Jianying Zhou

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/7465243/publications.pdf

Version: 2024-02-01

194 papers	5,634 citations	126907 33 h-index	102487 66 g-index
198 all docs	198 docs citations	198 times ranked	4277 citing authors

#	Article	IF	Citations
1	Challenges of post-quantum digital signing in real-world applications: a survey. International Journal of Information Security, 2022, 21, 937-952.	3.4	4
2	LARP: A Lightweight Auto-Refreshing Pseudonym Protocol for V2X. , 2022, , .		1
3	Modular Framework for Constructing IoT-Server AKE in Post-Quantum Setting. IEEE Access, 2022, 10, 71598-71611.	4.2	1
4	Strong leakage-resilient encryption: enhancing data confidentiality by hiding partial ciphertext. International Journal of Information Security, 2021, 20, 141-159.	3.4	2
5	Lightweight and Privacy-Preserving Delegatable Proofs of Storage with Data Dynamics in Cloud Storage. IEEE Transactions on Cloud Computing, 2021, 9, 212-225.	4.4	84
6	Building Low-Interactivity Multifactor Authenticated Key Exchange for Industrial Internet of Things. IEEE Internet of Things Journal, 2021, 8, 844-859.	8.7	16
7	Quantum Computing Threat Modelling on a Generic CPS Setup. Lecture Notes in Computer Science, 2021, , 171-190.	1.3	3
8	Server-Aided Bilateral Access Control for Secure Data Sharing With Dynamic User Groups. IEEE Transactions on Information Forensics and Security, 2021, 16, 4746-4761.	6.9	21
9	Model-Based CPS Attack Detection Techniques: Strengths and Limitations. Studies in Systems, Decision and Control, 2021, , 155-187.	1.0	2
10	Scanning the Cycle: Timing-based Authentication on PLCs. , 2021, , .		3
11	Categorizing Touch-Input Locations from Touchscreen Device Interfaces via On-Board Mechano-Acoustic Transducers. Applied Sciences (Switzerland), 2021, 11, 4834.	2.5	4
12	Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration. Information Fusion, 2021, 70, 60-71.	19.1	41
13	Modeling social worm propagation for advanced persistent threats. Computers and Security, 2021, 108, 102321.	6.0	8
14	Opportunities and Challenges in Securing Critical Infrastructures Through Cryptography. IEEE Security and Privacy, 2021, 19, 57-65.	1.2	2
15	Enabling isolation and recovery in PLC redundancy framework of metro train systems. International Journal of Information Security, 2021, 20, 783-795.	3.4	2
16	Machine Learning for CPS Security: Applications, Challenges andÂRecommendations. Studies in Computational Intelligence, 2021, , 397-421.	0.9	7
17	Bigdata-Facilitated Two-Party Authenticated Key Exchange forÂIoT. Lecture Notes in Computer Science, 2021, , 95-116.	1.3	3
18	Layering Quantum-Resistance into Classical Digital Signature Algorithms. Lecture Notes in Computer Science, 2021, , 26-41.	1.3	3

#	Article	IF	Citations
19	Group Time-based One-time Passwords and its Application to Efficient Privacy-Preserving Proof of Location. , 2021, , .		2
20	Attacks on smart grid: power supply interruption and malicious power generation. International Journal of Information Security, 2020, 19, 189-211.	3.4	26
21	Faster Authenticated Key Agreement With Perfect Forward Secrecy for Industrial Internet-of-Things. IEEE Transactions on Industrial Informatics, 2020, 16, 6584-6596.	11.3	35
22	Data Integrity Threats and Countermeasures in Railway Spot Transmission Systems. ACM Transactions on Cyber-Physical Systems, 2020, 4, 1-26.	2.5	13
23	Challenges and Opportunities in Cyberphysical Systems Security: A Physics-Based Perspective. IEEE Security and Privacy, 2020, 18, 14-22.	1.2	15
24	Right-of-Stake: Deterministic and Fair Blockchain Leader Election with Hidden Leader. , 2020, , .		2
25	Anomaly detection in Industrial Control Systems using Logical Analysis of Data. Computers and Security, 2020, 96, 101935.	6.0	56
26	A Tale of Two Testbeds: A Comparative Study of Attack Detection Techniques in CPS. Lecture Notes in Computer Science, 2020, , 17-30.	1.3	8
27	LiS: Lightweight Signature Schemes for Continuous Message Authentication in Cyber-Physical Systems. , 2020, , .		10
28	Evaluating Cascading Impact of Attacks on Resilience of Industrial Control Systems: A Design-Centric Modeling Approach. , 2020, , .		3
29	Process skew. , 2020, , .		8
30	Policy-based Chameleon Hash for Blockchain Rewriting with Black-box Accountability. , 2020, , .		26
31	Post-exploitation and Persistence Techniques Against Programmable LogicÂController. Lecture Notes in Computer Science, 2020, , 255-273.	1.3	0
32	Formalizing Bitcoin Crashes with Universally Composable Security. Lecture Notes in Computer Science, 2020, , 334-351.	1.3	0
33	Advances in security research in the Asiacrypt region. Communications of the ACM, 2020, 63, 76-81.	4.5	0
34	DecIED: Scalable k-Anonymous Deception for IEC61850-Compliant Smart Grid Systems. , 2020, , .		1
35	Design of a FDIA Resilient Protection Scheme for Power Networks by Securing Minimal Sensor Set. Lecture Notes in Computer Science, 2019, , 156-171.	1.3	1
36	SocialAuth: Designing Touch Behavioral Smartphone User Authentication Based on Social Networking Applications. IFIP Advances in Information and Communication Technology, 2019, , 180-193.	0.7	7

#	Article	IF	Citations
37	Zero Residual Attacks on Industrial Control Systems and Stateful Countermeasures. , 2019, , .		8
38	File Guard: automatic format-based media file sanitization. International Journal of Information Security, 2019, 18, 701-713.	3.4	1
39	A Modular Hybrid Learning Approach for Black-Box Security Testing of CPS. Lecture Notes in Computer Science, 2019, , 196-216.	1.3	15
40	A Survey on Lightweight Authenticated Encryption and Challenges for Securing Industrial IoT. Advanced Sciences and Technologies for Security Applications, 2019, , 71-94.	0.5	19
41	CAN-FD-Sec: Improving Security of CAN-FD Protocol. Lecture Notes in Computer Science, 2019, , 77-93.	1.3	7
42	Towards Semantic Sensitive Feature Profiling of IoT Devices. IEEE Internet of Things Journal, 2019, 6, 8056-8064.	8.7	9
43	A Novel Authenticated Key Agreement Protocol With Dynamic Credential for WSNs. ACM Transactions on Sensor Networks, 2019, 15, 1-27.	3.6	19
44	SCADAWall: A CPI-enabled firewall model for SCADA security. Computers and Security, 2019, 80, 134-154.	6.0	35
45	Strong Leakage Resilient Encryption by Hiding Partial Ciphertext. Lecture Notes in Computer Science, 2019, , 172-191.	1.3	1
46	IBWH: An Intermittent Block Withholding Attack with Optimal Mining Reward Rate. Lecture Notes in Computer Science, 2019, , 3-24.	1.3	8
47	Proof of aliveness. , 2019, , .		5
48	SMuF: State Machine Based Mutational Fuzzing Framework for Internet of Things. Lecture Notes in Computer Science, 2019, , 101-112.	1.3	0
49	Careful-Packing. , 2019, , .		3
50	Magic Train: Design of Measurement Methods against Bandwidth Inflation Attacks. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 98-111.	5.4	2
51	Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data. IEEE Access, 2018, 6, 7234-7243.	4.2	67
52	HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems. IEEE Transactions on Industrial Informatics, 2018, 14, 4101-4112.	11.3	173
53	Finding Dependencies between Cyber-Physical Domains for Security Testing of Industrial Control Systems. , 2018, , .		17
54	Noise Matters. , 2018, , .		64

#	Article	IF	Citations
55	ATG. , 2018, , .		21
56	Virtually Isolated Network: A Hybrid Network to Achieve High Level Security. Lecture Notes in Computer Science, 2018, , 299-311.	1.3	4
57	<i>NoisePrint</i>. , 2018, , .		43
58	Efficient outsourcing of secure k -nearest neighbour query over encrypted database. Computers and Security, 2017, 69, 65-83.	6.0	15
59	A Pilot Study of Multiple Password Interference Between Text and Map-Based Passwords. Lecture Notes in Computer Science, 2017, , 145-162.	1.3	11
60	On the Security of In-Vehicle Hybrid Network: Status and Challenges. Lecture Notes in Computer Science, 2017, , 621-637.	1.3	17
61	A New Functional Encryption for Multidimensional Range Query (Short Paper). Lecture Notes in Computer Science, 2017, , 361-372.	1.3	1
62	A scheme for lightweight SCADA packet authentication. , 2017, , .		3
63	Privacy-Preserving k-Nearest Neighbour Query on Outsourced Database. Lecture Notes in Computer Science, 2016, , 181-197.	1.3	1
64	Anonymous Announcement System (AAS) for Electric Vehicle in VANETs. Computer Journal, 2016, , .	2.4	1
65	Credential Wrapping. , 2016, , .		6
66	TMGuard: A Touch Movement-Based Security Mechanism for Screen Unlock Patterns on Smartphones. Lecture Notes in Computer Science, 2016, , 629-647.	1.3	25
67	Efficient Privacy-Preserving Charging Station Reservation System for Electric Vehicles. Computer Journal, 2016, 59, 1040-1053.	2.4	12
68	Scalable Two-Factor Authentication Using Historical Data. Lecture Notes in Computer Science, 2016, , 91-110.	1.3	6
69	Lightweight Delegatable Proofs of Storage. Lecture Notes in Computer Science, 2016, , 324-343.	1.3	8
70	A Forward-Secure Certificate-Based Signature Scheme. Computer Journal, 2015, 58, 853-866.	2.4	6
71	Achieving Revocable Fine-Grained Cryptographic Access Control over Cloud Data. Lecture Notes in Computer Science, 2015, , 293-308.	1.3	7
72	Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs. IEEE Transactions on Information Forensics and Security, 2015, 10, 613-625.	6.9	62

#	Article	IF	Citations
73	Surveying the Development of Biometric User Authentication on Mobile Phones. IEEE Communications Surveys and Tutorials, 2015, 17, 1268-1293.	39.4	202
74	Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption. IEEE Transactions on Information Forensics and Security, 2015, 10, 665-678.	6.9	117
75	Cross-layer design in wireless multi-hop networks: a bargaining game theoretic analysis. Telecommunication Systems, 2015, 60, 149-158.	2.5	0
76	A Secure, Intelligent Electric Vehicle Ecosystem for Safe Integration With the Smart Grid. IEEE Transactions on Intelligent Transportation Systems, 2015, 16, 3367-3376.	8.0	17
77	Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data. Lecture Notes in Computer Science, 2015, , 146-166.	1.3	54
78	Security and privacy of electronic health information systems. International Journal of Information Security, 2015, 14, 485-486.	3.4	6
79	Cost-Effective Authentic and Anonymous Data Sharing with Forward Security. IEEE Transactions on Computers, 2015, 64, 971-983.	3.4	93
80	Leakage-resilient password entry: Challenges, design, and evaluation. Computers and Security, 2015, 48, 196-211.	6.0	13
81	Time-Bound Anonymous Authentication for Roaming Networks. IEEE Transactions on Information Forensics and Security, 2015, 10, 178-189.	6.9	46
82	&lt;inline-formula&gt;&lt;tex-math&gt;$k$&lt;/tex-math&gt;&lt;alternatives&gt; &lt;inline-graphic xlink:type="simple" xlink:href="huang-ieq1-2366741.gif"/&gt;&lt;/alternatives&gt;&lt;/inline-formula&gt;-Times Attribute-Based Anonymous Access Control for Cloud Computing. IEEE Transactions on Computers, 2015, 64, 2595-2608.	3.4	44
83	Self-blindable Credential: Towards Anonymous Entity Authentication Upon Resource Constrained Devices. Lecture Notes in Computer Science, 2015, , 238-247.	1.3	4
84	On the Efficiency of Multi-party Contract Signing Protocols. Lecture Notes in Computer Science, 2015, , 227-243.	1.3	4
85	PPDCP-ABE: Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption. Lecture Notes in Computer Science, 2014, , 73-90.	1.3	33
86	Security in a completely interconnected world. Security and Communication Networks, 2014, 7, 2726-2727.	1.5	0
87	Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. Theoretical Computer Science, 2014, 539, 87-105.	0.9	47
88	Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage. IEEE Transactions on Parallel and Distributed Systems, 2014, 25, 468-477.	5.6	179
89	A New Payment System for Enhancing Location Privacy of Electric Vehicles. IEEE Transactions on Vehicular Technology, 2014, 63, 3-18.	6.3	70
90	On the security of cloud data storage and sharing. , 2014, , .		4

#	Article	IF	Citations
91	Cyberâ€"Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem. IEEE Journal on Selected Areas in Communications, 2014, 32, 1509-1517.	14.0	49
92	Robust Multi-Factor Authentication for Fragile Communications. IEEE Transactions on Dependable and Secure Computing, 2014, 11, 568-581.	5.4	105
93	Collaborative agglomerative document clustering with limited information disclosure. Security and Communication Networks, 2014, 7, 964-978.	1.5	2
94	Linkable Ring Signature with Unconditional Anonymity. IEEE Transactions on Knowledge and Data Engineering, 2014, 26, 157-165.	5.7	68
95	Protecting the internet of things. Security and Communication Networks, 2014, 7, 2637-2638.	1.5	0
96	Leakage Resilient Proofs of Ownership in Cloud Storage, Revisited. Lecture Notes in Computer Science, 2014, , 97-115.	1.3	12
97	New Insight to Preserve Online Survey Accuracy and Privacy in Big Data Era. Lecture Notes in Computer Science, 2014, , 182-199.	1.3	5
98	On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks. IEEE Communications Surveys and Tutorials, 2013, 15, 1223-1237.	39.4	165
99	An optimistic fair exchange protocol with active intermediaries. International Journal of Information Security, 2013, 12, 299-318.	3.4	6
100	Designing leakage-resilient password entry on touchscreen mobile devices. , 2013, , .		25
101	Security Concerns in Popular Cloud Storage Services. IEEE Pervasive Computing, 2013, 12, 50-57.	1.3	61
102	CloudHKA: A Cryptographic Approach for Hierarchical Access Control in Cloud Computing. Lecture Notes in Computer Science, 2013, , 37-52.	1.3	24
103	Realizing Fully Secure Unrestricted ID-Based Ring Signature in the Standard Model Based on HIBE. IEEE Transactions on Information Forensics and Security, 2013, 8, 1909-1922.	6.9	17
104	On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628. , 2013, 51, 58-65.		33
105	How to achieve non-repudiation of origin with privacy protection in cloud computing. Journal of Computer and System Sciences, 2013, 79, 1200-1213.	1.2	19
106	On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 2013, 57, 2266-2279.	5.1	992
107	Privacy-preserving smart metering with regional statistics and personal enquiry services. , 2013, , .		19
108	Weak leakage-resilient client-side deduplication of encrypted data in cloud storage. , 2013, , .		98

#	Article	IF	Citations
109	An Asynchronous Optimistic Protocol for Atomic Multi-Two-Party Contract Signing. Computer Journal, 2013, 56, 1258-1267.	2.4	10
110	Efficient Linkable and/or Threshold Ring Signature Without Random Oracles. Computer Journal, 2013, 56, 407-421.	2.4	41
111	Launching Generic Attacks on iOS with Approved Third-Party Applications. Lecture Notes in Computer Science, 2013, , 272-289.	1.3	21
112	Verifier-local revocation group signatures with time-bound keys. , 2012, , .		24
113	Challenges and opportunities in infrastructure support for electric vehicles and smart grid in a dense urban environment-Singapore. , 2012, , .		6
114	Dynamic Secure Cloud Storage with Provenance. Lecture Notes in Computer Science, 2012, , 442-464.	1.3	37
115	An Efficient and Secure Service Discovery Protocol for Ubiquitous Computing Environments. IEICE Transactions on Information and Systems, 2012, E95-D, 117-125.	0.7	1
116	A Survey on Privacy Frameworks for RFID Authentication. IEICE Transactions on Information and Systems, 2012, E95-D, 2-11.	0.7	5
117	Message from the Guest Editors. International Journal of Information Security, 2012, 11, 291-292.	3.4	0
118	Enhanced authentication for commercial video services. Security and Communication Networks, 2012, 5, 1248-1259.	1.5	6
119	Forward Secure Attribute-Based Signatures. Lecture Notes in Computer Science, 2012, , 167-177.	1.3	7
120	Detecting node replication attacks in mobile sensor networks: theory and approaches. Security and Communication Networks, 2012, 5, 496-507.	1.5	21
121	Detecting node replication attacks in wireless sensor networks: A survey. Journal of Network and Computer Applications, 2012, 35, 1022-1034.	9.1	86
122	Enhancing Location Privacy for Electric Vehicles (at the Right time). Lecture Notes in Computer Science, 2012, , 397-414.	1.3	28
123	A Generic Approach for Providing Revocation Support in Secret Handshake. Lecture Notes in Computer Science, 2012, , 276-284.	1.3	1
124	Intrusion Detection and Prevention in Wireless Sensor Networks. , 2012, , 487-510.		0
125	A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems. IEEE Transactions on Parallel and Distributed Systems, 2011, 22, 1390-1397.	5.6	191
126	Online/Offline Identity-Based Signcryption Revisited. Lecture Notes in Computer Science, 2011, , 36-51.	1.3	18

#	Article	IF	Citations
127	Identity-based online/offline key encapsulation and encryption. , 2011, , .		32
128	Short and Efficient Certificate-Based Signature. Lecture Notes in Computer Science, 2011, , 167-178.	1.3	12
129	Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signatures. IEEE Transactions on Information Forensics and Security, 2011, 6, 498-512.	6.9	24
130	Secure localization with attack detection in wireless sensor networks. International Journal of Information Security, 2011, 10, 155-171.	3.4	30
131	Message from the Guest Editors. International Journal of Information Security, 2011, 10, 267-268.	3.4	0
132	Better security enforcement in trusted computing enabled heterogeneous wireless sensor networks. Security and Communication Networks, 2011, 4, 11-22.	1.5	9
133	Secure SCADA framework for the protection of energy control systems. Concurrency Computation Practice and Experience, 2011, 23, 1431-1442.	2.2	20
134	Secure mobile subscription of sensor-encrypted data. , 2011, , .		4
135	Compact identity-based encryption without strong symmetric cipher. , 2011, , .		2
136	Forward Secure Ring Signature without Random Oracles. Lecture Notes in Computer Science, 2011, , 1-14.	1.3	22
137	Guest editors' preface. Journal of Computer Security, 2011, 19, 227-228.	0.8	0
138	Threshold ring signature without random oracles. , 2011, , .		14
139	Identity-Based Server-Aided Decryption. Lecture Notes in Computer Science, 2011, , 337-352.	1.3	8
140	On Shortening Ciphertexts: New Constructions for Compact Public Key and Stateful Encryption Schemes. Lecture Notes in Computer Science, 2011, , 302-318.	1.3	4
141	Efficient online/offline identity-based signature for wireless sensor network. International Journal of Information Security, 2010, 9, 287-296.	3.4	117
142	Time-Bound Hierarchical Key Assignment: An Overview. IEICE Transactions on Information and Systems, 2010, E93-D, 1044-1052.	0.7	5
143	Towards practical anonymous password authentication. , 2010, , .		16
144	Practical ID-based encryption for wireless sensor network. , 2010, , .		27

#	Article	IF	Citations
145	Authentication and Key Establishment in Dynamic Wireless Sensor Networks. Sensors, 2010, 10, 3718-3731.	3.8	31
146	Short Generic Transformation to Strongly Unforgeable Signature in the Standard Model. Lecture Notes in Computer Science, 2010, , 168-181.	1.3	3
147	An Agent-Mediated Fair Exchange Protocol. Lecture Notes in Computer Science, 2010, , 235-250.	1.3	2
148	Optionally Identifiable Private Handshakes. Lecture Notes in Computer Science, 2010, , 164-178.	1.3	0
149	Non-Repudiation. Chapman & Hall/CRC Cryptography and Network Security, 2010, , 83-108.	0.1	0
150	Security and Correctness Analysis on Privacy-Preserving k-Means Clustering Schemes. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 1246-1250.	0.3	6
151	Multiparty nonrepudiation. ACM Computing Surveys, 2009, 41, 1-43.	23.0	24
152	Fair and Secure Mobile Billing Systems. Wireless Personal Communications, 2009, 51, 81-93.	2.7	8
153	A New Approach for Anonymous Password Authentication. , 2009, , .		17
154	Achieving Better Privacy Protection in Wireless Sensor Networks Using Trusted Computing. Lecture Notes in Computer Science, 2009, , 384-395.	1.3	3
155	A New Variant of the Cramer-Shoup KEM Secure against Chosen Ciphertext Attack. Lecture Notes in Computer Science, 2009, , 143-155.	1.3	8
156	Conditional Proxy Broadcast Re-Encryption. Lecture Notes in Computer Science, 2009, , 327-342.	1.3	76
157	Hierarchical Self-healing Key Distribution for Heterogeneous Wireless Sensor Networks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2009, , 285-295.	0.3	8
158	Computationally Secure Hierarchical Self-healing Key Distribution for Heterogeneous Wireless Sensor Networks. Lecture Notes in Computer Science, 2009, , 135-149.	1.3	4
159	Online/Offline Ring Signature Scheme. Lecture Notes in Computer Science, 2009, , 80-90.	1.3	7
160	Certificate-based sequential aggregate signature. , 2009, , .		94
161	Distributed Noise Generation for Density Estimation Based Clustering without Trusted Third Party. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 1868-1871.	0.3	0
162	Self-enforcing Private Inference Control. Lecture Notes in Computer Science, 2009, , 260-274.	1.3	0

#	Article	IF	Citations
163	A practical SSL server performance improvement algorithm based on batch RSA decryption. Journal of Shanghai Jiaotong University (Science), 2008, 13, 67-70.	0.9	2
164	Achieving evenhandedness in certified email system for contract signing. International Journal of Information Security, 2008, 7, 383-394.	3.4	4
165	Realizing Stateful Public Key Encryption in Wireless Sensor Network. International Federation for Information Processing, 2008, , 95-107.	0.4	9
166	Using Trusted Computing Technology to Facilitate Security Enforcement in Wireless Sensor Networks. , 2008, , .		3
167	Trusted Connection between Mobile Nodes and Mobility Anchor Points in Hierarchical Mobile IPv6. , 2008, , .		0
168	A New Scheme for Distributed Density Estimation based Privacy-Preserving Clustering. , 2008, , .		5
169	Enforcing trust in pervasive computing. International Journal of System of Systems Engineering, 2008, 1, 96.	0.5	0
170	An Asynchronous Node Replication Attack in Wireless Sensor Networks. International Federation for Information Processing, 2008, , 125-139.	0.4	3
171	Efficient Certificate-Based Encryption in the Standard Model. Lecture Notes in Computer Science, 2008, , 144-155.	1.3	20
172	Constructing Strong KEM from Weak KEM (or How to Revive the KEM/DEM Framework). Lecture Notes in Computer Science, 2008, , 358-374.	1.3	8
173	Certificate-Based Signature Schemes without Pairings or Random Oracles. Lecture Notes in Computer Science, 2008, , 285-297.	1.3	37
174	Generic Constructions of Stateful Public Key Encryption and Their Applications. Lecture Notes in Computer Science, 2008, , 75-93.	1.3	8
175	Two-Party Privacy-Preserving Agglomerative Document Clustering. , 2007, , 193-208.		6
176	Privacy-Preserving Two-Party K-Means Clustering via Secure Approximation. , 2007, , .		16
177	New constructions of fuzzy identity-based encryption. , 2007, , .		47
178	An effective multi-layered defense framework against spam. Information Security Technical Report, 2007, 12, 179-185.	1.3	6
179	A secure double auction protocol against false bids. Decision Support Systems, 2007, 44, 147-158.	5.9	1
180	Integration of non-repudiation services in mobile DRM scenarios. Telecommunication Systems, 2007, 35, 161-176.	2.5	4

#	Article	IF	Citations
181	Evaluating the Effects of Model Generalization on Intrusion Detection Performance. International Federation for Information Processing, 2007, , 421-432.	0.4	0
182	Optimized multiâ€party certified email protocols. Information Management and Computer Security, 2005, 13, 350-366.	1.2	13
183	An Evenhanded Certified Email System for Contract Signing. Lecture Notes in Computer Science, 2005, , 1-13.	1.3	5
184	Agent-mediated non-repudiation protocols. Electronic Commerce Research and Applications, 2004, 3, 152-162.	5.0	10
185	Non-repudiation protocols for multiple entities. Computer Communications, 2004, 27, 1608-1616.	5.1	13
186	Practical Service Charge for P2P Content Distribution. Lecture Notes in Computer Science, 2003, , 112-123.	1.3	5
187	An intensive survey of fair non-repudiation protocols. Computer Communications, 2002, 25, 1606-1621.	5.1	225
188	Some Remarks on a Fair Exchange Protocol. Lecture Notes in Computer Science, 2000, , 46-57.	1.3	56
189	Electronic Payment Systems with Fair On-line Verification. IFIP Advances in Information and Communication Technology, 2000, , 451-460.	0.7	3
190	Undeniable billing in mobile communication. , 1998, , .		24
191	Evidence and non-repudiation. Journal of Network and Computer Applications, 1997, 20, 267-281.	9.1	62
192	A fair non-repudiation protocol. , 0, , .		98
193	Intermediary non-repudiation protocols. , 0, , .		7
194	Protecting all traffic channels in mobile IPv6 network. , 0, , .		3