要刊物	Protocal for SIP	议	全,2013,(10):5-7	收录	跃武
##	国内重要刊物	Research on Authentication Mechanisms in Cloud Computing	第28次计算机安全学术交流会 国内会议	信息网络安全,2013,(10)54-56	其他收录	朱荣华,高能、向继
##	国内重要刊物	Data Security Technology Development Report	第二十三届全国信息保密学术会议 国内会议	保密科学技术,(9):1-31	其他收录	高能,荆继武、马存庆、余幸杰
##	国外重要刊物	An Efficient Reconfigurable II-ONB Modular Multiplier	9th International Conference on Security and Privacy in Communication Networks 国际会议	2013	EI收录	李淼,何良生，杨同杰，高能，刘宗斌，章庆隆

电话：010-82546611 传真：010-82546564
地址：北京市海淀区闵庄路甲89号 100093