信息安全国家重点实验室2012年论文专著

2013-02-22 | 小 中 大 【关闭窗口】

序号	论文作者	论文名称	出版社名称 卷、期、页
1	Xiangyong Zeng, Jinyong Shan, and Lei Hu	A Triple-Error-Correcting Cyclic Code from the Gold and Kasami-Welch APN Power Functions	Finite Fields and Their Applications 18、1、70-92
2	Xiwang Cao, Lei Hu	On the reducibility of some composite polynomials over finite fields	Designs, Codes and Cryptography (DCC) 66、3、229-239
3	Zhengbang Zha, Lei Hu	Two Classes of Permutation Polynomials over Finite Fields	Finite Fields and Their Applications 18、4、781-790
4	W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao	Detecting node replication attacks in mobile sensor networks: Theory and approaches	Security and Communication Networks 5、5、496--507
5	W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao	Detecting node replication attacks in wireless sensor networks: A survey	Journal of Network and Computer Applications, Elsevier 35、3、1022--1034
6	W. T. Zhu	A comment on `MABS: Multicast authentication based on batch signature’	IEEE Transactions on Mobile Computing 11、11、1775--1776
7	Zhou Rui-Rui, Yang Li	Quantum election scheme based on anonymous quantum key distribution	中国物理B 2012,8:23-30
8	Liang Min, Yang Li	Public-key encryption and authentication of quantum information	SCIENCE CHINA physics,Mechanics&Astronomy 55、9、1618-1629
9	张斌，冯登国	改进的多步法快速相关	中国科学E辑 2012-

		攻击及其应用	04，469-483
10	X.D. Ma, Y. Sun and D.K. Wang	Computing Polynomial Univariate Representations of Zero-dimensional Ideals by Groebner Basis.	Science in China, Series A: Mathematics Vol. 55, No. 6, 1293-1302
11	1Jikai Teng,2Chuankun Wu	A provable authenticated certificateless group key agreement with constant rounds	Journal of Communications and Networks 14,1,104-110
12	1Hui Li, 2 Chuan-Kun Wu	CMQV+: An authenticated key exchange protocol from CMQV	Science China Information Sciences 55 7 1666-1674
13	1TENG Jikai，2 WU Chuankun，3 TANG Chunming(唐春明)	An ID-based authenticated dynamic group key agreement with optimal round	Science China Information Sciences 55 11 2542-2554
14	Jinwang Liu, Mingsheng Wang	New results on multivariate polynomial matrix factorizations	Linear algebra and its applications 438, 87-95
15	1Yun Cao, 2 Xianfeng Zhao，3 Dengguo Feng	Video steganalysis exploiting motion vector reversion-based features	IEEE Signal Processing Letters 19(1): 35-38
16	Liting Zhang,?Wenling Wu,?Peng Wang	Bo Liang:TrCBC: Another look at CBC-MAC	Information Processing Letters Volume 112(7): 302-307
17	Rui Zhang	Role-Based and Time-Bound Access and Management of EHR Data	Security and Communication Networks Networks 0000; 00:1–21
18	黄震宇	Parametric equation solving and quantifier elimination in finite fields with the characteristic set method	Journal of Systems Science and Complexity J Syst Sci Complex (2012) 25: 778–791
19	Liqun Chen, Yu Chen	The n-Diffie-Hellman problem and multiple-key encryption	International Journal of Information Security Vol. 11, No.5, 2012, pp. 305-320.

20	1Aijun Ge, 2 Chuangui Ma，3 Zhenfeng Zhang	Attribute-based signature scheme with constant size signature in the standard model	IET Information Security 6(2):47-54
21	Feng Liu, Teng Guo, Chuankun Wu and Lina Qian	Improving the Visual Quality of Size Invariant Visual Cryptography Scheme	Journal of Visual Communication and Image Representation Volume 23, Page 331-342
22	1 Meng Jin , 2 Xiaoliang Li, 3 Dongming Wang	A new algorithmic scheme for computing characteristic sets	Journal of Symbolic Computation 2013, 431－449
23	CHEN Kai, FENG Dengguo, SU Purui, ZHANG Yingjun	Black-box testing based on colorful taint analysis	Sci China Inf Sci 2012, 55: 171－183
24	Li Hongda, Feng Dengguo, Li Bao, Xu Haixia	Round-Optimal Zero-Knowledge Proofs of Knowledge for NP	Science China Information Sciences, 2012, 55 (11):2473-2484
25	Fangjun Huang，Jiwu Huang，Yun-Qing Shi	New channel selection rule for JPEG steganography	IEEE Transactions on Information Forensics and Security 2012，7（4）：1181-1191
26	Lin Dongdai，Faugère, Jean-Charles， Perret, Ludovic; Wang, Tianze	On enumeration of polynomial equivalence classes and their application to MPKC	Finite Fields and their Applications 2012.3,2（18）：283-302
27	Lin Dongdai，Shi Tao，Yang，Zifeng	Ergodic theory over F2 [T]	Finite Fields and their Applications 2012.5，Vol 18，Issue 3:473-491
28	Xiyong Zhang, Xiwang Cao, Rongquan Feng	A method of evaluation of exponential sum of binary quadratic functions,	Finite Fields and Their Applications 2012，18(6), pp 1089-1103
29	Peipei Wang, Xiwang Cao, Rongquan Feng	On the existence of some specific elements in finite fields of characteristic 2	Finite Fields and Their Applications, 2012，18(4)：800-813
30	Liu, Lili; Cao, Tianjie; Lu, Yulong; Zhang, Hongtai	Analysis on the weighting factor of wavelet-based watermarking scheme	Journal of Computational Information Systems 201219（9）：4285-4292
31	Junhan YANG, Tianjie CAO	Provably Secure Three-party Password	Journal of Systems and Software 2012.2,

		Authenticated Key Exchange Protocol in the Standard Model	2(85): 340-350
32	Enes Pasalic,韦永壮	On the construction of Cryptographically Significant Boolean Functions Using Objects in Projective Geometry Spaces	IEEE Transactions on INFORMATION THEORY LNCS 7232、34-45
33	Xiaoni Du, Zhixiong Chen, Lei Hu	Linear complexity of binary sequences derived from Euler quotients with prime-power modulus	Information Processing Letters 112、604-609
34	YANG Yang, ZENG Guang, JIN ChengHui,QU YunYing	New application methods for word-oriented cryptographic primitives	SCIENCE CHINA Information Sciences Vol 55, No 9, 2149-2160, 2012
35	Xiaoni Du, Andrew Klapper and Zhixiong Chen	Linear complexity of pseudorandom sequences generated by Fermat quotients and their generalizations	Information Processing Letters 2012, 112 (6): 233-237.
36	Chenhuang Wu, Zhixiong Chen and Xiaoni Du.	Binary Threshold Sequences Derived from Carmichael Quotients with Even Numbers Modulus.	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 2012, E95-A(7): 1197-1199.
37	WANG Xiang-yang, NIU Pan-pan, YANG Hong-ying, CHEN Li-li.	Affine invariant image watermarking using intensity probability density-based Harris Laplace detector	Journal of Visual Communication and Image Representation 2012, 23(6): 892-907
38	Hong-Ying Yang, Xiang-Yang Wang	LS-SVM based Image Segmentation Using Color and Texture Information.	Journal of Visual Communication and Image Representation 2012, 23(7): 1095-1112.
39	Shuhua Wu,Qiong Pu,Shengbao Wang,Debiao He	Cryptanalysis of a communication-efficient three-party password authenticated key exchange protocol	Information Sciences 2012,215:83-96
40	Hu Xiong, Xiaofeng Wang,	Security Flaw of an improved user	IEICE Transactions on Fundamentals of

	Fagen Li	authentication scheme with user anonymity for wireless communications	Electronics, Communications and Computer Sciences, Vol. E95-A, No. 1, pp. 256-258, 2012
41	项世军，杨建权，黄继武	抗几何失真的视频哈希算法研究	中国科学 2012,42（5）：578-587
42	Shengli Liu, Kefei Chen	Homomorphic Linear Authentication Schemes from epsilon-ASU2 Functions for Proofs of Retrievability	Control & Cybernetics Journal Vol. 42, No. 2, pp. 900-916
43	Wei-Wei Zhang, Dan Li, Ke-Jia Zhang, Hui-Juan Zuo	A quantum protocol for millionaire problem with Bell states	Quantum Information Processing (Online) DOI 10.1007/s11128-012-0520-6
44	Wei-Wei Zhang, Fei Gao, Bin Liu, Qiao-Yan Wen, Hui Chen	A watermark strategy for quantum images based on quantum Fourier transform	Quantum Information Processing (Online) DOI 10.1007/s11128-012-0423-6
45	Wei-Wei Zhang, Fei Gao, Bin Liu, Qiao-Yan Wen, Hui Chen	A Quantum Watermark Protocol. International Journal of Theoretical Physics	International Journal of Theoretical Physics 2012. 52(2): p. 504-513
46	Bin Liu, Fei Gao, Wei Huang, Qiao-yan Wen	Multiparty quantum key agreement with single particles	Quantum Information Processing (Online) DOI 10.1007/s11128-012-0492-6
47	Bin Liu, Fei Gao, Heng-Yue Jia, et al	Efficient quantum private comparison employing single photons and collective detection	Quantum Information Processing DOI 10.1007/s11128-012-0439-y
48	Wei-Wei Zhang • Ke-Jia Zhang	Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party	Quantum Information Processing (Online) DOI 10.1007/s11128-012-0507-3
49	Bin Liu, Fei Gao, and Qiao-Yan Wen	Eavesdropping and Improvement to Multiparty Quantum Secret Sharing with Collective Eavesdropping-Check	International Journal of Theoretical Physics 2012. 51(4): p. 1211-1223
50	Su-Juan Qin	Reexamining the Security of Controlled Quantum	International Journal of Theoretical Physics 2012,

		Secure Direct Communication by Using Four Particle Cluster States	51:2714 - 2718
51	Hu Xiong, Zhong Chen, Fagen Li	Provably Secure and Efficient Certificateless Authenticated Tripartite Key Agreement Protocol	Mathematical and Computer Modelling, Elsevier Press, 55 (3-4): 1213-1221, 2012
52	Hu Xiong, Zhiguang Qin, Fagen Li	New Identity-based Three-party authenticated key agreement protocol with Provable Security, Journal of Network and Computer Applications	Elsevier Press, in press
53	Hu Xiong, Guobin Zhu, Zhong Chen, Fagen Li	Efficient communication scheme with confidentiality and privacy for vehicular networks	Computers and Electrical Engineering，Elsevier Press
54	Hu Xiong, Zhong Chen, Fagen Li	Efficient and Multi-level Privacy-Preserving Communication Protocol for VANET	Computers and Electrical Engineering，Elsevier Press 38(3): 573-581, 2012
55	Hu Xiong, Zhong Chen, Fagen Li,	Bidder-anonymous English auction protocol based on revocable ring signature	Expert Systems With Applications 39(8): 7062-7066, 2012
56	Shuhua Wu,Qiong Pu	Comments on a Buyer-Seller Watermarking Protocol for Large Scale Networks	Internationa Journal of Network Securty 2012.1,14(1):53-58
57	Qiong Pu,Shuhua Wu	Secure and Efficient SIP Authentication Scheme for Converged VoIP Networks	The International Arab Journal of Information Technology 2012,9（6）：553-561
58	Qiong Pu,Jian Wang,Shuhua Wu,Ji Fu	Secure verifier-based three-party password-authenticaticated key exchange	Peer-to-Peer Networking and Applications,2012 DOI:10.1007/s12083-012-0125-y
59	Qiong Pu,Jian Wang,Shuhua Wu	Secure SIP Authentication Scheme Supporting Lawful Interception	Security Comm.Networks,2012 DOI:10.1002/sec.568
60	Shuhua Wu,Fei	Practical	Peer-to-Peer

	KangQiong Pu	authentication scheme for SIP	Networking and Applications,2012 DOI:10.1007/s12083-012-0129-7
61	Shuhua Wu,Fei Kang,Qiong Pu	Practical Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem	JIT Journal of Internet Technology, 2012,13(3):411-418
62	Shuhua Wu,Qiong Pu,Ji Fu	On the security of anonymous roaming protocol in UMTS mobile networks	Maejo International Journal of Science and Technology 2012,6:62-69
63	Qiong Pu,Jian Wang,Rongyong Zhao	Strong authentication scheme for telecare medicine information systems	Journal of Medical Systems 2012,36 (4):2609-2619
64	Shuhua Wu ,Kefei Chen, Yuefei Zhu	A Secure Lightweight RFID Binding Proof Protocol for Medication Errors and Patient Safety	Journal of Medical Systems 2012,36 (5):2743-2749
65	Shuhua Wu,Kefei Chen,Qiong Pu,Yuefei Zhu	Cryptanalysis and Enhancements of Efficient Three-party Password-based Key Exchange Scheme	International Journal of Communication Systems DOI: 10.1002/dac.1362
66	Xiang-Yang Wang, Xian-Jin Zhang,	A pixel-based color image segmentation using support vector machine and fuzzy c-means	Neural Networks, 2012, 33: 148-159.
67	Xiao-Qiu Cai, Chun-Yan Wei	Cryptanalysis of an inter-bank E-payment protocol based on quantum proxy blind signature	Quantum Inf Process DOI 10.1007/s11128-012-0477-5
68	Xiao-Qiu Cai, Hui-Fang Niu	Partially blind signatures based on quantum crypto - graphy.	International Journal of Modern Physics B 2012, 26(30): 1250163.
69	Xiao-Qiu Cai, Qing-Qing Liu	Robust message authentication schemes over a collective -noise channel	International Journal of Quantum Information 2012, 10 (6): 1250064.
70	Tian-Yin Wang, Xiao-Qiu Cai	An efficient quantum secret sharing scheme with decoy	International Journal of Modern Physics B 2012, 26(20):

		state	1250122.
71	Tian-Yin Wang, Yan-Ping Li	Cryptanalysis of dynamic quantum secret sharing	Quantum Information Processing doi:10.1007/s11128-012-0508-2
72	Tian-Yin Wang, Zong-Li Wei	One-time proxy signature based on quantum cryptography.	Quantum Information Processing 2012, 11 (2): 455-463
73	Gong Bei, Wei Jiang+, et.al	A Threshold Ring Signature Scheme Based on TPM	China Communications 2012, 卷: 9 期: 1 页: 80-85
74	Debiao He, Yitao Chen, Jianhua Chen	Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol	Nonlinear Dynamics 69(3), pp. 1149 - 1157, 2012
75	Juntao Gao, Yupu Hu and Xuelian Li	Linear spans of optimal sets of frequency hopping sequences	Theoretical Informatics and Applications 2012, 46(3): 343-354.
76	Zhixiong Chen, Xiaoni Du.	Constructing quasi-random subsets of ZN by using elliptic curves.	Applied Mathematics-A Journal of Chinese Universities(Ser. B) 2012, 27(1): 105-113.
77	Zhixiong Chen, Arne Winterhof	On the distribution of pseudorandom numbers and vectors derived from Euler-Fermat quotients	International Journal of Number Theory 2012, 8(3): 631-641.
78	Chen Zhixiong, Hu Lei, Du Xiaoni	Linear complexity of some binary sequences derived from Fermat quotients.	China Communications 2012, 9(2): 105-108.
79	S. J. Xu, X. B. Chen, R. Zhang, Y. X. Yang, and Y. C. Guo	An Improved Chaotic Cryptosystem Based on Circular Bit Shift and XOR Operations.	Physics Letters A 376 1003-1010 (2012).
80	M. M. Wang, X. B. Chen, S. S. Luo, and Y. X. Yang.	Efficient entanglement channel construction schemes for a theoretical quantum network model with d-level system.	Quantum Information Processing 51 (3): 912-924 (2012).
81	S. Y. Ma, P. Tang, X. B. Chen, and Y. X.	Schemes for Remotely Preparing a Six-Particle Entangled Cluster-Type State	International Journal of Theoretical Physics DOI: 10.1007/s10773-012-

			1409-y (2012).
82	X. W. Guan, X. B. Chen, and Y. X. Yang.	Controlled-Joint Remote Preparation of an Arbitrary Two-Qubit State via Non-maximally Entangled Channel.	International Journal of Theoretical Physics 51 (11): 3575-3586 (2012).
83	M. X. Luo, X. B. Chen, Y. X. Yang, and X. X.	Experimental architecture of joint remote state preparation.	Quantum Information Processing 11 (3): 751-767 (2012)
84	Y. Su, X. B. Chen, and Y. X. Yang	N-to-M joint remote state preparation of 2-level state.	International Journal of Quantum Information 10 (1): 1250006 (2012).
85	X. B. Chen, S. Y. Ma, Y. Su, R. Zhang, and Y. X. Yang	Controlled remote state preparation of arbitrary two and three qubit states via the Brown state	Quantum Information Processing 11 (6): 1653-1667 (2012).
86	M. M. Wang, X. B. Chen, X. X. Niu, and Y. X. Yang	Re-examining the security of blind quantum signature protocols	Physica Scripta 86 (5): 055006 (2012).
87	M. X. Luo, X. B. Chen, D. Yun, and Y. X. Yang.	Quantum Signature Scheme with Weak Arbitrator	International Journal of Theoretical Physics 51 (7): 2135-2142 (2012).
88	X. B. Chen, Y. Su, X. X. Niu, and Y. X. Yang	Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise	Quantum Information Processing DOI: 10.1007/s11128-012-0505-5 (2012).
89	G. A. Xu, X. B. Chen, Z. H. Wei, and Y. X. Yang	An efficient protocol for the quantum private comparison of equality with a four-qubit cluster state	International Journal of Quantum Information 10 (4): 1250045 (2012)
90	杨帅，陈秀波，杨义先	Attack on the Enhanced Multiparty Quantum Secret Sharing	Communications in Theoretical Physics 58 51-54 (2012)
91	X. B. Chen, S. Yang, Y. Su, and Y. X. Yang	Cryptanalysis on the improved multiparty quantum secret sharing protocol based on the GHZ state	Physica Scripta 86 (5): 055002 (2012)

92	Xiang-Yang Wang, E-No Miao, Hong-Ying Yang.	A new SVM-based image watermarking using Gaussian-Hermite Moments.	Applied Soft Computing 2012, 12 (2): 887-903.
93	Jingqiang Lin, Jiwu Jing, Peng Liu	Evaluating Intrusion-Tolerant Certification Authority Systems	Quality and Reliability Engineering International, Wiley 28、8、825－841
94	Yonghong Xie, Lei Hu	A matrix construction of Boolean functions with maximum algebraic immunity	Journal of Systems Science and Complexity 25、4、792-801
95	Shengli Liu, Fangguo Zhang, Kefei Chen	Selective Opening Chosen Ciphertext Security Directly from the DDH Assumption	NSS 2012 LNCS 7645, Springer, pp. 100-112
96	Liting Zhang,Wenling Wu,?Han Sui,?Peng Wang	3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound	ASIACRYPT 2012 Volume 7658, 2012, pp 296-312
97	1 Rui Wang, 2 Xiaoqi Jia, 3 Chujiang Nie	A Behavior Feature Generation Method for Obfuscated Malware Detection	The 2012 International Conference on Computer Science and Service System (CSSS2012). Volume 4,2105-2109
98	Liu Yang, Li Hongda, Niu Qihua	A Leakage-Resilient Zero Knowledge Proof for Lattice Problem	CSS2012 LNCS 7672、265-278
99	Zhenqi Li, Yao Lu, Wenhao Wang, Bin Zhang, Dongdai Lin	A New Variant of Time Memory Trade-Off on the Improvement of Thing and Ying’ s Attack	14th International Conference on Information and Communications Security- ICICS 2012 7618, 311-320
100	郭姝，徐海霞	A Non-interactive Secure Outsourced Computation Scheme in multi-party Cloud	INCoS2012 15-19
101	Li Hongda, Liu Yang, Niu Qihua	A note on constant-round concurrent zero-knowledge arguments of	NSS2012 LNCS 7646、202-216

		knowledge for NP	
102	Yingjun Zhang, Kai Chen, Yifeng Lian	A Path-based Access Control Method for Location Obfuscation in Mobile Environment	2012 IEEE Symposium on Electrical & Electronics Engineering 2012, pp.570 – 573.
103	Wentao Wang, Yuewu Wang, Jiwu Jing, Zhongwen Zhang	A Scalable Anonymity Scheme Based on DHT Distributed Inquiry	TrustCom 2012 1358-1363
104	Y. Sun, D.K. Wang, X.D. Ma and Y. Zhang	A Signature-Based Algorithm for Computing Groebner Bases in Solvable Polynomial Algebras.	Proceedings of ISSAC 2012. 351-358
105	Ting Wang, Dongyao Ji	Active Attacking Multicast Key Management Protocol Using Alloy	ABZ2012 LNCS7316、164-177
106	Hongru Wei，Yafei Zheng.	Algebraic Techniques in Linear Cryptanalysis	2012 International Conference on Computer Science and Communication Technology 2012.12
107	xusheng,Dongdai Lin	Analysis of Optimum Pairing Products at High Security Levels	INDOCRYPT 2012 Volume 7668, 2012, pp 412-430
108	Yu Chen, Zongyang Zhang, Dongdai Lin, and Zhenfu Cao	Anonymous Identity-Based Hash Proof System and Its Applications	ProvSec 2012 ProvSec 2012: 143-160
109	Zhenqi Li1, Bin Zhang2, Yao Lu2, Jing Zou2, and Dongdai Lin2	Applying Time-Memory-Data Trade-Off to Plaintext Recovery Attack	ICICS 2012 ICICS 2012: 321-330
110	Shengbao Wu, Mingsheng Wang	Automatic search of truncated impossible differentials and applications	Indocrypt 2012 2012
111	1W. Huang, 2X. Zhao, 3D. Feng, and 4R. Sheng	Benchmarking for steganog- raphy by kernel Fisher discriminant criterion	Inscrypt’2011 vol. 7537 of Lecture Notes in Computer Science, pp. 113–130
112	Aleksandar Kircanski,Yanzhao Shen,王高丽，Amr M.Youssef	Boomerang and Slide-Rotational Analysis of the SM3 Hash Function	SAC 2012 2012 LNCS 7707:305-321
113	Yang Yang, Guang Zeng, Zheng Wang, Wenbao Han	Calculation Components Analysis of the Lattice Sieve	GSAM2012 298-302, 2012

114	Gaoli Wang	Collision Attack for the Hash Function Extended MD4	ICICS2012 15-19
115	1 Wenhao Wang, 2 Meicheng Liu, 3 Yin Zhang,	Comments on “A design of Boolean functions resistant to (fast) algebraic cryptanalysis with efficient implementation”	Cryptography and Communications DOI 10.1007/s12095-012-0063-9
116	徐海霞，李宝，梅其祥	Complementary Witness Soundness Witness Indistinguishable Proof system and CCA2 Public-Key Encryption Schemes	INCoS2012 270-278
117	Wang Y.,Pu Q. Wu S.	Cryptanalysis and enhancements of delegation-based authentication protocol for secure roaming service	Int.J.Electronic Security and Digital Forensics 2012,4 (4):25-260
118	Jun Xu, Lei Hu, Siwei Sun, Ping Wang	Cryptanalysis of a Lattice-Knapsack Mixed Public Key Cryptosystem	CANS 2012 LNCS 7712、32－42
119	Debiao He, Jianhua Chen	Cryptanalysis of a three-party password-based key exchange protocol using weil pairing	International Journal of Electronic Security and Digital Forensics 4(4), pp. 244-251, 2012
120	Xiang Xie, Rui Xue, and Rui Zhang	Deterministic Public Key Encryption and Identity-Based Encryption from Lattices in the Auxiliary-Input Setting	SCN2012 Volume 7485, 2012, pp 1-18
121	Junxiang Wang Shengli Liu	Dynamic Provable Data Possession with batch-update verifiability	2012 IEEE International Conference on Intelligent Control,

			Automatic Detection and High-End Equipment (ICADE 2012) pp. 108 - 113
122	Lifeng Guo, Lei Hu	Efficient bidirectional proxy re-encryption with direct chosen-ciphertext Security	Computers and Mathematics with Applications 63、1、151-157
123	马存庆，林璟锵，王跃武	Efficient Missing Tag Detection in a Large RFID System	11th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom) 185-192
124	Wentao Zhang, Bozhan Su, Wenling Wu, Dengguo Feng, Chuankun Wu	Extending Higher-order Integral: An Efficient Unified Algorithm of Constructing Integral Distinguishers for Block Ciphers	Springer-Verlag LNCS 7341
125	H. Shuai and W. T. Zhu	F5P5: Keyword search over encrypted data with five functions and five privacy assurances	ICICS 2012 LNCS 7618、416--426
126	Zhang Xusheng,Chen Shan,Lin Dongdai	Fast tate pairing computation on twisted jacobi intersections curves	Inscrypt 2011, 2012 LNCS 7537：210-226
127	Feng Liu, Teng Guo, Chuankun Wu and Ching-Nung Yang	Flexible Visual Cryptography Scheme Without Distortion	IWDW2011 (10th International Workshop on Digital-forensics and Watermarking) LNCS Volume 7128/2012, page 211-227
128	林璟锵，罗勃，荆继武，张晓坤	GRADE: Graceful Degradation in Byzantine Quorum Systems	31st IEEE International Symposium on Reliable Distributed Systems (SRDS) 171-180
129	Yang Liu, Qiang Li, Weijun Qin, et al.	GreenTech: A Case Study for Using the Web of Things in Household Energy Conservation	UIC 2012 906-911
130	Wei Li, Ke-Wei Lv, Gang Yao	Hardware Performance Optimization and	ICICS 2012 LNCS 7618、105-118

		Evaluation of SM3 Hash Algorithm on FPGA	
131	Yu Chen1， Zongyang Zhang2， Dongdai Lin1， and Zhenfu Cao2，	Identity-Based Extractable Hash Proofs and Their Applications.	ACNS 2012 ACNS 2012: 153-170
132	Jun Xu， Lei Hu， Siwei Sun	Implicit Polynomial Recovery and Cryptanalysis of A Combinatorial Key Cryptosystem	ICICS2012 LNCS7618、45-57
133	Qian Quan， Wu Jinlin， Zhu Wei， Xin Mingjun	Improved Edit Distance Method for System Call Anomaly Detection	IEEE 12th International Conference on Computer and Information Technology pp: 1097 - 1102
134	Xianhui Lu， Bao Li，Qixiang Mei， 刘亚敏	Improved Efficiency of Chosen Ciphertext Secure Encryption from Factoring	ISPEC2012 LNCS 7232、34-45
135	Zhang Yin,Lin Dongdai,Liu Meicheng	Improving the lower bound on linear complexity of the sequences generated by nonlinear filtering	Chinese Journal of Electronics 2012.7,Vol 21,Issue 3:519-522
136	Wuqiong Pan， Yulong Zhang， Meng Yu， Jiwu Jing	Improving Virtualization Security by Splitting Hypervisor into Smaller Components	DBSec 2012 LNCS 7371、298-313
137	Chong Xiang， Li Yang	Indistinguishability and semantic security for quantum encryption scheme	Photonics Asia 2012 8554-15
138	Xiang Xie， Rui Xue， Rui Zhang	Inner-Product Lossy Trapdoor Functions and Applications	ACNS 2012 Volume 7341， 2012， pp 188-205
139	王丽萍	Lagrange interpolation polynomials and generalized Reed-Solomon codes over rings of matrices	ISIT 2012 3098-3100
140	Zhixiong Chen，， Domingo Gomez-Perez	Linear complexity of binary sequences derived from	7th Int’l Conf. on SEquences and Their Applications-SETA

		polynomial quotients	2012, LNCS, vol.7280, pp.181-189, Springer, Heidelberg (2012)
141	Tao Shi, Vladimir Anashin, and Dongdai Lin	Linear Weaknesses in T-functions	SETA 2012 SETA 2012: 279-290
142	H. Shuai and W. T. Zhu	Masque: Access control for interactive sharing of encrypted data in social networks	NSS 2012 LNCS 7645、503--515
143	Lingguang Lei, Yuewu Wang, Jiwu Jing, Zhongwen Zhang, Xingjie Yu	MeadDroid: Detecting Monetary Theft Attacks in Android by DVM Monitoring	ICISC 2012 LNCS
144	Jiqiang Lu,Yongzhuang Wei,Enes Pasalic ,Pierre-Alain Fouque	Meet-in-the-Middle Attack onReduced Versions of the Camellia Block Cipher	IWSEC 2012,Springer-Verlag Berlin Heidelberg LNCS 7631, pp.197-215,
145	L. He and W. T. Zhu	Mitigating DoS attacks against signature-based authentication in VANETs	proc. 2nd International Conference on Computer Science and Automation Engineering (CSAE'12) 261--265
146	Wenpan Jing, Haixia Xu, Bao Li	Non-Malleable Instance-Dependent Commitment in the Standard Model	ACISP 2012 LNCS 7372、450-457
147	马存庆，林璟锵，王跃武，尚铭	Offline RFID Grouping Proofs with Trusted Timestamps	11th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom) 674-681
148	Teng Guo, Feng Liu and Chuankun Wu	On the Equivalence of Two Definitions of Visual Cryptography Scheme	ISPEC 2012 pp. 217-227, LNCS 7232
149	1Haixin Song, 2Xiubin Fan, 3Chuankun Wu,4 Dengguo Feng	On the probability distribution of the carry cells of stream ciphers F-FCSR-H v2 and F-FCSR-H v3	Proceedings of Inscrypt 2011 LNCS 7537 pp.31-47
150	1 Yusong Du, 2 Fangguo Zhang, 3	On the resistance of Boolean functions	ICISC 2011(LNCS) 7259, 261-274

	Meicheng Liu	against fast algebraic attacks	
151	XU Lei, XU Xiaolong, ZHOU Yue Zhuo.	P2P Botnet Detection Using Min-Vertex Cover	Journal of Networks 2012, 7(8): 1176-1181
152	Meicheng Liu, Yin Zhang, and Dongdai Lin	Perfect Algebraic Immune Functions	ASIACRYPT 2012 LNCS (7658) 172-189
153	Jian Zhou, Jiwu Jing, Ji Xiang and Lei Wang	Privacy Preserving Social Network Publication on Bipartite Graphs	WISTP 2012 LNCS 7322、58-70
154	T. C. Li and W. T. Zhu	Protecting user anonymity in location-based services with fragmented cloaking region	proc. 2nd International Conference on Computer Science and Automation Engineering (CSAE'12) 227--231
155	Rui-Rui Zhou and Li Yang	Quantum election based on distributed scheme	Photonics Asia 2012 8554--3
156	Li Yang, Biyao Yang, and Jiangyou Pan	Quantum public-key encryption protocols with information-theoretic security	Photonics Europe 2012 8440-E
157	Chong Xiang, Li Yang	Quantum unicity distance	Photonics Europe 2012 8440-T
158	Min Liang, Li Yang	Quantum-message-oriented public-key encryption scheme beyond computational hypothesis	Photonics Europe 2012 8440-L
159	张楠，林璟锵，荆继武，高能	RIKE: Using Revocable Identities to Support Key Escrow in PKIs	ACNS 2012 LNCS 7341、48-65
160	Qiang Li, Weijun Qin, et al.	Smartphone Heterogeneous Network Handoff Based on the Closed Control Loop	ICCPS 2012 978-0-7695-4695-7
161	Wei, Jiang	Survey of network and computer attack taxonomy	2012 IEEE Symposium on Robotics and Applications 2012, 6，294-297
162	1Aijun Ge, 2 Jiang Zhang, 3 Rui	Threshold Ciphertext Policy Attribute-	ACISP 2012 LNCS 7372:336-349

	Zhang	based Encryption with Constant Size Ciphertexts	
163	Lei Wang, Ji Xiang, Jiwu Jing, Lingchen Zhang	Towards Fine-Grained Access Control on Browser Extensions	ISPEC2012 LNCS 7232、158-169
164	王文韬，林璟锵，荆继武，罗勃	TSS-BQS系统的Graceful Degradation机制	计算机学报 35、9、1793-1803
165	张李军，王鲲鹏，汪宏	Unified and complete point addition formula for ellipic curves	Chinese Journal of electronics 21、2、345-349
166	徐海霞，李红达，李宝	Universally composable zero-knowledge sets	Intenational Journal of Grid and Utility Computing 3、1、25-31
167	林璟锵，刘鹏，荆继武	Using Signaling Games to Model the Multi-step Attack-defense Scenarios on Confidentiality	GameSec 2012 LNCS 7638 118-137
168	葛爱军，马传贵，张振峰，陈少真	标准模型下固定长度的基于身份环签名方案	计算机学报 2012,35 (9):1874-1880
169	徐小龙，熊婧夷，杨庚，王汝传	大规模网络中基于HDHT的病毒疫苗分发算法	系统工程与电子技术 2012，34(8)：1708-1715
170	1刘俊，2范修斌，3武传坤	单圈T函数输出序列的线性复杂度	中国科学院研究生院学报 29，3，429-432
171	李雪莲 ，高军涛 ，胡予濮 ，张风荣	对广义自缩生成器的区分攻击	西安电子科技大学学报（自然科学版） 2012，39（4）：114—119.
172	李晓千(1)，吴文玲(2)，李宝(3)，于晓丽(4)	概率积分密码分析	计算机学报 35、9、1897-1905
173	于伟，王鲲鹏，李宝，田松	构造从字符串到C34曲线的散列函数	计算机学报 35、9、1868-1873
174	1黄炜,2赵险峰,3盛任农	基于KFD指标聚类的高隐蔽性JPEG隐写分析	计算机学报 35(9)：1951－1958
175	傅长明,杨玉花,李拓,陈岳东,程栋,王雅丽,	基于标量衍射理论的图像解密三维信息构造方	中国科学院研究生院学报 2012，(6)：757-

	史祎诗	法	766.
176	孙玉砚	基于路况相似性的城市公交车到站时间预测机制	软件学报　2012,23 (Suppl.(1)):87-99
177	万威，赵险峰，黄炜，盛任农	基于码表分布特征和重编码的MP3Stego隐写分析	中国科学院研究生院学报　29(1)，118－124
178	李瑞林，熊海，李超	基于循环移位和异或运算的对合线性变换的研究	国防科学技术大学学报 34(2):34-39，2012
179	1李红艳，2赵险峰，3黄炜，4盛任农	基于游程统计和Walsh谱能量分布的调色板隐写分析	中国科学院研究生院学报　29(3)，423-428
180	陈恺，苏璞睿，冯登国	基于有限约束满足问题的溢出漏洞动态检测方法	计算机学报　2012，5（35），898-909
181	1黄炜，2赵险峰，3冯登国，4盛任农	基于主成分分析进行特征融合的JPEG隐写分析	软件学报　23(7): 1869-1879
182	钱权,萧超杰,张瑞	结构化对等网络中P2P僵尸网络传播模型	软件学报　2012,23 (12):3161-3174.
183	高军涛，胡予濮，李雪莲，向上荣	两类最优跳频序列集的线性复杂度分析	通信学报　2012，（2）：175-181
184	1宋海欣，2范秀斌，3武传坤，4冯登国	流密码算法Grain的立方攻击	软件学报　23，1，171-176
185	徐小龙，杨庚，李玲娟，王汝传	面向绿色云计算数据中心的动态数据聚集算法.	系统工程与电子技术 2012，34(9)：1923-1929
186	1张弢，2赵险峰，3黄炜，4盛任农	三组隐写特征的互补性分析及其面向空域隐写的融合	中国科学院研究生院学报　29(2)，264-270
187	贾小英(1)，李宝(2)，刘亚敏(3)	随机谕言模型	软件学报　23、1、140-151
188	杨阳，曾光	序列密码算法RAKAPOSHI的动态移存器构造	通信学报　Vol 32，No 11A，178-183，2011
189	韦永壮，欧阳宁，马	一个基于稳固加密RFID	计算机研究与发展

	春波	协议的安全性分析	2012,19(5):958-961
190	张秋璞 徐震 叶顶锋	一个可追踪身份的基于属性签名方案	软件学报 23、9、2449-2464
191	黄杜煜,张振峰,张立武	一个适应性安全的支持用户私钥撤销的KP-ABE方案	小型微型计算机系统 .2012(2194)
192	王鹏翩，冯登国，张立武	一个支持完全细粒度属性撤销的CP-ABE方案	软件学报 2012,23 (10):2805-2816
193	李春雷，张焕国，曾祥勇，胡磊	一类Bent函数的二阶非线性度下线	计算机学报 35、8、1588-1593
194	谭刚敏，曾光，韩文报，刘向辉	一类本原s-LFSR序列的构造与计数	软件学报 55、9、1618-1629
195	李昕，林东岱，徐林	一种布尔多项式的高效计算机表示	计算机研究与发展 2012,49（12）：2568-2574
196	1邓果，2赵险峰，3黄炜，4盛任农	一种测评隐写分析的图像纹理估计方法	计算机工程 38(14), 116－118
197	1谢涛，2武传坤	一种无证书的家庭基站认证方案	中国科学院研究生院学报 29,1, 141-144
198	王海斌,陈少真	隐藏访问结构的基于属性加密方案	电子与信息学报 2012,34(2):457-461
199	1徐震,2刘韧， 于爱民，3汪丹	智能电网中的移动应用安全技术	电力系统自动化 V36，NO16，pp82~87
200	苏崇茂，韦永壮，马春波	10轮3D分组密码算法的中间相遇攻击	电子与信息学报 2012,34（3）:694-697
201	赵光耀，李瑞林，孙兵，李超	Piccolo算法的差分故障分析	计算机学报 Vol. 35，No.9. 2012: 1918-1926
202	刘宗斌 荆继武 夏鲁宁	BLAKE算法的硬件实现研究	计算机学报 35、4、703-711
203	1杨笑，2范秀斌，3武	BOMM算法的密码学性质	软件学报 23,7, 1899-

	传坤，4余玉银，5冯秀涛		1907
204	吕克伟、姚刚	代数、组合与线性码	金城出版社
205	1Chuankun Wu, 2Moti Yung,3 Dongdai Lin	Information Security and Cryptology - 7th International Conference, Inscrypt 2011	Springer
206	黄昆，李超，屈龙江	基于先验结果对涂-邓猜想一些情形下的递推证明	武汉大学学报(理学版) Vol.58, 2012: 493-496
207	Yong Wang, Xiuxia Tian, Jianping Xu, Shuai Chen, and Heng Yang	Intel SYSRET Privilege Escalation Vulnerability Analysis	NCIS 2012, 2012:30-37
208	Wang Yong,Tian Xiuxia,Xu Jianping,Chen Shuai,Yang Heng	Stuxnet Vulnerabilities Analysis of SCADA Systems	NCIS 2012, 2012: 640-646
209	韦永壮，苏崇茂，马春波	Rijndael-256算法的中间相遇攻击	计算机工程 2012，38（7）：107-109
210	卢尧，张锐，林东岱	Stronger Security Model for Public Key Encryption with Equality Test	Pairing 2012 (Lecture Notes in Computer Science) vol. 7708, 65-82
211	王高丽，王少辉	对MIBS算法的Integral攻击	小型微型计算机系统 Vol.33,NO.4:768-773,2012
212	徐小龙, 吴家兴, 杨庚	一种基于云-端计算模型的恶意代码联合防御网络	计算机应用研究 2012, 29(6):2214-2217
213	徐小龙, 吴家兴, 杨庚, 程春玲, 王汝传	基于大规模廉价计算平台的海量数据处理系统的研究	计算机应用研究 2012, 29(2):582-585
214	徐小龙, 耿卫建, 杨庚, 王汝传	开放云端计算环境中的任务执行代码安全机制	计算机科学 2012, 39 (7):7-10
215	周山东,宋新芳,金波,刘凯	基于TCM的全盘加密系统的研究与实现	计算机工程与设计 2012年 第9期,3291-3296
216	Li Yu, Wei Jiang	Research on User Permission Isolation	Int. J. Communications,

		for Multiusers Service-Oriented Program.	Network and System Sciences. 2012，5，Vol.5 No.2, pp.105-110
217	Zhixiong Chen, Arne Winterhof	Additive character sums of polynomial quotients	Tenth Int’l Conf. on Theory and Applications of Finite Fields-Fq10,Contemp. Math vol. 579, Amer. Math. Soc., pp.69-74, 2012.
218	曹喜望	Carlitz定理的一个注记	国防科技大学学报 2012，02期: 39-41
219	杨珺涵 曹天杰	基于口令与智能卡的可证安全认证密钥协商协议	江苏科技大学学报 2012.6,26（3）：282-287
220	梁钰敏 曹天杰	新的基于双难题的带有信息恢复的签名方案	微电子学与计算机 2012.9,29（9）：175-178
221	李红达, 冯登国, 李宝, 徐海霞	NP 问题的最优轮复杂性知识的零知识证明	中国科学 信息科学 42、1、 20-31
222	蔡权伟,林璟锵，荆继武，尚铭	PKI应用系统互操作性检测工具的设计与实现	中国科学院研究生院学报 29、6、799-804
223	孙锐，吴辰苗，杨理	网际空间认证框架及相关量子技术	网络新媒体技术 1、6、39-44
224	潘江游，杨理	基于一次一密的量子身份识别方案	中国科学院研究生院学报 29、2、277-280
225	马存庆，林璟锵，查达仁，尚铭	基于WCF的测试管理系统的设计与实现	计算机应用研究 29、增刊、417－419
226	朱玉涛，王雅哲，武传坤	两层架构的可信身份服务平台研究与设计	计算机应用与软件 2012.3 Vol.29 No.3
227	朱玉涛，王雅哲，武传坤	基于服务构件集成的安全访问业务建模方法	计算机应用与软件 2012.2 Vol.29 No.2
228	1孙磊, 2赵险峰, 3黄炜, 4盛任农	一种隐写分析盲性的评价及提高方法	计算机应用与软件 29（9），6-9

229	林东岱，刘峰	美国信息安全保密体系初探	保密科学与技术　期7，页6-13
230	1 胡建康，2 徐震，3 马多贺，4 杨婧	基于决策树的Webshell检测方法研究	网络新媒体技术　1 6 15-19
231	1 Bingbing Xia （夏冰冰）2 Xianfeng Zhao3 Dengguo Feng	Improve steganalysis by MWM feature-selection.	Watermarking, Intech Publishing　Volume 2

备案序号：京ICP备12047326号
联系电话：010-82546611
传 真：010-82546564
地址：北京市海淀区闵庄路甲89号