Josef P Pieprzyk

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/3313822/publications.pdf

Version: 2024-02-01

		218381	253896
208 papers	3,093 citations	26 h-index	43 g-index
226 all docs	226 docs citations	226 times ranked	1583 citing authors

#	Article	IF	Citations
1	Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. Lecture Notes in Computer Science, 2002, , 267-287.	1.0	388
2	Fundamentals of Computer Security. , 2003, , .		162
3	Universal Designated-Verifier Signatures. Lecture Notes in Computer Science, 2003, , 523-542.	1.0	138
4	Efficient Extension of Standard Schnorr/RSA Signatures into Universal Designated-Verifier Signatures. Lecture Notes in Computer Science, 2004, , 86-100.	1.0	71
5	Biosynthesis of 11-deoxycorticosteroids by teleost ovaries and discussion of their possible role in oocyte maturation and ovulation. General and Comparative Endocrinology, 1973, 21, 168-178.	0.8	69
6	A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion. IEEE Transactions on Information Forensics and Security, 2015, 10, 1193-1206.	4.5	59
7	Towards effective nonlinear cryptosystem design. IEE Proceedings E: Computers and Digital Techniques, 1988, 135, 325.	0.1	58
8	Permutation polynomials of the form <mml:math altimg="si1.gif" overflow="scroll" xmlns:xocs="http://www.elsevier.com/xml/xocs/dtd" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://www.elsevier.com/xml/ja/dtd" xmlns:ja="http://www.elsevier.com/xml/ja/dtd" xmlns:mml="http://www.w3.org/1998/Math/MathML" xmlns:tb="http://www.elsevier.com/xml/common/table/dtd" xmlns:sb="http://www.elsevier.com/xml/common/struct-bib/dtd" xmlns:ce="http://www.elsevier.. Finite	0.6	55
9	Keyword Field-Free Conjunctive Keyword Searches on Encrypted Data and Extension for Dynamic Groups. Lecture Notes in Computer Science, 2008, , 178-195.	1.0	55
10	Cube Attacks and Cube-Attack-Like Cryptanalysis on the Round-Reduced Keccak Sponge Function. Lecture Notes in Computer Science, 2015, , 733-761.	1.0	45
11	Dynamic Searchable Symmetric Encryption Schemes Supporting Range Queries with Forward (and) Tj ETQq1 1 0.784314 rgBT /Overlo	1.0	43
12	Dynamic Searchable Symmetric Encryption with Forward and Stronger Backward Privacy. Lecture Notes in Computer Science, 2019, , 283-303.	1.0	40
13	Distributed Private Matching and Set Operations. , 2008, , 347-360.		37
14	Lattice-Based Threshold Changeability for Standard Shamir Secret-Sharing Schemes. IEEE Transactions on Information Theory, 2007, 53, 2542-2559.	1.5	35
15	Characterising and predicting cyber attacks using the Cyber Attacker Model Profile (CAMP). Journal of Money Laundering Control, 2012, 15, 430-441.	0.7	35
16	An Efficient Authentication Scheme for Intra-Vehicular Controller Area Network. IEEE Transactions on Information Forensics and Security, 2020, 15, 3107-3122.	4.5	34
17	Homogeneous bent functions. Discrete Applied Mathematics, 2000, 102, 133-139.	0.5	33
18	How to Construct Pseudorandom Permutations from Single Pseudorandom Functions. Lecture Notes in Computer Science, 1991, , 140-150.	1.0	33

#	ARTICLE	IF	CITATIONS
19	Efficient One-Time Proxy Signatures. Lecture Notes in Computer Science, 2003, , 507-522.	1.0	32
20	Lattice-based threshold-changeability for standard CRT secret-sharing schemes. Finite Fields and Their Applications, 2006, 12, 653-680.	0.6	31
21	Conference Key Agreement from Secret Sharing. Lecture Notes in Computer Science, 1999, , 64-76.	1.0	31
22	Rotational Cryptanalysis of Round-Reduced Keccak. Lecture Notes in Computer Science, 2014, , 241-262.	1.0	31
23	Multiparty key agreement protocols. IEE Proceedings: Computers and Digital Techniques, 2000, 147, 229.	1.6	30
24	Identification of Bad Signatures in Batches. Lecture Notes in Computer Science, 2000, , 28-45.	1.0	30
25	New constructions of anonymous membership broadcasting schemes. Advances in Mathematics of Communications, 2007, 1, 29-44.	0.4	30
26	Broadcast anti-jamming systems. Computer Networks, 2001, 35, 223-236.	3.2	29
27	Homogeneous bent functions of degree n in 2n variables do not exist for n>3. Discrete Applied Mathematics, 2004, 142, 127-132.	0.5	28
28	Changing Thresholds in the Absence of Secure Channels. Lecture Notes in Computer Science, 1999, , 177-191.	1.0	27
29	Corticosteroidogenesis in Vitro by the Head Kidney of<i>Tilapia mossambica</i>(Cichlidae, Teleostei)1. Endocrinology, 1972, 91, 450-462.	1.4	26
30	Threshold Privacy Preserving Keyword Searches. , 2008, , 646-658.		25
31	Cryptanalysis of WG-7: a lightweight stream cipher. Cryptography and Communications, 2012, 4, 277-285.	0.9	24
32	On-the-fly web content integrity check boosts users' confidence. Communications of the ACM, 2002, 45, 33-37.	3.3	24
33	Reversible and Blind Database Watermarking Using Difference Expansion. International Journal of Digital Crime and Forensics, 2009, 1, 42-54.	0.5	22
34	Database Relation Watermarking Resilient against Secondary Watermarking Attacks. Lecture Notes in Computer Science, 2009, , 222-236.	1.0	21
35	On the Provable Security of an Efficient RSA-Based Pseudorandom Generator. Lecture Notes in Computer Science, 2006, , 194-209.	1.0	21
36	Reversible And Blind Database Watermarking Using Difference Expansion. , 2008, , .		21

#	Article	IF	Citations
37	SAT-based Cryptanalysis of Authenticated Ciphers from the CAESAR Competition. , 2017, , .		21
38	Conditionally secure secret sharing schemes with disenrollment capability. , 1994, , .		20
39	Forward and Backward Private DSSE for Range Queries. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 328-338.	3.7	20
40	Multiple-Time Signature Schemes against Adaptive Chosen Message Attacks. Lecture Notes in Computer Science, 2004, , 88-100.	1.0	20
41	An Efficient Scheme of Common Secure Indices for Conjunctive Keyword-Based Retrieval on Encrypted Data. Lecture Notes in Computer Science, 2009, , 145-159.	1.0	19
42	Provably secure three-party key agreement protocol using Chebyshev chaotic maps in the standard model. Nonlinear Dynamics, 2014, 77, 1427-1439.	2.7	19
43	Broadcast Authentication in Latency-Critical Applications: On the Efficiency of IEEE 1609.2. IEEE Transactions on Vehicular Technology, 2019, 68, 11577-11587.	3.9	19
44	Steroid transformations by the corpuscles of Stannius and the body kidney of Salmo gairdnerii (Teleostei). General and Comparative Endocrinology, 1971, 16, 74-84.	0.8	18
45	Hybrid threshold adaptable quantum secret sharing scheme with reverse Huffman-Fibonacci-tree coding. Scientific Reports, 2016, 6, 31350.	1.6	18
46	Rotational Cryptanalysis of ARX Revisited. Lecture Notes in Computer Science, 2015, , 519-536.	1.0	18
47	Case-based reasoning for intrusion detection. , 0, , .		17
48	Continuous authentication for VANET. Vehicular Communications, 2020, 25, 100255.	2.7	17
49	Common Secure Index for Conjunctive Keyword-Based Retrieval over Encrypted Data. Lecture Notes in Computer Science, 2007, , 108-123.	1.0	17
50	Binary Image Steganographic Techniques Classification Based on Multi-class Steganalysis. Lecture Notes in Computer Science, 2010, , 341-358.	1.0	16
51	A Non-malleable Group Key Exchange Protocol Robust Against Active Insiders. Lecture Notes in Computer Science, 2006, , 459-475.	1.0	16
52	Investigating Cube Attacks on the Authenticated Encryption Stream Cipher ACORN. Communications in Computer and Information Science, 2016, , 15-26.	0.4	16
53	Controllable quantum private queries using an entangled Fibonacci-sequence spiral source. Physics Letters, Section A: General, Atomic and Solid State Physics, 2015, 379, 2561-2568.	0.9	15
54	A Construction for Super Pseudorandom Permutations from A Single Pseudorandom Function. , 1992, , 267-284.		14

#	Article	IF	Citations
55	Lattice-Based Threshold-Changeability for Standard Shamir Secret-Sharing Schemes. Lecture Notes in Computer Science, 2004, , 170-186.	1.0	14
56	Winning the Phishing War: A Strategy for Australia. , 2010, , .		14
57	Quantum direct secret sharing with efficient eavesdropping-check and authentication based on distributed fountain codes. Quantum Information Processing, 2014, 13, 895-907.	1.0	14
58	A New Dynamic Accumulator for Batch Updates. Lecture Notes in Computer Science, 2007, , 98-112.	1.0	14
59	Known and Chosen Key Differential Distinguishers for Block Ciphers. Lecture Notes in Computer Science, 2011, , 29-48.	1.0	14
60	A message authentication code based on latin squares. Lecture Notes in Computer Science, 1997, , 194-203.	1.0	13
61	On the Security of PAS (Predicate-Based Authentication Service). , 2009, , .		13
62	Blind Steganalysis: A Countermeasure for Binary Image Steganography. , 2010, , .		13
63	ICEPOLE: High-Speed, Hardware-Oriented Authenticated Encryption. Lecture Notes in Computer Science, 2014, , 392-413.	1.0	13
64	A New Human Identification Protocol and Coppersmithâ€™s Baby-Step Giant-Step Algorithm. Lecture Notes in Computer Science, 2010, , 349-366.	1.0	13
65	An improved coding method of quantum key distribution protocols based on Fibonacci-valued OAM entangled states. Physics Letters, Section A: General, Atomic and Solid State Physics, 2017, 381, 2922-2926.	0.9	12
66	Compcryptâ€"Lightweight ANS-Based Compression and Encryption. IEEE Transactions on Information Forensics and Security, 2021, 16, 3859-3873.	4.5	11
67	Authentication strategies in vehicular communications: a taxonomy and framework. Eurasip Journal on Wireless Communications and Networking, 2021, 2021, .	1.5	11
68	Authenticating Multicast Streams in Lossy Channels Using Threshold Techniques. Lecture Notes in Computer Science, 2001, , 239-249.	1.0	11
69	Converse Results to the Wiener Attack on RSA. Lecture Notes in Computer Science, 2005, , 184-198.	1.0	11
70	On the (In)Security of IDEA in Various Hashing Modes. Lecture Notes in Computer Science, 2012, , 163-179.	1.0	11
71	Rotation-symmetric functions and fast hashing. Lecture Notes in Computer Science, 1998, , 169-180.	1.0	10
72	Analysis of bilinear pairing-based accumulator for identity escrowing. IET Information Security, 2008, 2, 99.	1.1	10

#	Article	IF	Citations
73	Multi-party computation with conversion of secret sharing. Designs, Codes, and Cryptography, 2012, 62, 259-272.	1.0	10
74	Lattice-based certificateless public-key encryption in the standard model. International Journal of Information Security, 2014, 13, 315-333.	2.3	10
75	The resistance of PRESENT-80 against related-key differential attacks. Cryptography and Communications, 2014, 6, 171-187.	0.9	10
76	An efficient quantum blind digital signature scheme. Science China Information Sciences, 2017, 60, 1.	2.7	10
77	A differential fault attack on the WG family of stream ciphers. Journal of Cryptographic Engineering, 2020, 10, 189-195.	1.5	10
78	On Algebraic Immunity and Annihilators. Lecture Notes in Computer Science, 2006, , 65-80.	1.0	10
79	Threshold MACs. Lecture Notes in Computer Science, 2003, , 237-252.	1.0	10
80	Secret sharing in hierarchical groups. Lecture Notes in Computer Science, 1997, , 81-86.	1.0	9
81	An On-Line Secure E-Passport Protocol. , 2008, , 14-28.		9
82	Estimating Hidden Message Length in Binary Image Embedded by Using Boundary Pixels Steganography. , 2010, , .		9
83	Cryptanalysis of the convex hull click human identification protocol. International Journal of Information Security, 2013, 12, 83-96.	2.3	9
84	On the Linearization of Human Identification Protocols: Attacks Based on Linear Algebra, Coding Theory, and Lattices. IEEE Transactions on Information Forensics and Security, 2015, 10, 1643-1655.	4.5	9
85	A Model to Evaluate Reliability of Authentication Protocols in C-ITS Safety-Critical Applications. IEEE Transactions on Vehicular Technology, 2021, 70, 9306-9319.	3.9	9
86	On the Symmetric Property of Homogeneous Boolean Functions. Lecture Notes in Computer Science, 1999, , 26-35.	1.0	9
87	Cube attacks on round-reduced TinyJAMBU. Scientific Reports, 2022, 12, 5317.	1.6	9
88	A multi-level view model for secure object-oriented databases. Data and Knowledge Engineering, 1997, 23, 97-117.	2.1	8
89	Source Code Watermarking Based on Function Dependency Oriented Sequencing. , 2008, , .		8
90	Cryptanalysis of RC4(n, m) stream cipher. , 2013, , .		8

#	Article	IF	Citations
91	Investigating Cube Attacks on the Authenticated Encryption Stream Cipher MORUS. , 2017, , .		8
92	High-capacity (2,3) threshold quantum secret sharing based on asymmetric quantum lossy channels. Quantum Information Processing, 2020, 19, 1.	1.0	8
93	Random Differential Fault Attacks on the Lightweight Authenticated Encryption Stream Cipher Grain-128AEAD. IEEE Access, 2021, 9, 72568-72586.	2.6	8
94	Codes Identifying Bad Signatures in Batches. Lecture Notes in Computer Science, 2000, , 143-154.	1.0	8
95	Cheating Prevention in Linear Secret Sharing. Lecture Notes in Computer Science, 2002, , 121-135.	1.0	8
96	Efficient Disjointness Tests for Private Datasets. Lecture Notes in Computer Science, 2008, , 155-169.	1.0	8
97	On Secure Multi-party Computation in Black-Box Groups. , 2007, , 591-612.		8
98	Multiple Modular Additions and Crossword Puzzle Attack on NLSv2. Lecture Notes in Computer Science, 2007, , 230-248.	1.0	8
99	Security Evaluation of Rakaposhi Stream Cipher. Lecture Notes in Computer Science, 2013, , 361-371.	1.0	8
100	Puncturable Encryption: A Generic Construction from Delegatable Fully Key-Homomorphic Encryption. Lecture Notes in Computer Science, 2020, , 107-127.	1.0	8
101	On necessary and sufficient conditions for the construction of super pseudorandom permutations. Lecture Notes in Computer Science, 1993, , 194-209.	1.0	7
102	Broadcast anti-jamming systems. , 0, , .		7
103	An Efficient eAuction Protocol. , 2007, , .		7
104	Unconditionally secure disjointness tests for private datasets. International Journal of Applied Cryptography, 2009, 1, 225.	0.4	7
105	Graph Coloring Applied to Secure Computation in Non-Abelian Groups. Journal of Cryptology, 2012, 25, 557-600.	2.1	7
106	On the Efficiency of Pairing-Based Authentication for Connected Vehicles: Time is Not on Our Side!. IEEE Transactions on Information Forensics and Security, 2021, 16, 3678-3693.	4.5	7
107	Cryptanalysis of FORK-256. Lecture Notes in Computer Science, 2007, , 19-38.	1.0	7
108	Comments on Soviet encryption algorithm. Lecture Notes in Computer Science, 1995, , 433-438.	1.0	6

#	ARTICLE	IF	CITATIONS
109	How to prevent cheating in Pinch's scheme. Electronics Letters, 1997, 33, 1453.	0.5	6
110	Privacy Enhanced Electronic Cheque System. , 0, , .		6
111	Decomposition Construction for Secret Sharing Schemes with Graph Access Structures in Polynomial Time. SIAM Journal on Discrete Mathematics, 2010, 24, 617-638.	0.4	6
112	Socio-technological phishing prevention. Information Security Technical Report, 2011, 16, 67-73.	1.3	6
113	Software Watermarking Resilient to Debugging Attacks. Journal of Multimedia, 2007, 2, .	0.3	6
114	Cryptography based on transcendental numbers. Lecture Notes in Computer Science, 1996, , 96-107.	1.0	5
115	On password-based authenticated key exchange using collisionful hash functions. Lecture Notes in Computer Science, 1996, , 299-310.	1.0	5
116	Generalised Cumulative Arrays in Secret Sharing. Designs, Codes, and Cryptography, 2006, 40, 191-209.	1.0	5
117	A Critical Look at Cryptographic Hash Function Literature. , 2008, , .		5
118	Protecting Web 2.0 Services from Botnet Exploitations. , 2010, , .		5
119	Critical analysis of spam prevention techniques. , 2011, , .		5
120	NTRUCCA: How to Strengthen NTRUEncrypt to Chosen-Ciphertext Security in the Standard Model. Lecture Notes in Computer Science, 2012, , 353-371.	1.0	5
121	Finding state collisions in the authenticated encryption stream cipher ACORN. , 2016, , .		5
122	Distinguishing Attack on SOBER-128 with Linear Masking. Lecture Notes in Computer Science, 2006, , 29-39.	1.0	5
123	Shared Generation of Pseudo-Random Functions with Cumulative Maps. Lecture Notes in Computer Science, 2003, , 281-295.	1.0	5
124	Efficient Fuzzy Matching and Intersection on Private Datasets. Lecture Notes in Computer Science, 2010, , 211-228.	1.0	5
125	Fail-Stop Threshold Signature Schemes Based on Elliptic Curves. Lecture Notes in Computer Science, 1999, , 103-116.	1.0	5
126	Crossword Puzzle Attack on NLS. Lecture Notes in Computer Science, 2007, , 249-265.	1.0	5

#	ARTICLE	IF	CITATIONS
127	RSA-based fail-stop signature schemes. , 0, , .		4
128	An attack-localizing watermarking scheme for natural language documents. , 2006, , .		4
129	Verifiable Multi-secret Sharing Schemes for Multiple Threshold Access Structures. Lecture Notes in Computer Science, 2007, , 167-181.	1.0	4
130	MÃ¶bius transforms, coincident Boolean functions and non-coincidence property of Boolean functions. International Journal of Computer Mathematics, 2011, 88, 1398-1416.	1.0	4
131	Security analysis of linearly filtered NLFSRs. Journal of Mathematical Cryptology, 2013, 7, 313-332.	0.4	4
132	Large-Capacity Three-Party Quantum Digital Secret Sharing Using Three Particular Matrices Coding. Communications in Theoretical Physics, 2016, 66, 501-508.	1.1	4
133	A Quantum Secret Sharing Scheme Using Orbital Angular Momentum onto Multiple Spin States Based on Fibonacci Compression Encoding. Communications in Theoretical Physics, 2018, 70, 384.	1.1	4
134	High-rate and high-capacity measurement-device-independent quantum key distribution with Fibonacci matrix coding in free space. Science China Information Sciences, 2018, 61, 1.	2.7	4
135	A large-alphabet three-party quantum key distribution protocol based on orbital and spin angular momenta hybrid entanglement. Quantum Information Processing, 2018, 17, 1.	1.0	4
136	Cryptanalysis of WG-8 and WG-16 stream ciphers. Cryptography and Communications, 2019, 11, 351-362.	0.9	4
137	Two types of dynamic quantum state secret sharing based on tensor networks states. Physica A: Statistical Mechanics and Its Applications, 2021, 582, 126257.	1.2	4
138	A Low-Cost Attack on Branch-Based Software Watermarking Schemes. Lecture Notes in Computer Science, 2006, , 282-293.	1.0	4
139	Authentication of Concast Communication. Lecture Notes in Computer Science, 2002, , 185-198.	1.0	4
140	Linear nonequivalence versus nonlinearity. Lecture Notes in Computer Science, 1993, , 156-164.	1.0	4
141	Extensions of the Cube Attack Based on Low Degree Annihilators. Lecture Notes in Computer Science, 2009, , 87-102.	1.0	4
142	Cryptanalysis of the Convex Hull Click Human Identification Protocol. Lecture Notes in Computer Science, 2011, , 24-30.	1.0	4
143	Multi-Party Computation with Omnipresent Adversary. Lecture Notes in Computer Science, 2009, , 180-195.	1.0	4
144	Low Probability Differentials and the Cryptanalysis of Full-Round CLEFIA-128. Lecture Notes in Computer Science, 2014, , 141-157.	1.0	4

#	Article	IF	Citations
145	On selectable collisionful hash functions. Lecture Notes in Computer Science, 1996, , 287-298.	1.0	3
146	A coding approach to the multicast stream authentication problem. International Journal of Information Security, 2008, 7, 265-283.	2.3	3
147	An Improved Distinguisher for Dragon. , 2008, , .		3
148	Can We CAN the Email Spam. , 2013, , .		3
149	Lattice-based completely non-malleable public-key encryption in the standard model. Designs, Codes, and Cryptography, 2014, 71, 293-313.	1.0	3
150	Fast and simple high-capacity quantum cryptography with error detection. Scientific Reports, 2017, 7, 46302.	1.6	3
151	Novel quantum key distribution with shift operations based on Fibonacci and Lucas valued orbital angular momentum entangled states. Physica A: Statistical Mechanics and Its Applications, 2020, 554, 124694.	1.2	3
152	A Strong Lightweight Authentication Protocol for Low-cost RFID Systems. International Journal of Security and Its Applications, 2014, 8, 225-234.	0.5	3
153	Trapdoor Delegation and HIBE from Middle-Product LWE in Standard Model. Lecture Notes in Computer Science, 2020, , 130-149.	1.0	3
154	Physical publicly verifiable randomness from pulsars. Astronomy and Computing, 2022, 38, 100549.	0.8	3
155	Features-Pooling Blind JPEG Image Steganalysis. , 2008, , .		2
156	A survey: Error control methods used in bio-cryptography. , 2014, , .		2
157	Dual compressible hybrid quantum secret sharing schemes based on extended unitary operations. , 2014, , .		2
158	Analysing recursive preprocessing of BKZ lattice reduction algorithm. IET Information Security, 2017, 11, 114-120.	1.1	2
159	Round-robin-differential-phase-shift quantum key distribution based on wavelength division multiplexing. Laser Physics Letters, 2018, 15, 115201.	0.6	2
160	Analysis of weighted quantum secret sharing based on matrix product states. Quantum Information Processing, 2020, 19, 1.	1.0	2
161	Democratic Systems. Lecture Notes in Computer Science, 2001, , 392-402.	1.0	2
162	Cryptanalysis of LASH. Lecture Notes in Computer Science, 2008, , 207-223.	1.0	2

#	Article	IF	Citations
163	Authentication of Transit Flows and K-Siblings One-Time Signature. IFIP Advances in Information and Communication Technology, 2002, , 41-55.	0.5	2
164	A Combinatorial Approach to Anonymous Membership Broadcast. Lecture Notes in Computer Science, 2002, , 162-170.	1.0	2
165	Lattice-Based Completely Non-malleable PKE in the Standard Model (Poster). Lecture Notes in Computer Science, 2011, , 407-411.	1.0	2
166	Active Security in Multiparty Computation over Black-Box Groups. Lecture Notes in Computer Science, 2012, , 503-521.	1.0	2
167	Quantum-key-expansion protocol based on number-state-entanglement-preserving tensor network with compression. Physical Review A, 2022, 105, .	1.0	2
168	ANS-based compression and encryption with 128-bit security. International Journal of Information Security, 2022, 21, 1051-1067.	2.3	2
169	Linear Secret Sharing with Divisible Shares. Lecture Notes in Computer Science, 1999, , 71-86.	1.0	1
170	Copyright Protection of Object-Oriented Software. Lecture Notes in Computer Science, 2002, , 186-199.	1.0	1
171	The eight variable homogeneous degree three bent functions. Journal of Discrete Algorithms, 2008, 6, 66-72.	0.7	1
172	Improvement of a Dynamic Accumulator at ICICS 07 and Its Application in Multi-user Keyword-Based Retrieval on Encrypted Data. , 2008, , .		1
173	JPEG Image Steganalysis Improvement Via Image-to-Image Variation Minimization. , 2008, , .		1
174	On the Hardness of the Sum of k Mins Problem. Computer Journal, 2011, 54, 1652-1660.	1.5	1
175	New security notions and relations for public-key encryption. Journal of Mathematical Cryptology, 2012, 6, 183-227.	0.4	1
176	Secure Computation of the Vector Dominance Problem. , 2008, , 319-333.		1
177	Verifiable Secret Sharing and Time Capsules. Lecture Notes in Computer Science, 2000, , 169-183.	1.0	1
178	An Ideal and Robust Threshold RSA. Lecture Notes in Computer Science, 2006, , 312-321.	1.0	1
179	Extending FORK-256 Attack to the Full Hash Function. Lecture Notes in Computer Science, 2007, , 296-305.	1.0	1
180	Parallel Signcryption. Information Security and Cryptography, 2010, , 175-192.	0.2	1

#	Article	IF	Citations
181	Truncated Differential Analysis of Reduced-Round LBlock. Lecture Notes in Computer Science, 2013, , 291-308.	1.0	1
182	Randomized Authentication Systems. , 1991, , 472-481.		1
183	Modeling a multi-level secure object-oriented database using views. Lecture Notes in Computer Science, 1996, , 190-206.	1.0	0
184	Evidential reasoning in network intrusion detection systems. Lecture Notes in Computer Science, 1996, , 253-265.	1.0	0
185	Securing Multicast Groups in Ad Hoc Networks. Lecture Notes in Computer Science, 2004, , 194-207.	1.0	0
186	Shared generation of pseudo-random functions. Journal of Complexity, 2004, 20, 458-472.	0.7	0
187	Evolution of cryptographic hashing. , 2010, , .		0
188	Privacy Enhancements for Hardware-Based Security Modules. Communications in Computer and Information Science, 2011, , 224-236.	0.4	0
189	Bucket attack on numeric set watermarking model and safeguards. Information Security Technical Report, 2011, 16, 59-66.	1.3	0
190	Predicting tours and probabilistic simulation for BKZ lattice reduction algorithm. , 2014, , .		0
191	Evaluating the performance of the practical lattice reduction algorithms. , 2014, , .		0
192	A subexponential construction of graph coloring for multiparty computation. Journal of Mathematical Cryptology, 2014, 8, 363-403.	0.4	0
193	Practical attack on NLM-MAC scheme. Information Processing Letters, 2014, 114, 547-550.	0.4	0
194	Special issue on trust and security in wireless sensor networks. Concurrency Computation Practice and Experience, 2015, 27, 3791-3793.	1.4	0
195	Optimizing preprocessing method of recursive-BKZ lattice reduction algorithm. , 2015, , .		0
196	A hybrid quantum key distribution protocol based on extended unitary operations and fountain codes. Quantum Information Processing, 2015, 14, 697-713.	1.0	0
197	State recovery attacks against Ï€-cipher. , 2016, , .		0
198	High-capacity quantum key distribution using Chebyshev-map values corresponding to Lucas numbers coding. Quantum Information Processing, 2016, 15, 4663-4679.	1.0	0

#	Article	IF	Citations
199	Efficient quantum key distribution using Fibonacci-number coding with a biased basis choice. Information Processing Letters, 2018, 134, 24-30.	0.4	0
200	Preprocessing optimisation: revisiting recursiveâ€BKZ lattice reduction algorithm. IET Information Security, 2018, 12, 551-557.	1.1	0
201	Tunable multi-party high-capacity quantum key distribution based on m-generalized Fibonacci sequences using golden coding. Quantum Information Processing, 2018, 17, 1.	1.0	0
202	Sâ€boxes representation and efficiency of algebraic attack. IET Information Security, 2019, 13, 448-458.	1.1	0
203	Characterisations of Extended Resiliency and Extended Immunity of S-Boxes. Lecture Notes in Computer Science, 2006, , 210-228.	1.0	0
204	Identifying Steganographic Payload Location in Binary Image. Lecture Notes in Computer Science, 2010, , 590-600.	1.0	0
205	Robust Numeric Set Watermarking: Numbers Donâ€™t Lie. Communications in Computer and Information Science, 2011, , 253-265.	0.4	0
206	Taxonomy and Control Measures of SPAM and SPIM. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2012, , 529-542.	0.2	0
207	Probabilistic Analysis of Elementary Randomizers. , 1991, , 542-546.		0
208	Inspiring Technologies for Digital Inclusivity - Preface. Journal of Telecommunications and Information Technology, 2022, 1, 1-2.	0.3	0