New hash functions and their use in authentication and

Journal of Computer and System Sciences
22, 265-279
DOI: 10.1016/0022-0000(81)90033-7

Citation Report

#	Article	IF	Citations
1	The theory of signature testing for VLSI. , 1982, , .		25
2	The program complexity of searching a table. , 1983, , .		7
3	Algorithms for Public Key Cryptosystems: Theory and Application. Advances in Computers, 1983, 22, 45-108.	1.2	2
4	How to Reduce your Enemyâ€™s Information (extended abstract). , 1985, , 468-476.		22
5	Privacy Amplification by Public Discussion. SIAM Journal on Computing, 1988, 17, 210-229.	0.8	694
6	Universal one-way hash functions and their cryptographic applications. , 1989, , .		532
7	Designing programs that check their work. , 1989, , .		207
8	A complexity theory of efficient parallel algorithms. Theoretical Computer Science, 1990, 71, 95-132.	0.5	168
9	Unique binary search tree representations and equality-testing of sets and sequences. , 1990, , .		12
10	Communication-space tradeoffs for unrestricted protocols. , 0, , .		3
11	Cryptography Based Data Security. Advances in Computers, 1990, 30, 171-222.	1.2	1
12	Unconditional Byzantine Agreement with good majority. , 1991, , 285-295.		8
13	Perfect cryptographic security from partially independent channels. , 1991, , .		30
15	Hash functions for information authentication. , 0, , .		4
16	Experimental quantum cryptography. Journal of Cryptology, 1992, 5, 3-28.	2.1	1,507
17	Representing sets with constant time equality testing. Journal of Algorithms, 1992, 13, 353-373.	0.9	10
18	Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 1992, 68, 3121-3124.	2.9	2,396
19	Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory, 1993, 39, 733-742.	1.5	1,581

#	Article	IF	Citations
20	Immunizing public key cryptosystems against chosen ciphertext attacks. IEEE Journal on Selected Areas in Communications, 1993, 11, 715-724.	9.7	47
21	Universal Hashing and Unconditional Authentication Codes. , 0, , .		1
22	Reusing Shares in Secret Sharing Schemes. Computer Journal, 1994, 37, 199-205.	1.5	16
23	Broadcast Encryption. , 1993, , 480-491.		658
24	Program result-checking: a theory of testing meets a test of theory. , 0, , .		20
25	An algorithm for dynamic subset and intersection testing. Theoretical Computer Science, 1994, 129, 397-406.	0.5	8
26	Universal hashing and authentication codes. Designs, Codes, and Cryptography, 1994, 4, 369-380.	1.0	178
27	A combinatorial characterization of certain universal classes of hash functions. Journal of Combinatorial Designs, 1994, 2, 161-166.	0.3	2
28	Combinatorial techniques for universal hashing. Journal of Computer and System Sciences, 1994, 48, 337-346.	0.9	40
29	An Integrity Check Value Algorithm for Stream Ciphers. , 1993, , 40-48.		34
30	Bounds on the probability of deception in multiple authentication. IEEE Transactions on Information Theory, 1994, 40, 1586-1591.	1.5	17
31	Secret-Key Reconciliation by Public Discussion. , 1993, , 410-423.		421
32	Unique Binary-Search-Tree Representations and Equality Testing of Sets and Sequences. SIAM Journal on Computing, 1994, 23, 24-44.	0.8	5
33	Communication-Space Tradeoffs for Unrestricted Protocols. SIAM Journal on Computing, 1994, 23, 652-661.	0.8	14
36	Generalized privacy amplification. IEEE Transactions on Information Theory, 1995, 41, 1915-1923.	1.5	1,045
37	Quantum Oblivious Mutual Identification. Lecture Notes in Computer Science, 1995, , 133-146.	1.0	37
38	Designing programs that check their work. Journal of the ACM, 1995, 42, 269-291.	1.8	271
39	Measurement of Complex Volume Elastic Modulus of Liquid by Holography. Japanese Journal of Applied Physics, 1995, 34, 2012-2017.	0.8	0

#	Article	IF	Citations
40	A2â€"codes from universal hash classes. Lecture Notes in Computer Science, 1995, , 311-318.	1.0	3
41	Bucket Hashing and its Application to Fast Message Authentication. Lecture Notes in Computer Science, 1995, , 29-42.	1.0	62
42	A secure and efficient conference key distribution system. Lecture Notes in Computer Science, 1995, , 275-286.	1.0	518
44	Quantum cryptography: How to beat the code breakers using quantum mechanics. Contemporary Physics, 1995, 36, 165-195.	0.8	86
45	Quantum cryptography. Contemporary Physics, 1995, 36, 149-163.	0.8	121
46	Chernoffâ€"Hoeffding Bounds for Applications with Limited Independence. SIAM Journal on Discrete Mathematics, 1995, 8, 223-250.	0.4	219
47	On the Composition of Zero-Knowledge Proof Systems. SIAM Journal on Computing, 1996, 25, 169-192.	0.8	280
49	On selectable collisionful hash functions. Lecture Notes in Computer Science, 1996, , 287-298.	1.0	3
50	On the cardinality of systematic authentication codes via error-correcting codes. IEEE Transactions on Information Theory, 1996, 42, 566-578.	1.5	34
51	A parallel tree difference algorithm. Information Processing Letters, 1996, 60, 231-235.	0.4	4
52	Universal Hash Functions from Exponential Sums over Finite Fields and Galois Rings. Lecture Notes in Computer Science, 1996, , 31-44.	1.0	22
54	Software reliability via run-time result-checking. Journal of the ACM, 1997, 44, 826-849.	1.8	144
55	On the construction of pseudo-random permutations. , 1997, , .		42
56	Efficient and secure conference-key distribution. Lecture Notes in Computer Science, 1997, , 119-129.	1.0	58
57	A message authentication code based on latin squares. Lecture Notes in Computer Science, 1997, , 194-203.	1.0	13
58	On the foundations of modern cryptography. Lecture Notes in Computer Science, 1997, , 46-74.	1.0	28
59	Efficient generation of shared RSA keys. Lecture Notes in Computer Science, 1997, , 425-439.	1.0	159
60	Unconditional security against memory-bounded adversaries. Lecture Notes in Computer Science, 1997, , 292-306.	1.0	109

#	Article	IF	Citations
61	Traceable visual cryptography. Lecture Notes in Computer Science, 1997, , 61-71.	1.0	10
62	New directions in cryptography: twenty some years later (or cryptograpy and complexity theory: a) Tj ETQq1 1 0.784314 rgBT /Overlo		8
63	About a method for distribution keys of a computer network using elliptic curves. , 0, , .		0
64	Fast message authentication using efficient polynomial evaluation. Lecture Notes in Computer Science, 1997, , 190-204.	1.0	15
65	Collision-Resistant hashing: Towards making UOWHFs practical. Lecture Notes in Computer Science, 1997, , 470-484.	1.0	120
66	MMH: Software message authentication in the Gbit/second rates. Lecture Notes in Computer Science, 1997, , 172-189.	1.0	104
68	Universal Hashing and Geometric Codes. Designs, Codes, and Cryptography, 1997, 11, 207-221.	1.0	23
69	Security analysis of the message authenticator algorithm (MAA). European Transactions on Telecommunications, 1997, 8, 455-470.	1.2	11
70	Multiround Unconditionally Secure Authentication. Designs, Codes, and Cryptography, 1998, 15, 67-86.	1.0	7
71	Quantum Cryptography on Optical Fiber Networks. Optical Fiber Technology, 1998, 4, 345-370.	1.4	55
72	An improved scheme for set equality testing and updating. Theoretical Computer Science, 1998, 201, 85-97.	0.5	1
73	On probabilities of hash value matches. Computers and Security, 1998, 17, 171-176.	4.0	16
74	Unconditionally secure entity authentication. , 0, , .		0
75	Robust and secure light-weight resource reservation for unicast IP traffic. , 0, , .		6
76	Provable security for block ciphers by decorrelation. Lecture Notes in Computer Science, 1998, , 249-275.	1.0	60
77	Cryptographic Primitives for Information Authentication â€" State of the Art. Lecture Notes in Computer Science, 1998, , 49-104.	1.0	13
78	Cryptanalysis of message authentication codes. Lecture Notes in Computer Science, 1998, , 55-65.	1.0	6
80	From unpredictability to indistinguishability: A simple construction of pseudo-random functions from MACs. Lecture Notes in Computer Science, 1998, , 267-282.	1.0	31

#	Article	IF	Citations
81	Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible. Lecture Notes in Computer Science, 1998, , 266-280.	1.0	54
82	The chain & sum primitive and its applications to MACs and stream ciphers. Lecture Notes in Computer Science, 1998, , 281-293.	1.0	14
83	Threshold traitor tracing. Lecture Notes in Computer Science, 1998, , 502-517.	1.0	68
84	Incremental Authentication of Tree-Structured Documents. Lecture Notes in Computer Science, 1999, , 275-283.	1.0	1
85	Trading off strength and performance in network authentication: experience with the ACSA project. , 0, , .		2
86	The State of Cryptographic Hash Functions. Lecture Notes in Computer Science, 1999, , 158-182.	1.0	40
87	Generalized beam-splitting attack in quantum cryptography with dim coherent states. Optics Communications, 1999, 169, 103-108.	1.0	32
88	Reliable communication over partially authenticated networks. Theoretical Computer Science, 1999, 220, 185-210.	0.5	24
89	Multireceiver Authentication Codes: Models, Bounds, Constructions, and Extensions. Information and Computation, 1999, 151, 148-172.	0.5	48
90	On the Construction of Pseudorandom Permutations: Lubyâ€"Rackoff Revisited. Journal of Cryptology, 1999, 12, 29-66.	2.1	226
91	Bucket Hashing and Its Application to Fast Message Authentication. Journal of Cryptology, 1999, 12, 91-115.	2.1	34
92	On the security of iterated message authentication codes. IEEE Transactions on Information Theory, 1999, 45, 188-199.	1.5	70
93	Strongly universal hashing and identification codes via channels. IEEE Transactions on Information Theory, 1999, 45, 2091-2095.	1.5	23
94	Quantum computers and quantum coherence. Journal of Magnetism and Magnetic Materials, 1999, 200, 202-218.	1.0	131
96	Quantum nonlocality without entanglement. Physical Review A, 1999, 59, 1070-1091.	1.0	829
97	Estimates for practical quantum cryptography. Physical Review A, 1999, 59, 3301-3319.	1.0	156
98	Information-Theoretic Cryptography. Lecture Notes in Computer Science, 1999, , 47-65.	1.0	33
99	Modern Cryptography, Probabilistic Proofs and Pseudorandomness. Algorithms and Combinatorics, 1999, , .	0.6	130

#	Article	IF	Citations
100	The Security of the Cipher Block Chaining Message Authentication Code. Journal of Computer and System Sciences, 2000, 61, 362-399.	0.9	357
101	Constructions of authentication codes from algebraic curves over finite fields. IEEE Transactions on Information Theory, 2000, 46, 886-892.	1.5	20
102	Tracing traitors. IEEE Transactions on Information Theory, 2000, 46, 893-910.	1.5	237
103	CBC MAC for Real-Time Data Sources. Journal of Cryptology, 2000, 13, 315-338.	2.1	96
104	Authority-based user authentication in quantum key distribution. Physical Review A, 2000, 62, .	1.0	93
105	Daylight Quantum Key Distribution over 1.6 km. Physical Review Letters, 2000, 84, 5652-5655.	2.9	159
106	Selected Areas in Cryptography. Lecture Notes in Computer Science, 2000, , .	1.0	5
107	The Physics of Quantum Information. , 2000, , .		1,218
108	Quantum cryptography for secure satellite communications. , 0, , .		17
109	A novel suite of tests for evaluating one-way hash functions for electronic commerce applications. , 0, , .		3
110	Security against individual attacks for realistic quantum key distribution. Physical Review A, 2000, 61, .	1.0	578
111	Free-space quantum key distribution in daylight. Journal of Modern Optics, 2000, 47, 549-562.	0.6	36
112	Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness. Lecture Notes in Computer Science, 2000, , 49-61.	1.0	25
113	Quantum key distribution over a 48 km optical fibre network. Journal of Modern Optics, 2000, 47, 533-547.	0.6	137
114	Unconditional security in quantum cryptography. Journal of the ACM, 2001, 48, 351-406.	1.8	709
115	Quantum authentication of classical messages. Physical Review A, 2001, 64, .	1.0	100
116	Almost k -Wise Independent Sample Spaces and Their Cryptologic Applications. Journal of Cryptology, 2001, 14, 231-253.	2.1	22
117	Broadcast authentication for group communication. Theoretical Computer Science, 2001, 269, 1-21.	0.5	19

#	Article	IF	Citations
118	Deterministic Dictionaries. Journal of Algorithms, 2001, 41, 69-85.	0.9	86
119	Combinatorial Bounds on Authentication Codes with Arbitration. Designs, Codes, and Cryptography, 2001, 22, 265-281.	1.0	9
120	Cryptographic quantum communication schemes for two-party addresser authentication. , 0, , .		0
122	Advances in Cryptology â€" EUROCRYPT 2001. Lecture Notes in Computer Science, 2001, , .	1.0	17
123	The faithfulness of abstract protocol analysis. , 2001, , .		23
124	Towards practical quantum key distribution: Theeqcspotsystem. Journal of Modern Optics, 2001, 48, 1943-1956.	0.6	1
125	Extracting quantum entanglement (general entanglement purification protocols). , 0, , .		5
126	Pseudorandomness and average-case complexity via uniform reductions. , 0, , .		24
127	Confidential multimedia communication in IP networks. , 0, , .		6
128	Qubit authentication. Physical Review A, 2002, 66, .	1.0	56
129	Practical free-space quantum key distribution over 10 km in daylight and at night. New Journal of Physics, 2002, 4, 43-43.	1.2	373
130	Introduction to Cryptography. Information Security and Cryptography, 2002, , .	0.2	125
131	Black-Box Concurrent Zero-Knowledge Requires (Almost) Logarithmically Many Rounds. SIAM Journal on Computing, 2002, 32, 1-47.	0.8	41
132	Authentication of quantum messages. , 0, , .		97
133	On the state of strength-three covering arrays. Journal of Combinatorial Designs, 2002, 10, 217-238.	0.3	108
134	Secrecy, Computational Loads and Rates in Practical Quantum Cryptography. Algorithmica, 2002, 34, 314-339.	1.0	16
135	Security of Practical Time-Reversed EPR Quantum Key Distribution. Algorithmica, 2002, 34, 340-365.	1.0	68
136	Qubit authentication. Physica A: Statistical Mechanics and Its Applications, 2002, 314, 130-139.	1.2	1

#	Article	IF	Citations
137	Oblivious Transfers and Privacy Amplification. Journal of Cryptology, 2003, 16, 219-237.	2.1	36
138	Decorrelation: A Theory for Block Cipher Security. Journal of Cryptology, 2003, 16, 249-286.	2.1	119
139	Logarithm cartesian authentication codes. Information and Computation, 2003, 184, 93-108.	0.5	15
140	Linear authentication codes: bounds and constructions. IEEE Transactions on Information Theory, 2003, 49, 866-872.	1.5	76
141	Non-cryptographic primitive for pseudorandom permutation. Theoretical Computer Science, 2003, 306, 139-154.	0.5	0
142	Security of the Bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel. Physical Review A, 2003, 67, .	1.0	20
143	Foundations of security for hash chains in ad hoc networks. , 0, , .		2
144	Fundamentals of Computer Security. , 2003, , .		162
145	Practical random number generation in software. , 0, , .		19
146	Selected Areas in Cryptography. Lecture Notes in Computer Science, 2003, , .	1.0	0
147	Quantum authentication with unitary coding sets. Journal of Modern Optics, 2003, 50, 1035-1047.	0.6	4
148	An adaptive algorithm for detection of duplicate records. , 0, , .		0
149	SIA. , 2003, , .		470
150	On the sample size of k-restricted min-wise independent permutations and other k-wise distributions. , 2003, , .		8
151	Quantum cryptography in practice. , 2003, , .		87
152	Neural network based benchmarks in the quality assessment of message digest algorithms for digital signatures based secure Internet communications. , 0, , .		0
153	How to Re-use Round Function in Super-Pseudorandom Permutation. Lecture Notes in Computer Science, 2004, , 224-235.	1.0	2
154	The faithfulness of abstract protocol analysis: Message authentication*. Journal of Computer Security, 2004, 12, 865-891.	0.5	7

#	Article	IF	Citations
155	CWC: AÂHigh-Performance Conventional Authenticated Encryption Mode. Lecture Notes in Computer Science, 2004, , 408-426.	1.0	66
156	Source coding using a class of universal hash functions. , 0, , .		0
157	Universal hash functions over GF (2/sup n/). , 0, , .		2
158	MULTIPLE TRANSITIVITY AND MIN-WISE INDEPENDENCE IN PERMUTATION GROUPS. Journal of Algebra and Its Applications, 2004, 03, 427-435.	0.3	2
159	Information Security and Privacy. Lecture Notes in Computer Science, 2004, , .	1.0	3
160	A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). ACM Transactions on Information and System Security, 2004, 7, 319-332.	4.5	78
161	On the Use of GF-Inversion as a Cryptographic Primitive. Lecture Notes in Computer Science, 2004, , 234-247.	1.0	8
162	On Universal Classes of Extremely Random Constant-Time Hash Functions. SIAM Journal on Computing, 2004, 33, 505-543.	0.8	73
163	A combined genetic optimization and multilayer perceptron methodology for efficient digital fingerprint modeling and evaluation in secure communications. , 2004, , .		0
164	Data stream algorithms for scalable bandwidth management. , 2004, , .		1
165	The Security and Performance of the Galois/Counter Mode (GCM) of Operation. Lecture Notes in Computer Science, 2004, , 343-355.	1.0	259
166	Detecting quantum correlations for quantum key distribution. , 2005, 5631, 9.		1
167	Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption. Lecture Notes in Computer Science, 2005, , 87-103.	1.0	170
168	Public-Key Steganography with Active Attacks. Lecture Notes in Computer Science, 2005, , 210-226.	1.0	46
169	On the Power of Quantum Memory. IEEE Transactions on Information Theory, 2005, 51, 2391-2401.	1.5	53
170	CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. Journal of Cryptology, 2005, 18, 111-131.	2.1	48
171	Efficient reliable communication over partially authenticated networks. Distributed Computing, 2005, 18, 1-19.	0.7	10
172	MRD Hashing. Designs, Codes, and Cryptography, 2005, 37, 229-242.	1.0	1

#	Article	IF	Citations
173	Foundations of Security for Hash Chains in Ad Hoc Networks. Cluster Computing, 2005, 8, 189-195.	3.5	6
174	Badger â€“ A Fast and Provably Secure MAC. Lecture Notes in Computer Science, 2005, , 176-191.	1.0	21
176	The Universal Composable Security of Quantum Key Distribution. Lecture Notes in Computer Science, 2005, , 386-406.	1.0	109
177	Stronger Security Bounds for Wegman-Carter-Shoup Authenticators. Lecture Notes in Computer Science, 2005, , 164-180.	1.0	44
178	A NOVEL PROTOCOL-AUTHENTICATION ALGORITHM RULING OUT A MAN-IN-THE MIDDLE ATTACK IN QUANTUM CRYPTOGRAPHY. International Journal of Quantum Information, 2005, 03, 225-231.	0.6	22
179	Authentication. , 2005, , 21-22.		0
180	Information-theoretic security proof for quantum-key-distribution protocols. Physical Review A, 2005, 72, .	1.0	353
181	The Complexity of Online Memory Checking. , 0, , .		58
182	The Poly1305-AES Message-Authentication Code. Lecture Notes in Computer Science, 2005, , 32-49.	1.0	193
183	Energy Scalable Universal Hashing. IEEE Transactions on Computers, 2005, 54, 1484-1495.	2.4	35
185	Efficient Authentication of Large, Dynamic Data Sets Using Galois/Counter Mode (GCM). , 0, , .		11
186	An introduction to quantum cryptography. Xrds, 2005, 11, 3-3.	0.2	20
187	Constructions of Almost Resilient Functions. Lecture Notes in Computer Science, 2005, , 236-246.	1.0	2
188	Universally Composable Privacy Amplification Against Quantum Adversaries. Lecture Notes in Computer Science, 2005, , 407-425.	1.0	162
189	A Variant of Poly1305 MAC and Its Security Proof. Lecture Notes in Computer Science, 2005, , 375-380.	1.0	1
190	New Proofs for NMAC and HMAC: Security Without Collision-Resistance. Lecture Notes in Computer Science, 2006, , 602-619.	1.0	204
192	Quantum cryptography. Progress in Optics, 2006, 49, 381-454.	0.4	94
193	Stream-Based Implementation of Hash Functions for Multi-Gigabit Message Authentication Codes. , 2006, , .		6

#	Article	IF	Citations
196	An Efficient One-key Carter-Wegman Message Authentication Code. , 2006, , .		3
197	FUNCTION FIELDS OVER FINITE FIELDS AND THEIR APPLICATIONS TO CRYPTOGRAPHY. , 2006, , 59-104.		3
198	A High-Speed Hardware Architecture for Universal Message Authentication Code. IEEE Journal on Selected Areas in Communications, 2006, 24, 1831-1839.	9.7	9
199	Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets. Lecture Notes in Computer Science, 2006, , 232-250.	1.0	91
201	Security aspects of the authentication used in quantum key growing. , 2006, 6399, 131.		0
202	Theory of Quantum Key Distribution (QKD). , 0, , 271-284.		3
203	Variationally universal hashing. Information Processing Letters, 2006, 100, 36-39.	0.4	3
204	Quantum identity authentication based on ping-pong technique for photons. Physics Letters, Section A: General, Atomic and Solid State Physics, 2006, 356, 199-205.	0.9	71
205	Secret sharing schemes with partial broadcast channels. Designs, Codes, and Cryptography, 2006, 41, 5-22.	1.0	5
206	Secret keys from quantum correlations. Computer Science - Research and Development, 2006, 21, 29-37.	0.9	1
207	Efficient anonymity schemes for clustered wireless sensor networks. International Journal of Sensor Networks, 2006, 1, 50.	0.2	63
208	High-throughput sketch update on a low-power stream processor. , 2006, , .		12
211	Unconditionally secure ring authentication. , 2007, , .		2
212	Pseudo-random number generation for sketch-based estimations. ACM Transactions on Database Systems, 2007, 32, 11.	1.5	17
213	Alpaca. , 2007, , .		21
214	Microstructural Investigation of Se_xTe_{100-x} Thin Films Deposited on Si(100) Substrates by X-ray Diffractometer and Transmission Electron Microscopy Analysis. Japanese Journal of Applied Physics, 2007, 46, 7392.	0.8	1
215	Linear probing with constant independence. , 2007, , .		16
216	Protecting XML Databases against Ontology-Based Inference Attack. , 2007, , .		1

#	Article	IF	Citations
217	Privacy amplification for quantum key distribution. Journal of Physics A: Mathematical and Theoretical, 2007, 40, F99-F104.	0.7	10
218	Quantum technology and cryptology for information security. , 2007, , .		0
219	Chosenâ€Ciphertext Security from Identityâ€Based Encryption. SIAM Journal on Computing, 2007, 36, 1301-1328.	0.8	220
221	A Single Key MAC Based on Hash127. , 2007, , .		1
222	An introduction to modern cryptology. , 2007, , 565-592.		1
223	SIA: Secure information aggregation in sensor networks. Journal of Computer Security, 2007, 15, 69-102.	0.5	116
224	Counting distinct items over update streams. Theoretical Computer Science, 2007, 378, 211-222.	0.5	29
225	A survey of recent developments in cryptographic algorithms for smart cards. Computer Networks, 2007, 51, 2223-2233.	3.2	16
226	Cryptography on a Speck of Dust. Computer, 2007, 40, 38-44.	1.2	34
227	A Generic Construction of Cartesian Authentication Codes. IEEE Transactions on Information Theory, 2007, 53, 2229-2235.	1.5	83
228	Source Coding Using Families of Universal Hash Functions. IEEE Transactions on Information Theory, 2007, 53, 3226-3233.	1.5	8
229	On Defining Partition Entropy by Inequalities. IEEE Transactions on Information Theory, 2007, 53, 3233-3239.	1.5	9
230	Constructions of vector output Boolean functions with high generalized nonlinearity. Journal of China Universities of Posts and Telecommunications, 2008, 15, 77-81.	0.8	0
231	Security Aspects of the Authentication Used in Quantum Cryptography. IEEE Transactions on Information Theory, 2008, 54, 1735-1741.	1.5	41
232	Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models. IEEE Transactions on Information Theory, 2008, 54, 2408-2425.	1.5	10
233	Wireless Information-Theoretic Security. IEEE Transactions on Information Theory, 2008, 54, 2515-2534.	1.5	1,522
234	Distributed QAM-Based Space-Time Block Codes for Efficient Cooperative Multiple-Access Communication. IEEE Transactions on Information Theory, 2008, 54, 4342-4354.	1.5	10
235	Trusted-HB: A Low-Cost Version of HB$^+$ Secure Against Man-in-the-Middle Attacks. IEEE Transactions on Information Theory, 2008, 54, 4339-4342.	1.5	48

#	Article	IF	Citations
236	Authenticating ad hoc networks by comparison of short digests. Information and Computation, 2008, 206, 250-271.	0.5	33
237	Information Security. Lecture Notes in Computer Science, 2008, , .	1.0	0
238	Uniform Hashing in Constant Time and Optimal Space. SIAM Journal on Computing, 2008, 38, 85-96.	0.8	56
239	Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM Journal on Computing, 2008, 38, 97-139.	0.8	1,172
240	SECURITY OF QUANTUM KEY DISTRIBUTION. International Journal of Quantum Information, 2008, 06, 1-127.	0.6	416
241	Randomized Synopses for Query Assurance on Data Streams. , 2008, , .		14
242	Wireless network secrecy with public feedback. , 2008, , .		0
243	Extracting classical randomness in a quantum world. , 2008, , .		1
244	Comment on â€œArbitrated quantum-signature schemeâ€• Physical Review A, 2008, 77, .	1.0	76
245	On the Relative Efficiency of Resolution-Like Proofs and Ordered Binary Decision Diagram Proofs. , 2008, , .		4
246	Games for exchanging information. , 2008, , .		66
248	Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. Physical Review Letters, 2008, 100, 200501.	2.9	249
249	Classification of Hash Functions Suitable for Real-Life Systems. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2008, E91-A, 64-73.	0.2	4
251	Protection relay systems employing unconditionally secure authentication codes. , 2009, , .		5
252	Optimal secure message transmission by public discussion. , 2009, , .		6
253	Secrecy Extraction from Increased Randomness in a Time-Variant MIMO Channel. , 2009, , .		6
254	Secure authentication of classical messages with single photons. Chinese Physics B, 2009, 18, 3189-3192.	0.7	19
255	An Implementation of Post-Processing Software in Quantum Key Distribution. , 2009, , .		5

#	Article	IF	Citations
256	Practical long-distance quantum key distribution system using decoy levels. New Journal of Physics, 2009, 11, 045009.	1.2	63
257	Distributed authentication for randomly compromised networks. New Journal of Physics, 2009, 11, 085005.	1.2	1
258	Small synopses for group-by query verification on outsourced data streams. ACM Transactions on Database Systems, 2009, 34, 1-42.	1.5	25
259	Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD. New Journal of Physics, 2009, 11, 055051.	1.2	45
260	Composability in quantum cryptography. New Journal of Physics, 2009, 11, 085006.	1.2	107
261	VULNERABILITY OF "A NOVEL PROTOCOL-AUTHENTICATION ALGORITHM RULING OUT A MAN-IN-THE-MIDDLE ATTACK IN QUANTUM CRYPTOGRAPHY". International Journal of Quantum Information, 2009, 07, 1047-1052.	0.6	9
262	RESPONSE TO "VULNERABILITY OF 'A NOVEL PROTOCOL-AUTHENTICATION ALGORITHM RULING OUT A MAN-IN-THE-MIDDLE ATTACK IN QUANTUM CRYPTOGRAPHY'". International Journal of Quantum Information, 2009, 07, 1401-1407.	0.6	7
263	Hierarchical Sampling from Sketches: EstimatingÂFunctions over Data Streams. Algorithmica, 2009, 53, 549-582.	1.0	4
264	Eavesdropping on secure quantum telephone protocol with dishonest server. Optics Communications, 2009, 282, 3375-3378.	1.0	11
265	Secure authentication of classical messages with decoherence-free states. Optics Communications, 2009, 282, 3382-3385.	1.0	24
266	Two improved range-efficient algorithms for <mml:math altimg="si1.gif" display="inline" 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/co	0.5	7
267	The security of practical quantum key distribution. Reviews of Modern Physics, 2009, 81, 1301-1350.	16.4	2,489
268	SSL/TLS with Quantum Cryptography. , 2009, , .		4
269	The complexity of online memory checking. Journal of the ACM, 2009, 56, 1-46.	1.8	56
270	Quantum Coin-Flipping-Based Authentication. , 2009, , .		2
271	HAIL. , 2009, , .		515
272	Continuous high speed coherent one-way quantum key distribution. Optics Express, 2009, 17, 13326.	1.7	61
273	de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. Physical Review Letters, 2009, 102, 110504.	2.9	277

#	Article	IF	Citations
274	High rate, long-distance quantum key distribution over 250â€‰km of ultra low loss fibres. New Journal of Physics, 2009, 11, 075003.	1.2	229
275	Optical networking for quantum key distribution and quantum communications. New Journal of Physics, 2009, 11, 105001.	1.2	185
276	Dense wavelength multiplexing of 1550â€‰nm QKD with strong classical channels in reconfigurable networking environments. New Journal of Physics, 2009, 11, 045012.	1.2	151
278	On noise insertion strategies for wireless network secrecy. , 2009, , .		12
279	On Cooperative Wireless Network Secrecy. , 2009, , .		32
280	BB84 Implementation and Computer Reality. , 2009, , .		5
281	A Fuzzy Extractor Based on Smooth Entropy. , 2009, , .		0
282	Adaptive Error Correction with Dynamic Initial Block Size in Quantum Cryptographic Key Distribution Protocols. , 2009, , .		2
283	Linear Probing with Constant Independence. SIAM Journal on Computing, 2009, 39, 1107-1120.	0.8	22
284	The M<scp>ARVIN</scp> message authentication code and the L<scp>ETTER</scp>S<scp>OUP</scp> authenticated encryption scheme. Security and Communication Networks, 2009, 2, 165-180.	1.0	22
285	Remote data checking for network coding-based distributed storage systems. , 2010, , .		125
286	Changes to Quantum Cryptography. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 872-879.	0.2	0
287	Quantum key distribution and 1â€‰Gbps data encryption over a single fibre. New Journal of Physics, 2010, 12, 063027.	1.2	202
288	Cryptographic hash functions. European Transactions on Telecommunications, 1994, 5, 431-448.	1.2	70
289	Generic Certificateless Encryption Secure Against Malicious-but-Passive KGC Attacks in the Standard Model. Journal of Computer Science and Technology, 2010, 25, 807-826.	0.9	9
291	Information-Theoretically Secret Key Generation for Fading Wireless Channels. IEEE Transactions on Information Forensics and Security, 2010, 5, 240-254.	4.5	325
292	Minutiae and modified Biocode fusion for fingerprint-based key generation. Journal of Network and Computer Applications, 2010, 33, 221-235.	5.8	22
293	REACT: An RFID-based privacy-preserving children tracking scheme for large amusement parks. Computer Networks, 2010, 54, 2744-2755.	3.2	24

#	Article	IF	Citations
294	Network Security. , 2010, , .		7
295	The power of primes: security of authentication based on a universal hash-function family. Journal of Mathematical Cryptology, 2010, 4, .	0.4	11
296	Practical issues in quantum-key-distribution postprocessing. Physical Review A, 2010, 81, .	1.0	139
297	Fast Message Authentication Code for Multiple Messages with Provable Security. , 2010, , .		2
298	Computer Network Security. Lecture Notes in Computer Science, 2010, , .	1.0	2
299	Security of trusted repeater quantum key distribution networks. Journal of Computer Security, 2010, 18, 61-87.	0.5	66
300	Zone Based Systems Design Framework for the Realisation of Efficient Block Cipher Based Message Authentication Code Algorithms. , 2010, , .		2
301	Information and Communications Security. Lecture Notes in Computer Science, 2010, , .	1.0	1
302	Efficient Authentication for Mobile and Pervasive Computing. Lecture Notes in Computer Science, 2010, , 186-202.	1.0	9
303	Securing Wireless Communications at the Physical Layer. , 2010, , .		174
304	Quantum Communication and Quantum Networking. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , .	0.2	6
305	Understanding Cryptography. , 2010, , .		478
306	Fast Software Encryption. Lecture Notes in Computer Science, 2010, , .	1.0	2
307	Cryptography for Network Security: Failures, Successes and Challenges. Lecture Notes in Computer Science, 2010, , 36-54.	1.0	6
308	Random modulation privacy for RFID channels. , 2010, , .		0
309	Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients. IEEE Transactions on Mobile Computing, 2011, 10, 205-215.	3.9	137
310	On Hardware-Oriented Message Authentication with Applications towards RFID. , 2011, , .		11
311	Efficient key-dependent message authentication in reconfigurable hardware. , 2011, , .		16

#	Article	IF	Citations
312	F-HB: An Efficient Forward Private Protocol. , 2011, , .		8
313	A Private and Scalable Authentication for RFID Systems Using Reasonable Storage. , 2011, , .		0
314	Linear Probing with 5-wise Independence. SIAM Review, 2011, 53, 547-558.	4.2	12
315	Secure quantum private information retrieval using phase-encoded queries. Physical Review A, 2011, 84, .	1.0	100
316	Investigations for the simulations of a quantum key distribution in WiFi. , 2011, , .		0
317	Scalable rational secret sharing. , 2011, , .		10
318	A New Spin on Quantum Cryptography: Avoiding Trapdoors and Embracing Public Keys. Lecture Notes in Computer Science, 2011, , 255-274.	1.0	5
321	Comparison of Authenticated-Encryption schemes in Wireless Sensor Networks. , 2011, , .		17
322	Post-Quantum Cryptography. Lecture Notes in Computer Science, 2011, , .	1.0	4
323	Lossy Trapdoor Functions and Their Applications. SIAM Journal on Computing, 2011, 40, 1803-1844.	0.8	107
324	On the Power of the Randomized Iterate. SIAM Journal on Computing, 2011, 40, 1486-1528.	0.8	14
325	F-HB+: A Scalable Authentication Protocol for Low-Cost RFID Systems. , 0, , .		2
326	A Universal Affine Code for Symmetric Channels. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 2097-2104.	0.2	0
327	On Optimal Secure Message Transmission by Public Discussion. IEEE Transactions on Information Theory, 2011, 57, 572-585.	1.5	8
328	Fully Homomorphic Encryption over the Integers with Shorter Public Keys. Lecture Notes in Computer Science, 2011, , 487-504.	1.0	242
329	A trade-off between collision probability and key size in universal hashing using polynomials. Designs, Codes, and Cryptography, 2011, 58, 271-278.	1.0	9
330	Certifying algorithms. Computer Science Review, 2011, 5, 119-161.	10.2	119
331	Universally composable and customizable post-processing for practical quantum key distribution. Computers and Security, 2011, 30, 172-177.	4.0	30

#	Article	IF	Citations
332	FUZZY UNIVERSAL HASHING AND APPROXIMATE AUTHENTICATION. Discrete Mathematics, Algorithms and Applications, 2011, 03, 587-607.	0.4	5
333	Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New Journal of Physics, 2011, 13, 123001.	1.2	243
334	Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey. Journal of Computer Security, 2011, 19, 139-201.	0.5	50
335	Private randomness expansion with untrusted devices. Journal of Physics A: Mathematical and Theoretical, 2011, 44, 095305.	0.7	243
336	Improving Classical Authentication over a Quantum Channel. Entropy, 2012, 14, 2531-2549.	1.1	6
337	Air to ground quantum key distribution. Proceedings of SPIE, 2012, , .	0.8	5
338	Field test of classical symmetric encryption with continuous variables quantum key distribution. Optics Express, 2012, 20, 14030.	1.7	97
339	On hardware-oriented message authentication. IET Information Security, 2012, 6, 329-336.	1.1	1
340	Deterministic parallel random-number generation for dynamic-multithreading platforms. , 2012, , .		26
341	The Power of Simple Tabulation Hashing. Journal of the ACM, 2012, 59, 1-50.	1.8	39
342	Deterministic parallel random-number generation for dynamic-multithreading platforms. ACM SIGPLAN Notices, 2012, 47, 193-204.	0.2	29
343	Ultrafast quantum random number generation based on quantum phase fluctuations. Optics Express, 2012, 20, 12366.	1.7	158
344	QUANTUM KEY EVOLUTION AND ITS APPLICATIONS. International Journal of Quantum Information, 2012, 10, 1250044.	0.6	3
346	Tabulation-Based 5-Independent Hashing with Applications to Linear Probing and Second Moment Estimation. SIAM Journal on Computing, 2012, 41, 293-331.	0.8	46
347	Robust Fuzzy Extractors and Authenticated Key Agreement From Close Secrets. IEEE Transactions on Information Theory, 2012, 58, 6207-6222.	1.5	63
348	Capacity of Byzantine consensus in capacity limited point-to-point networks. , 2012, , .		0
349	Resistance against Iterated Attacks by Decorrelation Revisited. Lecture Notes in Computer Science, 2012, , 741-757.	1.0	2
350	Pseudorandomness. Foundations and Trends in Theoretical Computer Science, 2012, 7, 1-336.	2.0	160

#	Article	IF	Citations
351	Traffic Anomaly Detection and Containment Using Filter-Ary-Sketch. Procedia Engineering, 2012, 29, 4297-4306.	1.2	6
352	Revisiting the Security of the ALRED Design and Two of Its Variants: Marvin and LetterSoup. IEEE Transactions on Information Theory, 2012, 58, 6223-6238.	1.5	3
353	Information and Communications Security. Lecture Notes in Computer Science, 2012, , .	1.0	1
354	Entropy uncertainty relations and stability of phase-temporal quantum cryptography with finite-length transmitted strings. Journal of Experimental and Theoretical Physics, 2012, 115, 969-985.	0.2	3
355	Introduction to Hardware Security and Trust. , 2012, , .		166
357	Construction of Orthogonal Arrays of Index Unity Using Logarithm Tables for Galois Fields. , 2012, , .		2
358	Reverse Authentication in Financial Transactions and Identity Management. Mobile Networks and Applications, 2013, 18, 712-727.	2.2	3
359	Dual Universality of Hash Functions and Its Applications to Quantum Cryptography. IEEE Transactions on Information Theory, 2013, 59, 4700-4717.	1.5	44
360	Efficient Public Key Cryptosystem Resilient to Key Leakage Chosen Ciphertext Attacks. Lecture Notes in Computer Science, 2013, , 84-100.	1.0	34
361	Topics in Cryptology â€“ CT-RSA 2013. Lecture Notes in Computer Science, 2013, , .	1.0	0
362	Rational secret sharing as extensive games. Science China Information Sciences, 2013, 56, 1-13.	2.7	11
363	Non-uniformity issues and workarounds in bounded-size sampling. VLDB Journal, 2013, 22, 753-772.	2.7	3
364	Device-Independent Quantum Key Distribution with Local Bell Test. Physical Review X, 2013, 3, .	2.8	52
365	A new multi-linear universal hash family. Designs, Codes, and Cryptography, 2013, 69, 351-367.	1.0	9
366	Experimental Bit Commitment Based on Quantum Communication and Special Relativity. Physical Review Letters, 2013, 111, 180504.	2.9	73
367	On the Existence of Quantum Signature for Quantum Messages. International Journal of Theoretical Physics, 2013, 52, 4335-4341.	0.5	10
368	Efficient leakage-resilient public key encryption from DDH assumption. Cluster Computing, 2013, 16, 797-806.	3.5	27
369	Simple Tabulation, Fast Expanders, Double Tabulation, and High Independence. , 2013, , .		17

#	Article	IF	Citations
370	Unconditionally-secure ideal robust secret sharing schemes for threshold and multilevel access structure. Journal of Mathematical Cryptology, 2013, 7, .	0.4	1
371	Format-Preserving Fuzzy Query Mechanism. , 2013, , .		1
372	MISRs for Fast Authentication of Long Messages. , 2013, , .		2
373	Polar coding for secret-key generation. , 2013, , .		17
374	Secure Storage and Fuzzy Query over Encrypted Databases. Lecture Notes in Computer Science, 2013, , 439-450.	1.0	4
375	Survey and comparison of message authentication solutions on wireless sensor networks. Ad Hoc Networks, 2013, 11, 1221-1236.	3.4	30
376	Towards self-repairing replication-based storage systems using untrusted clouds. , 2013, , .		21
377	Efficient Lattice-Based Signcryption in Standard Model. Mathematical Problems in Engineering, 2013, 2013, 1-18.	0.6	13
378	Weak leakage-resilient client-side deduplication of encrypted data in cloud storage. , 2013, , .		98
379	Bottom-k and priority sampling, set similarity and subset sums with minimal independence. , 2013, , .		19
380	Protocols for Message Authentication from a Weak Secret. Applied Mechanics and Materials, 0, 380-384, 2892-2896.	0.2	0
381	On Cheater Identifiable Secret Sharing Schemes Secure against Rushing Adversary. Lecture Notes in Computer Science, 2013, , 258-271.	1.0	11
382	Analysis of a rate-adaptive reconciliation protocol and the effect of leakage on the secret key rate. Physical Review A, 2013, 87, .	1.0	7
383	Fundamental data structures. , 2013, , 123-147.		0
384	SQL-Based Fuzzy Query Mechanism Over Encrypted Database. International Journal of Data Warehousing and Mining, 2014, 10, 71-87.	0.4	12
385	Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 2014, 560, 7-11.	0.5	1,318
386	Intercepting tokens in cryptographic protocols: The empire strikes back in the clone wars. , 2014, , .		0
387	Fast implementation of length-adaptive privacy amplification in quantum key distribution. Chinese Physics B, 2014, 23, 090310.	0.7	12

#	Article	IF	Citations
388	A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. New Journal of Physics, 2014, 16, 013047.	1.2	90
389	Security analysis of the decoy method with the Bennettâ€“Brassard 1984 protocol for finite key lengths. New Journal of Physics, 2014, 16, 063009.	1.2	47
390	Generating k-Independent Variables in Constant Time. , 2014, , .		3
391	Robust set reconciliation. , 2014, , .		13
392	Selected Areas in Cryptography -- SAC 2014. Lecture Notes in Computer Science, 2014, , .	1.0	7
393	Security analysis of GCM for communication. Security and Communication Networks, 2014, 7, 854-864.	1.0	5
394	Strongly Universal String Hashing is Fast. Computer Journal, 2014, 57, 1624-1638.	1.5	12
395	Cache-Oblivious Hashing. Algorithmica, 2014, 69, 864-883.	1.0	5
396	Modes of operations for encryption and authentication using stream ciphers supporting an initialisation vector. Cryptography and Communications, 2014, 6, 189-231.	0.9	15
397	Key-leakage evaluation of authentication in quantum key distribution with finite resources. Quantum Information Processing, 2014, 13, 935-955.	1.0	4
398	Explicit and Efficient Hash Families Suffice for Cuckoo Hashing with a Stash. Algorithmica, 2014, 70, 428-456.	1.0	17
399	Direct proof of security of Wegmanâ€“Carter authentication with partially known key. Quantum Information Processing, 2014, 13, 2155-2170.	1.0	13
400	Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. Physical Review A, 2014, 90, .	1.0	49
401	Non-asymptotic and asymptotic analyses on Markov chains in several problems. , 2014, , .		9
402	Using quantum key distribution for cryptographic purposes: A survey. Theoretical Computer Science, 2014, 560, 62-81.	0.5	116
403	Delayed error verification in quantum key distribution. Science Bulletin, 2014, 59, 2825-2828.	1.7	47
404	E-MACs: Toward More Secure and More Efficient Constructions of Secure Channels. IEEE Transactions on Computers, 2014, 63, 204-217.	2.4	2
405	Large Deviation Analysis for Quantum Security via Smoothing of RÃ©nyi Entropy of Order 2. IEEE Transactions on Information Theory, 2014, 60, 6702-6732.	1.5	20

#	Article	IF	Citations
406	Separation of Reliability and Secrecy in Rate-Limited Secret-Key Generation. IEEE Transactions on Information Theory, 2014, 60, 4941-4957.	1.5	31
407	Concise security bounds for practical decoy-state quantum key distribution. Physical Review A, 2014, 89, .	1.0	248
409	Secure Device Pairing: A Survey. IEEE Communications Surveys and Tutorials, 2014, 16, 17-40.	24.8	37
410	Key Recycling in Authentication. IEEE Transactions on Information Theory, 2014, 60, 4383-4396.	1.5	37
411	Asymmetric â€œ4+2â€•protocol for quantum key distribution with finite resources. Quantum Information Processing, 2014, 13, 5-20.	1.0	3
412	A practical protocol for three-party authenticated quantum key distribution. Quantum Information Processing, 2014, 13, 2355-2374.	1.0	16
413	Revisiting iterated attacks in the context of decorrelation theory. Cryptography and Communications, 2014, 6, 279-311.	0.9	1
414	Sample (x) = (a*x<=t) is a Distinguisher with Probability 1/8. , 2015, , .		0
415	Experimental quantum key distribution with source flaws. Physical Review A, 2015, 92, .	1.0	69
416	Unconditionally Secure Quantum Signatures. Entropy, 2015, 17, 5635-5659.	1.1	42
418	Knock Yourself Out: Secure Authentication with Short Re-Usable Passwords. , 2015, , .		1
419	Hashing for Statistics over K-Partitions. , 2015, , .		13
420	An authentication scheme with high throughput based on FPGA for a practical QKD system. Optik, 2015, 126, 4747-4750.	1.4	3
421	CRC-Based Message Authentication for 5G Mobile Technology. , 2015, , .		17
422	More efficient privacy amplification with less random seeds. , 2015, , .		3
423	Scalable mechanisms for rational secret sharing. Distributed Computing, 2015, 28, 171-187.	0.7	1
424	Efficient bit sifting scheme of post-processing in quantum key distribution. Quantum Information Processing, 2015, 14, 3785-3811.	1.0	5
425	Quantum digital signatures with quantum-key-distribution components. Physical Review A, 2015, 91, .	1.0	96

#	Article	IF	Citations
426	Introduction to Cryptography. Information Security and Cryptography, 2015, , .	0.2	46
427	Information and Communication Technology. Lecture Notes in Computer Science, 2015, , .	1.0	1
428	Construction and Impromptu Repair of an MST in a Distributed Network with o(m) Communication. , 2015, , .		22
429	Polar Coding for Secret-Key Generation. IEEE Transactions on Information Theory, 2015, 61, 6213-6237.	1.5	74
430	From Independence to Expansion and Back Again. , 2015, , .		10
431	On the Size of Source Space in a Secure MAC. IEEE Transactions on Information Forensics and Security, 2015, 10, 2007-2015.	4.5	3
432	Error-Control Coding for Physical-Layer Secrecy. Proceedings of the IEEE, 2015, 103, 1725-1746.	16.4	81
433	On Weak Keys and Forgery Attacks Against Polynomial-Based MAC Schemes. Journal of Cryptology, 2015, 28, 769-795.	2.1	10
434	A survey on secret key generation mechanisms on the physical layer in wireless networks. Security and Communication Networks, 2015, 8, 332-341.	1.0	45
435	New Proofs for NMAC and HMAC: Security without Collision Resistance. Journal of Cryptology, 2015, 28, 844-878.	2.1	41
438	Energy aware medium access control for CPS-based wireless networks. International Journal of Communication Networks and Distributed Systems, 2016, 16, 352.	0.3	3
439	Efficient chosen ciphertext secure identityâ€based encryption against key leakage attacks. Security and Communication Networks, 2016, 9, 1417-1434.	1.0	14
440	Post-processing procedure for industrial quantum key distribution systems. Journal of Physics: Conference Series, 2016, 741, 012081.	0.3	29
441	HISC/R: An Efficient Hypersparse-Matrix Storage Format for Scalable Graph Processing. , 2016, , .		0
442	The smooth entropy formalism for von Neumann algebras. Journal of Mathematical Physics, 2016, 57, .	0.5	22
443	Quantum random number generation. Npj Quantum Information, 2016, 2, .	2.8	233
444	Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing. Scientific Reports, 2016, 6, 28988.	1.6	22
445	Memory Encryption for General-Purpose Processors. IEEE Security and Privacy, 2016, 14, 54-62.	1.5	51

#	Article	IF	Citations
446	Authenticated multi-user quantum key distribution with single particles. International Journal of Quantum Information, 2016, 14, 1650002.	0.6	5
447	Quadtrees and Morton Indexing. , 2016, , 1637-1642.		1
448	Optimal Las Vegas reduction from one-way set reconciliation to error correction. Theoretical Computer Science, 2016, 621, 14-21.	0.5	0
449	GCM implementations of Camellia-128 and SMS4 by optimizing the polynomial multiplier. Microprocessors and Microsystems, 2016, 45, 129-140.	1.8	8
450	Performance of device-independent quantum key distribution. Physical Review A, 2016, 94, .	1.0	7
451	Kryptografie verstÃndlich. EXamen Press, 2016, , .	0.0	22
452	AG codes, WeierstraÃŸ points and universal hashing. , 2016, , 431-445.		0
453	PTE. , 2016, , .		44
454	On Methodology of E-wallet Construction for Partially Off-line Payment System. Communications in Computer and Information Science, 2016, , 753-765.	0.4	0
456	MAC Precomputation with Applications to Secure Memory. ACM Transactions on Privacy and Security, 2016, 19, 1-21.	2.2	0
457	Study on the security of the authentication scheme with key recycling in QKD. Quantum Information Processing, 2016, 15, 3815-3831.	1.0	6
458	Quantum Key Distribution. , 2016, , 1703-1707.		0
459	Role of Quantum Information Theory in Information Theory. Ieice Ess Fundamentals Review, 2016, 10, 4-13.	0.1	1
460	Join Sizes, Frequency Moments, and Applications. Data-centric Systems and Applications, 2016, , 87-102.	0.2	2
462	Public key cryptosystems secure against memory leakage attacks. IET Information Security, 2016, 10, 403-412.	1.1	0
463	General Constructions of Rational Secret Sharing with Expected Constant-Round Reconstruction: Table 1.. Computer Journal, 0, , .	1.5	1
464	Quantum cryptography: Theoretical protocols for quantum key distribution and tests of selected commercial QKD systems in commercial fiber networks. International Journal of Quantum Information, 2016, 14, 1630002.	0.6	2
465	Sequential aggregate authentication codes with information theoretic security. , 2016, , .		2

#	Article	IF	Citations
466	An Optimally Fair Coin Toss. Journal of Cryptology, 2016, 29, 491-513.	2.1	23
467	On message authentication with a correlated setup. Information Processing Letters, 2016, 116, 289-293.	0.4	0
468	More Efficient Privacy Amplification With Less Random Seeds via Dual Universal Hash Function. IEEE Transactions on Information Theory, 2016, 62, 2213-2232.	1.5	49
469	Continuous-variable quantum identity authentication based on quantum teleportation. Quantum Information Processing, 2016, 15, 2605-2620.	1.0	31
470	Experimental demonstration of kilometer-range quantum digital signatures. Physical Review A, 2016, 93, .	1.0	65
471	Attacks on quantum key distribution protocols that employ non-ITS authentication. Quantum Information Processing, 2016, 15, 327-362.	1.0	16
472	Security Analysis of <inline-formula> <tex-math notation="LaTeX">$varepsilon $ </tex-math> </inline-formula>-Almost Dual Universal‹sub›2‹/sub›Hash Functions: Smoothing of Min Entropy Versus Smoothing of RÃ©nyi Entropy of Order 2. IEEE Transactions on Information Theory, 2016, 62, 3451-3476.	1.5	28
473	Attacks on practical quantum key distribution systems (and how to prevent them). Contemporary Physics, 2016, 57, 366-387.	0.8	63
475	On modes of operations of a block cipher for authentication and authenticated encryption. Cryptography and Communications, 2016, 8, 455-511.	0.9	8
476	An FPGA-Based 4 Mbps Secret Key Distillation Engine for Quantum Key Distribution Systems. Journal of Signal Processing Systems, 2017, 86, 1-15.	1.4	20
477	Regular and almost universal hashing: an efficient implementation. Software - Practice and Experience, 2017, 47, 1299-1323.	2.5	3
478	Secure pseudonymisation for privacy-preserving probabilistic record linkage. Journal of Information Security and Applications, 2017, 34, 271-279.	1.8	18
479	d-k-min-wise independent family of hash functions. Journal of Computer and System Sciences, 2017, 84, 171-184.	0.9	2
480	Quantum random number generators. Reviews of Modern Physics, 2017, 89, .	16.4	412
481	Accelerating Integrity Verification on Secure Processors by Promissory Hash. , 2017, , .		0
482	Quantum key distribution network for multiple applications. Quantum Science and Technology, 2017, 2, 034003.	2.6	15
483	Information-theoretic physical layer security for satellite channels. , 2017, , .		9
484	Wiretapped Oblivious Transfer. IEEE Transactions on Information Theory, 2017, 63, 2560-2595.	1.5	3

#	Article	IF	Citations
485	An analysis of LPN based HB protocols. , 2017, , .		2
486	A novel anomaly detection system using feature-based MSPCA with sketch. , 2017, , .		5
487	A New Look at Counters: Donâ€™t Run Like Marathon in a Hundred Meter Race. IEEE Transactions on Computers, 2017, 66, 1851-1864.	2.4	2
488	Quantum Authentication with Key Recycling. Lecture Notes in Computer Science, 2017, , 339-368.	1.0	16
489	Hashing Techniques. ACM Computing Surveys, 2018, 50, 1-36.	16.1	87
490	Comment on â€œA practical protocol for three-party authenticated quantum key distributionâ€• Quantum Information Processing, 2017, 16, 1.	1.0	1
491	Detection of network anomalies using Improved-MSPCA with sketches. Computers and Security, 2017, 65, 314-328.	4.0	16
492	Symmetric Blind Information Reconciliation for Quantum Key Distribution. Physical Review Applied, 2017, 8, .	1.5	44
494	The effect of bias on the guesswork of hash functions. , 2017, , .		6
495	Instantiability of RSA-OAEP Under Chosen-Plaintext Attack. Journal of Cryptology, 2017, 30, 889-919.	2.1	9
496	Share a pie?. , 2017, , .		0
497	Secure wireless communication under spatial and local Gaussian noise assumptions. , 2017, , .		7
498	Experimental study of a quantum random-number generator based on two independent lasers. Physical Review A, 2017, 96, .	1.0	12
499	Analyzing Multi-key Security Degradation. Lecture Notes in Computer Science, 2017, , 575-605.	1.0	14
500	True randomness from an incoherent source. Review of Scientific Instruments, 2017, 88, 113101.	0.6	19
501	Remote data integrity checking with server-side repair1. Journal of Computer Security, 2017, 25, 537-584.	0.5	9
502	Hashing, Load Balancing and Multiple Choice. Foundations and Trends in Theoretical Computer Science, 2017, 12, 275-379.	2.0	18
503	Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length. Lecture Notes in Computer Science, 2017, , 446-470.	1.0	23

#	Article	IF	Citations
504	Zero-Knowledge Contingent Payments Revisited. , 2017, , .		79
505	Secure Processors Part II: Intel SGX Security Analysis and MIT Sanctum Architecture. Foundations and Trends in Electronic Design Automation, 2017, 11, 249-361.	1.0	14
506	Experimental performance analysis of lightweight block ciphers and message authentication codes for wireless sensor networks. International Journal of Distributed Sensor Networks, 2017, 13, 155014771774416.	1.3	7
507	Multi-message Authentication over Noisy Channel with Polar Codes. , 2017, , .		7
508	Coding for the Large-Alphabet Adversarial Channel. IEEE Transactions on Information Theory, 2017, 63, 6347-6363.	1.5	3
509	Finite-block-length analysis in classical and quantum information theory. Proceedings of the Japan Academy Series B: Physical and Biological Sciences, 2017, 93, 99-124.	1.6	6
510	Improved Asymmetric Cipher Based on Matrix Power Function with Provable Security. Symmetry, 2017, 9, 9.	1.1	8
511	Analysis of the single-permutation encrypted Daviesâ€“Meyer construction. Designs, Codes, and Cryptography, 2018, 86, 2703-2723.	1.0	12
512	Practical cryptographic strategies in the post-quantum era. AIP Conference Proceedings, 2018, , .	0.3	6
513	Analysis of Remaining Uncertainties and Exponents Under Various Conditional RÃ©nyi Entropies. IEEE Transactions on Information Theory, 2018, 64, 3734-3755.	1.5	9
514	On rate-1 and beyond-the-birthday bound secure online ciphers using tweakable block ciphers. Cryptography and Communications, 2018, 10, 731-753.	0.9	4
515	Security of quantum key distribution with iterative sifting. Quantum Science and Technology, 2018, 3, 014002.	2.6	6
516	Security Formalizations and Their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography. IEEE Transactions on Information Theory, 2018, 64, 654-685.	1.5	20
517	Public-Key Encryption with Tight Simulation-Based Selective-Opening Security. Computer Journal, 2018, 61, 288-318.	1.5	2
518	Super-strong RKA secure MAC, PKE and SE from tag-based hash proof system. Designs, Codes, and Cryptography, 2018, 86, 1411-1449.	1.0	2
519	Secure uniform random-number extraction via incoherent strategies. Physical Review A, 2018, 97, .	1.0	17
520	High-Speed Implementation of Length-Compatible Privacy Amplification in Continuous-Variable Quantum Key Distribution. IEEE Photonics Journal, 2018, 10, 1-9.	1.0	23
521	Message Authentication Based on Cryptographically Secure CRC without Polynomial Irreducibility Test. Cryptography and Communications, 2018, 10, 383-399.	0.9	16

#	Article	IF	Citations
522	Randomized OBDD-based graph algorithms. Theoretical Computer Science, 2018, 751, 24-45.	0.5	0
523	Tightly CCA-secure identity-based encryption with ciphertext pseudorandomness. Designs, Codes, and Cryptography, 2018, 86, 517-554.	1.0	3
524	Connecting tweakable and multi-key blockcipher security. Designs, Codes, and Cryptography, 2018, 86, 623-640.	1.0	7
525	Efficient Detection for Malicious and Random Errors in Additive Encrypted Computation. IEEE Transactions on Computers, 2018, 67, 16-31.	2.4	8
526	Sample(x)=(a*x<=t) Is a Distinguisher with Probability 1/8. SIAM Journal on Computing, 2018, 47, 2510-2526.	0.8	0
527	A (k, n)-Threshold Progressive Visual Secret Sharing without Expansion. Cryptography, 2018, 2, 28.	1.4	2
528	Inverted Leftover Hash Lemma. , 2018, , .		2
529	Lightweight Message Authentication for Constrained Devices. , 2018, , .		2
530	Survey of design and security evaluation of authenticated encryption algorithms in the CAESAR competition. Frontiers of Information Technology and Electronic Engineering, 2018, 19, 1475-1499.	1.5	10
531	On an Almost-Universal Hash Function Family with Applications to Authentication and Secrecy Codes. International Journal of Foundations of Computer Science, 2018, 29, 357-375.	0.8	9
532	Perfectly Secure Message Transmission Against Rational Timid Adversaries. Lecture Notes in Computer Science, 2018, , 127-144.	1.0	2
533	Enumerating Trillion Subgraphs On Distributed Systems. ACM Transactions on Knowledge Discovery From Data, 2018, 12, 1-30.	2.5	10
534	Symmetric Blind Information Reconciliation and Hash-function-based Verification for Quantum Key Distribution. Lobachevskii Journal of Mathematics, 2018, 39, 992-996.	0.1	11
535	Memory-Saving Implementation of High-Speed Privacy Amplification Algorithm for Continuous-Variable Quantum Key Distribution. IEEE Photonics Journal, 2018, 10, 1-12.	1.0	7
536	Communication Efficient Checking of Big Data Operations. , 2018, , .		1
537	Bernstein Bound on WCS is Tight. Lecture Notes in Computer Science, 2018, , 213-238.	1.0	5
538	Generic Attacks Against Beyond-Birthday-Bound MACs. Lecture Notes in Computer Science, 2018, , 306-336.	1.0	12
539	VAULT. , 2018, , .		70

#	Article	IF	Citations
540	Multi-photon Quantum Secure Communication. Signals and Communication Technology, 2019, , .	0.4	10
541	Hardness-Preserving Reductions via Cuckoo Hashing. Journal of Cryptology, 2019, 32, 361-392.	2.1	3
542	Non-empty Bins with Simple Tabulation Hashing. , 2019, , 2498-2512.		0
543	Implementation Security Certification of Decoyâ€BB84 Quantum Key Distribution Systems. Advanced Quantum Technologies, 2019, 2, 1900005.	1.8	6
544	Structure-preserving public-key encryption with leakage-resilient CCA security. Theoretical Computer Science, 2019, 795, 57-80.	0.5	0
545	Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic. Entropy, 2019, 21, 887.	1.1	35
546	Adversarial and Uncertain Reasoning for Adaptive Cyber Defense. Lecture Notes in Computer Science, 2019, , .	1.0	4
547	Architectures for Security: A comparative analysis of hardware security features in Intel SGX and ARM TrustZone. , 2019, , .		15
548	High-Speed and Adaptive FPGA-Based Privacy Amplification in Quantum Key Distribution. IEEE Access, 2019, 7, 21482-21490.	2.6	19
549	Attribute-Based Signcryption From Lattices in the Standard Model. IEEE Access, 2019, 7, 56039-56050.	2.6	9
550	Linking Stamâ€™s Bounds with Generalized Truncation. Lecture Notes in Computer Science, 2019, , 313-329.	1.0	7
551	Quantum identity authentication in the orthogonal-state-encoding QKD system. Quantum Information Processing, 2019, 18, 1.	1.0	17
552	Foiling covert channels and malicious classical post-processing units in quantum key distribution. Npj Quantum Information, 2019, 5, .	2.8	20
553	On Optimal Information-Theoretically Secure Key Management*. , 2019, , .		0
554	Composable, Unconditionally Secure Message Authentication without any Secret Key. , 2019, , .		1
555	Private Votes on Untrusted Platforms: Models, Attacks and Provable Scheme. , 2019, , .		5
556	Proving Erasure. , 2019, , .		6
557	Generation of k-wise independent random variables with small randomness. Monte Carlo Methods and Applications, 2019, 25, 259-270.	0.3	0

#	Article	IF	Citations
558	Physical Layer Security for RF Satellite Channels in the Finite-Length Regime. IEEE Transactions on Information Forensics and Security, 2019, 14, 981-993.	4.5	20
559	Evaluating Bernsteinâ€“Rabinâ€“Winograd polynomials. Designs, Codes, and Cryptography, 2019, 87, 527-546.	1.0	1
560	Physical Layer based Message Authentication with Secure Channel Codes. IEEE Transactions on Dependable and Secure Computing, 2020, 17, 1079-1093.	3.7	38
561	A Novel Approach to Quality-of-Service Provisioning in Trusted Relay Quantum Key Distribution Networks. IEEE/ACM Transactions on Networking, 2020, 28, 168-181.	2.6	32
562	Entropy Accumulation. Communications in Mathematical Physics, 2020, 379, 867-913.	1.0	45
563	Effective cache replacement policy for packet processing cache. International Journal of Communication Systems, 2020, 33, e4526.	1.6	2
564	Delegation-based conversion from CPA to CCA-secure predicate encryption. International Journal of Applied Cryptography, 2020, 4, 16.	0.4	3
565	Locally private frequency estimation of physical symptoms for infectious disease analysis in Internet of Medical Things. Computer Communications, 2020, 162, 139-151.	3.1	19
566	Information-Theoretically Secure Data Origin Authentication with Quantum and Classical Resources. Cryptography, 2020, 4, 31.	1.4	4
567	Tight security bounds for decoy-state quantum key distribution. Scientific Reports, 2020, 10, 14312.	1.6	31
568	Authenticated QKD Protocol Based on Single-Photon Interference. IEEE Access, 2020, 8, 135357-135370.	2.6	1
569	Secure Network Code for Adaptive and Active Attacks With No-Randomness in Intermediate Nodes. IEEE Transactions on Information Theory, 2020, 66, 1428-1448.	1.5	16
570	Cyber-Security in Critical Infrastructures. Advanced Sciences and Technologies for Security Applications, 2020, , .	0.4	14
571	Towards Usable Cloud Storage Auditing. IEEE Transactions on Parallel and Distributed Systems, 2020, 31, 2605-2617.	4.0	16
572	Multiple Private Key Generation for Continuous Memoryless Sources With a Helper. IEEE Transactions on Information Forensics and Security, 2020, 15, 2629-2640.	4.5	4
574	Randomness Expansion Secured by Quantum Contextuality. Physical Review Applied, 2020, 13, .	1.5	10
575	Two-Way Physical Layer Security Protocol for Gaussian Channels. IEEE Transactions on Communications, 2020, 68, 3068-3078.	4.9	10
576	Randomness Extraction via a Quantum Generalization of the Conditional Collision Entropy. IEEE Transactions on Information Theory, 2020, 66, 1171-1177.	1.5	4

#	Article	IF	Citations
577	Quantum cryptography networks in support of path verification in service function chains. Journal of Optical Communications and Networking, 2020, 12, B9.	3.3	11
578	Physical Layer Security Protocol for Poisson Channels for Passive Man-in-the-Middle Attack. IEEE Transactions on Information Forensics and Security, 2020, 15, 2295-2305.	4.5	13
579	Theoretical framework for physical unclonable functions, including quantum readout. Physical Review A, 2020, 101, .	1.0	13
580	Finite-Length Analyses for Source and Channel Coding on Markov Chains. Entropy, 2020, 22, 460.	1.1	9
581	Simple analysis of security of the BB84 quantum key distribution protocol. Quantum Information Processing, 2020, 19, 1.	1.0	9
582	Lightweight Authentication for Quantum Key Distribution. IEEE Transactions on Information Theory, 2020, 66, 6354-6368.	1.5	16
583	Single-Trace Side-Channel Analysis on Polynomial-Based MAC Schemes. Lecture Notes in Computer Science, 2021, , 43-67.	1.0	0
584	Security of the decoy state method for quantum key distribution. Physics-Uspekhi, 2021, 64, 88-102.	0.8	17
585	Quantum Key Distribution. , 2021, , 703-784.		0
586	Improved Channel Reciprocity for Secure Communication in Next Generation Wireless Systems. Computers, Materials and Continua, 2021, 67, 2619-2630.	1.5	6
587	Artificial Noise-Aided MIMO Physical Layer Authentication With Imperfect CSI. IEEE Transactions on Information Forensics and Security, 2021, 16, 2173-2185.	4.5	22
588	Revisiting Construction of Online Cipher in Hash-ECB-Hash Structure. Lecture Notes in Computer Science, 2021, , 491-503.	1.0	0
589	Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. Nature Communications, 2021, 12, 605.	5.8	33
590	Toward Usable Cloud Storage Auditing, Revisited. IEEE Systems Journal, 2022, 16, 693-700.	2.9	14
591	Variants of Wegman-Carter message authentication code supporting variable tag lengths. Designs, Codes, and Cryptography, 2021, 89, 709-736.	1.0	1
592	An Introduction to Practical Quantum Key Distribution. IEEE Aerospace and Electronic Systems Magazine, 2021, 36, 30-55.	2.3	16
593	Quantum Key Distribution Networks: Challenges and Future Research Issues in Security. Applied Sciences (Switzerland), 2021, 11, 3767.	1.3	20
594	Breaking LWC candidates: sESTATE and Elephant in quantum setting. Designs, Codes, and Cryptography, 2021, 89, 1405-1432.	1.0	1

#	Article	IF	Citations
595	Authentication of Diffie-Hellman Protocol for Mobile Units Executing a Secure Device Pairing Procedure in Advance. , 2021, , .		1
596	Quantum key distribution with PRF(Hash, Nonce) achieves everlasting security. Quantum Information Processing, 2021, 20, 1.	1.0	8
597	Information-theoretic Key Encapsulation and its Application to Secure Communication. , 2021, , .		2
598	Quantum technologies in the telecommunications industry. EPJ Quantum Technology, 2021, 8, .	2.9	28
599	Secure Modulo Sum via Multiple Access Channel. , 2021, , .		1
600	Low-congestion shortcut and graph parameters. Distributed Computing, 2021, 34, 349-365.	0.7	0
601	Improving Tug-of-War sketch using Control-Variates method. , 2021, , 66-76.		0
602	Quantum Key Distribution Protocols. Lecture Notes in Physics, 2021, , 91-116.	0.3	0
603	Multibit quantum digital signature with continuous variables using basis encoding over insecure channels. Physical Review A, 2021, 103, .	1.0	16
605	Results on Almost Resilient Functions. Lecture Notes in Computer Science, 2006, , 421-432.	1.0	2
606	Provably Secure MACs from Differentially-Uniform Permutations and AES-Based Implementations. Lecture Notes in Computer Science, 2006, , 226-241.	1.0	23
607	A New Mode of Encryption Providing a Tweakable Strong Pseudo-random Permutation. Lecture Notes in Computer Science, 2006, , 293-309.	1.0	38
610	A complexity theory of efficient parallel algorithms. Lecture Notes in Computer Science, 1988, , 333-346.	1.0	13
611	Redistribution of Mechanical Secret Shares. Lecture Notes in Computer Science, 2003, , 238-252.	1.0	2
612	On the Universal Hash Functions in Luby-Rackoff Cipher. Lecture Notes in Computer Science, 2003, , 226-237.	1.0	4
613	Provably Secure Public-Key Encryption for Length-Preserving Chaumian Mixes. Lecture Notes in Computer Science, 2003, , 244-262.	1.0	22
614	Arbitrated Unconditionally Secure Authentication Can Be Unconditionally Protected against Arbiterâ€™s Attacks. , 1990, , 177-188.		21
615	Structural Properties of One-Way Hash Functions. , 1990, , 285-302.		10

#	Article	IF	Citations
616	Collision Free Hash Functions and Public Key Signature Schemes. Lecture Notes in Computer Science, 1987, , 203-216.	1.0	147
617	New Block Cipher DONUT Using Pairwise Perfect Decorrelation. Lecture Notes in Computer Science, 2000, , 262-270.	1.0	2
620	Almost Independent and Weakly Biased Arrays: Efficient Constructions and Cryptologic Applications. Lecture Notes in Computer Science, 2000, , 533-543.	1.0	16
621	MDx-MAC and Building Fast MACs from Hash Functions. Lecture Notes in Computer Science, 1995, , 1-14.	1.0	69
622	Does Encryption with Redundancy Provide Authenticity?. Lecture Notes in Computer Science, 2001, , 512-528.	1.0	19
623	Linear Authentication Codes: Bounds and Constructions. Lecture Notes in Computer Science, 2001, , 127-135.	1.0	3
624	Performance Tuning an Algorithm for Compressing Relational Tables. Lecture Notes in Computer Science, 2002, , 398-407.	1.0	2
625	A Composition Theorem for Universal One-Way Hash Functions. Lecture Notes in Computer Science, 2000, , 445-452.	1.0	63
627	A Block-Cipher Mode of Operation for Parallelizable Message Authentication. Lecture Notes in Computer Science, 2002, , 384-397.	1.0	150
628	Indistinguishability of Random Systems. Lecture Notes in Computer Science, 2002, , 110-132.	1.0	129
629	Cryptographically Strong Undeniable Signatures, Unconditionally Secure for the Signer. Lecture Notes in Computer Science, 1992, , 470-484.	1.0	104
630	Universal hashing and authentication codes. , 1991, , 74-85.		86
631	Experimental Quantum Cryptography. Lecture Notes in Computer Science, 1991, , 253-265.	1.0	241
632	The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability. , 1989, , 690-690.		55
633	Practical Approaches to Attaining Security against Adaptively Chosen Ciphertext Attacks. , 1992, , 292-304.		26
634	Protocols for Secret Key Agreement by Public Discussion Based on Common Information. , 1992, , 461-470.		44
635	On the Relation Between A-Codes and Codes Correcting Independent Errors. , 1993, , 1-11.		44
636	On Families of Hash Functions via Geometric Codes and Concatenation. , 1993, , 331-342.		76

#	Article	IF	Citations
637	Codes for Interactive Authentication. , 1993, , 355-367.		26
638	Another Method for Attaining Security Against Adaptively Chosen Ciphertext Attacks. , 1993, , 420-434.		21
639	UMAC: Fast and Secure Message Authentication. Lecture Notes in Computer Science, 1999, , 216-233.	1.0	198
641	Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions. Lecture Notes in Computer Science, 1999, , 252-269.	1.0	49
642	Stateless Evaluation of Pseudorandom Functions: Security Beyond the Birthday Barrier. Lecture Notes in Computer Science, 1999, , 270-287.	1.0	28
643	Cryptanalysis of the Gemmell and Naor Multiround Authentication Protocol. , 1994, , 121-128.		6
644	New Bound on Authentication Code with Arbitration. , 1994, , 140-149.		20
645	Tracing Traitors. Lecture Notes in Computer Science, 1994, , 257-270.	1.0	327
646	Feistel Ciphers with L 2-Decorrelation. Lecture Notes in Computer Science, 1999, , 1-14.	1.0	13
647	Resistance Against General Iterated Attacks. Lecture Notes in Computer Science, 1999, , 255-271.	1.0	15
648	Software Performance of Universal Hash Functions. Lecture Notes in Computer Science, 1999, , 24-41.	1.0	36
649	Secure Multiround Authentication Protocols. Lecture Notes in Computer Science, 1995, , 158-167.	1.0	3
650	Bounds and Constructions for Multireceiver Authentication Codes. Lecture Notes in Computer Science, 1998, , 242-256.	1.0	5
652	Program checking. Lecture Notes in Computer Science, 1991, , 1-9.	1.0	5
653	Unconditional Byzantine agreement for any number of faulty processors. Lecture Notes in Computer Science, 1992, , 337-350.	1.0	33
655	Universal Hashing and Multiple Authentication. Lecture Notes in Computer Science, 1996, , 16-30.	1.0	20
656	On Fast and Provably Secure Message Authentication Based on Universal Hashing. Lecture Notes in Computer Science, 1996, , 313-328.	1.0	112
657	Quantum Key Distribution and String Oblivious Transfer in Noisy Channels. Lecture Notes in Computer Science, 1996, , 343-357.	1.0	105

#	Article	IF	Citations
658	Bucket Hashing with a Small Key Size. Lecture Notes in Computer Science, 1997, , 149-162.	1.0	16
659	Information-Theoretically Secure Secret-Key Agreement by NOT Authenticated Public Discussion. Lecture Notes in Computer Science, 1997, , 209-225.	1.0	59
660	Oblivious Transfers and Privacy Amplification. Lecture Notes in Computer Science, 1997, , 334-347.	1.0	18
661	Almost k-wise Independent Sample Spaces and Their Cryptologic Applications. Lecture Notes in Computer Science, 1997, , 409-421.	1.0	10
662	The Strong Secret Key Rate of Discrete Random Triples. , 1994, , 271-285.		98
663	On the Security of Compressed Encodings. , 1984, , 209-230.		19
664	Hash-Based Techniques for High-Speed Packet Processing. Computer Communications and Networks, 2010, , 181-218.	0.8	53
665	Towards Tight Security of Cascaded LRW2. Lecture Notes in Computer Science, 2018, , 192-222.	1.0	9
666	Beyond Birthday Bound Secure MAC in Faulty Nonce Model. Lecture Notes in Computer Science, 2019, , 437-466.	1.0	16
667	Lightweight MACs from Universal HashÂFunctions. Lecture Notes in Computer Science, 2020, , 195-215.	1.0	3
668	Incremental Cryptography Revisited: PRFs, Nonces and Modular Design. Lecture Notes in Computer Science, 2020, , 576-598.	1.0	4
669	Authentication Codes and Algebraic Curves. , 2001, , 239-244.		1
670	Practical Dual-Receiver Encryption. Lecture Notes in Computer Science, 2014, , 85-105.	1.0	10
671	Efficient Leakage-Resilient Identity-Based Encryption with CCA Security. Lecture Notes in Computer Science, 2014, , 149-167.	1.0	14
672	Universal Hash-Function Families: From Hashing to Authentication. Lecture Notes in Computer Science, 2014, , 459-474.	1.0	1
673	Approximately Minwise Independence with Twisted Tabulation. Lecture Notes in Computer Science, 2014, , 134-145.	1.0	6
674	Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. Lecture Notes in Computer Science, 2014, , 306-323.	1.0	113
675	Faster Binary-Field Multiplication and Faster Binary-Field MACs. Lecture Notes in Computer Science, 2014, , 92-111.	1.0	6

#	Article	IF	Citations
676	Weak-Key and Related-Key Analysis of Hash-Counter-Hash Tweakable Enciphering Schemes. Lecture Notes in Computer Science, 2015, , 3-19.	1.0	3
677	Efficient Threshold Secret Sharing Schemes Secure Against Rushing Cheaters. Lecture Notes in Computer Science, 2016, , 3-23.	1.0	12
678	The Many Entropies in One-Way Functions. Information Security and Cryptography, 2017, , 159-217.	0.2	5
679	Message Franking via Committing Authenticated Encryption. Lecture Notes in Computer Science, 2017, , 66-97.	1.0	37
680	New Security Notions and Feasibility Results for Authentication of Quantum Data. Lecture Notes in Computer Science, 2017, , 342-371.	1.0	23
681	Collision Resistant Hashing for Paranoids: Dealing with Multiple Collisions. Lecture Notes in Computer Science, 2018, , 162-194.	1.0	25
682	Optimal Forgeries Against Polynomial-Based MACs and GCM. Lecture Notes in Computer Science, 2018, , 445-467.	1.0	8
683	Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds. Lecture Notes in Computer Science, 2018, , 468-499.	1.0	27
684	A Hybrid Protocol for Quantum Authentication of Classical Messages. Lecture Notes in Computer Science, 2004, , 1077-1082.	1.0	3
685	A Concrete Security Analysis for 3GPP-MAC. Lecture Notes in Computer Science, 2003, , 154-169.	1.0	8
686	A Message Authentication Code Based on Unimodular Matrix Groups. Lecture Notes in Computer Science, 2003, , 500-512.	1.0	4
687	True Random Number Generators Secure in a Changing Environment. Lecture Notes in Computer Science, 2003, , 166-180.	1.0	68
688	Broadcast Authentication in Group Communication. Lecture Notes in Computer Science, 1999, , 399-412.	1.0	5
689	A Fast and Key-Efficient Reduction of Chosen-Ciphertext to Known-Plaintext Security. Lecture Notes in Computer Science, 2007, , 498-516.	1.0	16
690	Generic Certificateless Key Encapsulation Mechanism. , 2007, , 215-229.		15
691	On Estimating Frequency Moments of Data Streams. Lecture Notes in Computer Science, 2007, , 479-493.	1.0	19
692	Message Authentication on 64-Bit Architectures. Lecture Notes in Computer Science, 2006, , 327-341.	1.0	26
693	Improved Security Analysis of XEX and LRW Modes. Lecture Notes in Computer Science, 2006, , 96-113.	1.0	27

#	Article	IF	Citations
694	Improving the Security of MACs Via Randomized Message Preprocessing. Lecture Notes in Computer Science, 2007, , 414-433.	1.0	8
695	New Bounds for PMAC, TMAC, and XCBC. Lecture Notes in Computer Science, 2007, , 434-451.	1.0	19
696	Tweakable Enciphering Schemes from Hash-Sum-Expansion. , 2007, , 252-267.		11
697	Randomness Extraction Via Î´-Biased Masking in the Presence of a QuantumÂAttacker. , 2008, , 465-481.		23
698	On Notions of Security for Deterministic Encryption, and Efficient Constructions without Random Oracles. Lecture Notes in Computer Science, 2008, , 335-359.	1.0	147
699	Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms. Lecture Notes in Computer Science, 2008, , 144-161.	1.0	69
700	An Improved Robust Fuzzy Extractor. Lecture Notes in Computer Science, 2008, , 156-171.	1.0	14
701	Security Bounds for Quantum Cryptography with Finite Resources. Lecture Notes in Computer Science, 2008, , 83-95.	1.0	19
702	Quantum Cryptography. , 2012, , 1521-1543.		4
703	An Optimally Fair Coin Toss. Lecture Notes in Computer Science, 2009, , 1-18.	1.0	50
704	Fairness with an Honest Minority and a Rational Majority. Lecture Notes in Computer Science, 2009, , 36-53.	1.0	61
705	Security of Truncated MACs. Lecture Notes in Computer Science, 2009, , 96-114.	1.0	5
706	Beyond-Birthday-Bound Security Based on Tweakable Block Cipher. Lecture Notes in Computer Science, 2009, , 308-326.	1.0	43
707	MAC Reforgeability. Lecture Notes in Computer Science, 2009, , 345-362.	1.0	23
708	HBS: A Single-Key Mode of Operation for Deterministic Authenticated Encryption. Lecture Notes in Computer Science, 2009, , 394-415.	1.0	31
709	Nonce Generators and the Nonce Reset Problem. Lecture Notes in Computer Science, 2009, , 411-426.	1.0	11
710	MAC Precomputation with Applications to Secure Memory. Lecture Notes in Computer Science, 2009, , 427-442.	1.0	6
711	HMAC without the â€œSecondâ€•Key. Lecture Notes in Computer Science, 2009, , 443-458.	1.0	11

#	Article	IF	Citations
712	QKD in Standard Optical Telecommunications Networks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 142-149.	0.2	20
713	The Case for Quantum Key Distribution. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 283-296.	0.2	21
715	On the k-Independence Required by Linear Probing and Minwise Independence. Lecture Notes in Computer Science, 2010, , 715-726.	1.0	11
716	Revisiting the Security of the Alred Design. Lecture Notes in Computer Science, 2011, , 69-83.	1.0	2
717	Secret Keys from Channel Noise. Lecture Notes in Computer Science, 2011, , 266-283.	1.0	9
718	An Almost-Optimal Forward-Private RFID Mutual Authentication Protocol with Tag Control. Lecture Notes in Computer Science, 2011, , 69-84.	1.0	6
719	Unconditionally Secure Rational Secret Sharing in Standard Communication Networks. Lecture Notes in Computer Science, 2011, , 355-369.	1.0	13
720	Program Obfuscation with Leaky Hardware. Lecture Notes in Computer Science, 2011, , 722-739.	1.0	29
721	Efficient Threshold Encryption from Lossy Trapdoor Functions. Lecture Notes in Computer Science, 2011, , 163-178.	1.0	8
722	Analysis of the Initial and Modified Versions of the Candidate 3GPP Integrity Algorithm 128-EIA3. Lecture Notes in Computer Science, 2012, , 230-242.	1.0	8
723	Hardness Preserving Constructions of Pseudorandom Functions. Lecture Notes in Computer Science, 2012, , 369-382.	1.0	8
724	Unconditionally-Secure Robust Secret Sharing with Compact Shares. Lecture Notes in Computer Science, 2012, , 195-208.	1.0	35
725	Message Authentication, Revisited. Lecture Notes in Computer Science, 2012, , 355-374.	1.0	65
726	Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes. Lecture Notes in Computer Science, 2012, , 216-225.	1.0	45
727	On Security of Universal Hash Function Based Multiple Authentication. Lecture Notes in Computer Science, 2012, , 303-310.	1.0	2
728	New Universal Hash Functions. Lecture Notes in Computer Science, 2012, , 99-108.	1.0	8
729	SipHash: A Fast Short-Input PRF. Lecture Notes in Computer Science, 2012, , 489-508.	1.0	101
730	Quantum Security Analysis via Smoothing of Renyi Entropy of Order 2. Lecture Notes in Computer Science, 2013, , 128-140.	1.0	5

#	Article	IF	Citations
731	Hardness Preserving Reductions via Cuckoo Hashing. Lecture Notes in Computer Science, 2013, , 40-59.	1.0	10
732	Quantum-Secure Message Authentication Codes. Lecture Notes in Computer Science, 2013, , 592-608.	1.0	64
733	The Security and Performance of â€œGCMâ€•when Short Multiplications Are Used Instead. Lecture Notes in Computer Science, 2013, , 225-245.	1.0	8
734	Quantum Algorithms for the Subset-Sum Problem. Lecture Notes in Computer Science, 2013, , 16-33.	1.0	33
735	Quantum Key Distribution in the Classical Authenticated Key Exchange Framework. Lecture Notes in Computer Science, 2013, , 136-154.	1.0	22
736	Unconditionally-Secure Robust Secret Sharing with Minimum Share Size. Lecture Notes in Computer Science, 2013, , 96-110.	1.0	11
737	Automated Security Proofs for Almost-Universal Hash for MAC Verification. Lecture Notes in Computer Science, 2013, , 291-308.	1.0	3
738	Universal Security. Lecture Notes in Computer Science, 2013, , 121-124.	1.0	5
739	A Modular Framework for Building Variable-Input-Length Tweakable Ciphers. Lecture Notes in Computer Science, 2013, , 405-423.	1.0	24
740	On Weak Keys and Forgery Attacks Against Polynomial-Based MAC Schemes. Lecture Notes in Computer Science, 2014, , 287-304.	1.0	21
741	Fast Pseudorandomness for Independence and Load Balancing. Lecture Notes in Computer Science, 2014, , 859-870.	1.0	6
742	Cryptography from Compression Functions: The UCE Bridge to the ROM. Lecture Notes in Computer Science, 2014, , 169-187.	1.0	9
743	Forging Attacks on Two Authenticated Encryption Schemes COBRA and POET. Lecture Notes in Computer Science, 2014, , 126-140.	1.0	6
744	General Statistically Secure Computation with Bounded-Resettable Hardware Tokens. Lecture Notes in Computer Science, 2015, , 319-344.	1.0	10
745	Graph-Induced Multilinear Maps from Lattices. Lecture Notes in Computer Science, 2015, , 498-527.	1.0	126
746	Pipelineable On-line Encryption. Lecture Notes in Computer Science, 2015, , 205-223.	1.0	19
748	Twisted Polynomials and Forgery Attacks on GCM. Lecture Notes in Computer Science, 2015, , 762-786.	1.0	12
750	On the Influence of Message Length in PMACâ€™s Security Bounds. Lecture Notes in Computer Science, 2016, , 596-621.	1.0	6

#	Article	IF	Citations
751	Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications. Lecture Notes in Computer Science, 2016, , 514-532.	1.0	6
752	Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers. Lecture Notes in Computer Science, 2016, , 33-63.	1.0	64
753	EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. Lecture Notes in Computer Science, 2016, , 121-149.	1.0	45
754	On the Computational Overhead of MPC with Dishonest Majority. Lecture Notes in Computer Science, 2017, , 369-395.	1.0	4
755	Quantum key distribution integration with optical dense wavelength division multiplexing: a review. IET Quantum Communication, 2020, 1, 9-15.	2.2	16
756	Practical issues in decoy-state quantum key distribution based on the central limit theorem. Physical Review A, 2017, 96, .	1.0	17
757	A quantum key distribution protocol for rapid denial of service detection. EPJ Quantum Technology, 2020, 7, .	2.9	10
758	On the k -Independence Required by Linear Probing and Minwise Independence. ACM Transactions on Algorithms, 2016, 12, 1-27.	0.9	9
759	Triangle Finding and Listing in CONGEST Networks. , 2017, , .		20
760	VAULT. ACM SIGPLAN Notices, 2018, 53, 665-678.	0.2	14
761	Quantum Key Distribution. ACM Computing Surveys, 2021, 53, 1-41.	16.1	100
762	Sketch-based change detection. , 2003, , .		360
763	Authentication of Quantum Messages. , 2011, , .		1
764	Experimental composable security decoy-state quantum key distribution using time-phase encoding. Optics Express, 2020, 28, 29479.	1.7	17
765	Establishing Software Root of Trust Unconditionally. , 2019, , .		12
766	Pairwise Independence and Derandomization. Foundations and Trends in Theoretical Computer Science, 2005, 1, 237-301.	2.0	37
767	Generalization and Extension of XEX* Mode. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 517-524.	0.2	7
768	Security Proof of Quantum Key Distribution. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 880-888.	0.2	2

#	Article	IF	Citations
769	Further More on Key Wrapping. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A, 8-20.	0.2	3
772	A largely self-contained and complete security proof for quantum key distribution. Quantum - the Open Journal for Quantum Science, 0, 1, 14.	0.0	71
773	How to Extract and Train the Classifier in Traffic Anomaly Detection System. Jisuanji Xuebao/Chinese Journal of Computers, 2012, 35, 719-729.	0.3	3
774	On the Capacity and Security of Steganography Approaches: An Overview. Journal of Applied Sciences, 2010, 10, 1825-1833.	0.1	60
776	Sound Probabilistic #SAT with Projection. Electronic Proceedings in Theoretical Computer Science, EPTCS, 0, 227, 15-29.	0.8	5
777	802.11i Encryption Key Distribution Using Quantum Cryptography. Journal of Networks, 2006, 1, .	0.4	30
780	Sublinear-Space Approximation Algorithms for Max r-SAT. Lecture Notes in Computer Science, 2021, , 124-136.	1.0	0
781	Son Ä°ÅŸlem AlgoritmalarÄ± Ä°Ã§in Web TabanlÄ± YazÄ±lÄ±m Suiti GeliÅŸtirilmesi. European Journal of Science and Technology, 0, , .	0.5	0
782	Method for Authentication of Diffie â€' Hellman Values Based on Pre-Distributed Random Sequences and Wegman â€' Carter One-Time Pad Algorithm. Proceedings of Telecommunication Universities, 2021, 7, 79-90.	0.1	0
784	A Parallel Algorithm for Extending Cryptographic Hash Functions. Lecture Notes in Computer Science, 2001, , 40-49.	1.0	6
786	Quantum vernam cipher. Quantum Information and Computation, 2002, 2, 14-34.	0.1	41
787	Provable Security of 3GPP Integrity Algorithm f9. The KIPS Transactions PartC, 2002, 9C, 573-580.	0.2	0
788	Single-Path Authenticated-Encryption Scheme Based on Universal Hashing. Lecture Notes in Computer Science, 2003, , 94-109.	1.0	1
789	An Efficient MAC for Short Messages. Lecture Notes in Computer Science, 2003, , 353-368.	1.0	8
790	Square Hash with a Small Key Size. Lecture Notes in Computer Science, 2003, , 522-531.	1.0	2
791	An Empirical Test Suite for Message Authentication Evaluation in Communications Based on Support Vector Machines. Lecture Notes in Computer Science, 2004, , 622-627.	1.0	0
792	New encoding schemes for quantum authentication. Quantum Information and Computation, 2005, 5, 1-12.	0.1	14
793	Unconditionally Secure Information Authentication in Presence of Erasures. Lecture Notes in Computer Science, 2005, , 304-321.	1.0	1

#	Article	IF	Citations
794	Can quantum cryptography imply quantum mechanics?. Quantum Information and Computation, 2005, 5, 161-169.	0.1	5
795	Cryptanalysis of a Practical Quantum Key Distribution with Polarization-Entangled Photons. Quantum Information and Computation, 2005, 5, 181-186.	0.1	6
796	A Cramer-Shoup Variant Related to the Quadratic Residuosity Problem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2006, E89-A, 203-205.	0.2	0
797	New Constructions of Universal Hash Functions Based on Function Sums. Lecture Notes in Computer Science, 2006, , 416-425.	1.0	1
799	Hybrid Symmetric Encryption Using Known-Plaintext Attack-Secure Components. Lecture Notes in Computer Science, 2006, , 242-260.	1.0	4
800	Unconditionally Secure Authentication in Quantum Key Distribution. SSRN Electronic Journal, 0, , .	0.4	0
801	Improved MACs from Differentially-Uniform Permutations. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007, E90-A, 2908-2915.	0.2	2
802	Quantum Key Distribution. , 2008, , 708-711.		0
803	A fast real-time memory authentication protocol. , 2008, , .		7
804	Towards a Reliable Evaluation Framework for Message Authentication in Web-Based Transactions Based on an Improved Computational Intelligence and Dynamical Systems Methodology. Lecture Notes in Computer Science, 2009, , 595-602.	1.0	0
805	Secret Key Generation Among Multiple Terminals with Applications to Wireless Systems. , 2009, , 231-260.		0
806	Quantum direct communication with mutual authenticationQuantum direct communication with mutual authenticationQuantum direct communication with mutual authentication. Quantum Information and Computation, 2009, 9, 376-394.	0.1	30
807	On parallel composition of zero-knowledge proofs with black-box quantum. Quantum Information and Computation, 2009, 9, 513-532.	0.1	1
808	Crypto Topics and Applications I. Chapman & Hall/CRC Applied Algorithms and Data Structures Series, 2009, , 1-31.	0.1	1
809	Sketch-Based Anomalies Detection with IP Address Traceability. Ruan Jian Xue Bao/Journal of Software, 2009, 20, 2899-2906.	0.3	4
810	Domain Extension for Enhanced Target Collision-Resistant Hash Functions. Lecture Notes in Computer Science, 2010, , 153-167.	1.0	3
811	Quantum Authentication. , 2010, , 167-215.		0
812	Quantum Key Distribution. Lecture Notes in Physics, 2010, , 23-47.	0.3	1

#	Article	IF	Citations
813	Conventional Cryptographic Primitives. , 2010, , 207-227.		0
814	Quantum Key Distribution. , 2010, , 103-134.		0
817	Practical quantum cryptography for secure free-space communications. International Journal of Computer and Communication Technology, 2010, , 208-217.	0.1	0
818	Quantum-Resilient Randomness Extraction. Lecture Notes in Computer Science, 2011, , 52-57.	1.0	0
820	$mathcal{E}$ -MACs: Towards More Secure and More Efficient Constructions of Secure Channels. Lecture Notes in Computer Science, 2011, , 292-310.	1.0	1
821	Characterization of the Relations between Information-Theoretic Non-malleability, Secrecy, and Authenticity. Lecture Notes in Computer Science, 2011, , 6-24.	1.0	5
822	Public Discussion Must Be Back and Forth in Secure Message Transmission. Lecture Notes in Computer Science, 2011, , 325-337.	1.0	1
823	GMAC. , 2011, , 513-514.		0
824	Authentication, From an Information Theoretic Perspective. , 2011, , 63-65.		0
825	Quantum Cryptography. , 2011, , 1005-1010.		0
826	Authenticated Encryption. , 2011, , 52-61.		2
827	Memory Integrity Protection. , 2012, , 305-324.		0
828	Quantum Key Distribution. , 0, , .		4
829	Methods of collision characteristic research of the message authentification codes. Military Technical Collection, 2011, .	0.1	0
830	Resistance against Adaptive Plaintext-Ciphertext Iterated Distinguishers. Lecture Notes in Computer Science, 2012, , 528-544.	1.0	1
831	The Low-Call Diet: Authenticated Encryption for Call Counting HSM Users. Lecture Notes in Computer Science, 2013, , 359-374.	1.0	1
832	Authentication using Secure Node Signature Verification Algorithm with Quantum Cryptography. International Journal of Computer Applications, 2013, 79, 43-47.	0.2	1
833	Fundamentals of Physical Layer Security. Wireless Networks and Mobile Communications, 2013, , 1-16.	1.0	0

#	Article	IF	Citations
834	Symmetrische Verfahren. EXamen Press, 2014, , 175-207.	0.0	0
835	How to construct a family of strong one way permutations. Lecture Notes in Computer Science, 1993, , 97-110.	1.0	0
837	Efficient equality-testing and updating of sets. Lecture Notes in Computer Science, 1995, , 48-58.	1.0	0
839	Quantum cryptography on optical fiber networks. Lecture Notes in Computer Science, 1998, , 35-46.	1.0	0
840	MRD Hashing. Lecture Notes in Computer Science, 1998, , 134-149.	1.0	1
841	Visual Cryptography â€" How to Use Images to Share a Secret. Informatik Aktuell, 1998, , 3-12.	0.4	0
842	Message Authentication Codes. , 2014, , 127-172.		5
843	A Novel Distributed Secret Key Extraction Technique for Wireless Network. The Journal of Korean Institute of Communications and Information Sciences, 2014, 39A, 708-717.	0.0	1
844	Quantum Key Distribution. , 2015, , 1-6.		1
845	Efficient Almost Strongly Universal Hash Function for Quantum Key Distribution. Lecture Notes in Computer Science, 2015, , 282-285.	1.0	1
847	Fundamental Two-Party Quantum Secret Sharing Protocol without Quantum Entanglement. International Journal of Security and Its Applications, 2015, 9, 293-302.	0.5	1
848	Message Authentication Codes (MACs). EXamen Press, 2016, , 363-375.	0.0	0
852	A flexible continuous-variable QKD system using off-the-shelf components. , 2017, , .		6
853	Ubiquitous Weak-Key Classes ofÂBRW-Polynomial Function. Lecture Notes in Computer Science, 2018, , 33-50.	1.0	0
854	Quantum Cryptography. , 2018, , 813-845.		0
855	Hash Functions and Their Applications. Advances in Information Security, Privacy, and Ethics Book Series, 2018, , 66-77.	0.4	2
857	Quantum cryptography with malicious devices. , 2018, , .		0
858	Physical-Layer Security. , 2019, , 93-161.		0

#	Article	IF	Citations
859	Online and Scalable Adaptive Cyber Defense. Lecture Notes in Computer Science, 2019, , 232-261.	1.0	1
860	Fast Locality-Sensitive Hashing Frameworks for Approximate Near Neighbor Search. Lecture Notes in Computer Science, 2019, , 3-17.	1.0	8
861	Multi-bit quantum digital signature based on temporal quantum ghost imaging. , 2019, , .		0
862	Parallelizable MACs Based on the Sum of PRPs with Security Beyond the Birthday Bound. Lecture Notes in Computer Science, 2019, , 131-151.	1.0	5
864	Implementation Security Certification of a Quantum Key Distribution System through Device Characterization. , 2019, , .		0
865	Perfectly Secure Message Transmission Against Independent Rational Adversaries. Lecture Notes in Computer Science, 2019, , 563-582.	1.0	2
866	Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange. Lecture Notes in Computer Science, 2019, , 206-226.	1.0	35
867	Quantum Encryption with Certified Deletion. Lecture Notes in Computer Science, 2020, , 92-122.	1.0	20
868	Universal Forgery Attack Against GCM-RUP. Lecture Notes in Computer Science, 2020, , 15-34.	1.0	0
869	Threshold trapdoor functions and their applications. IET Information Security, 2020, 14, 220-231.	1.1	1
870	Fast hashing with strong concentration bounds. , 2020, , .		1
871	Securing Blockchain with Quantum Safe Cryptography: When and How?. Advances in Intelligent Systems and Computing, 2021, , 371-379.	0.5	0
872	FORMATION OF HASH CODES BASED ON THE UMAC ALGORITHM ON HYBRID CRYPTO-CODE CONSTRUCTIONS OF McELICE ON DAMAGED CODES. International Journal of 3d Printing Technologies and Digital Industry, 2020, 4, 106-115.	0.3	0
874	The Summation-Truncation Hybrid: Reusing Discarded Bits for Free. Lecture Notes in Computer Science, 2020, , 187-217.	1.0	3
875	The circulant hash revisited. Journal of Mathematical Cryptology, 2020, 15, 250-257.	0.4	0
876	Cryptographic Games. Advanced Sciences and Technologies for Security Applications, 2020, , 223-247.	0.4	0
877	On the Query Complexity of Constructing PRFs from Non-adaptive PRFs. Lecture Notes in Computer Science, 2020, , 546-565.	1.0	0
878	Improved Security Analysis for Nonce-Based Enhanced Hash-then-Mask MACs. Lecture Notes in Computer Science, 2020, , 697-723.	1.0	6

#	Article	IF	Citations
879	Packed Multiplication: How to Amortize the Cost of Side-Channel Masking?. Lecture Notes in Computer Science, 2020, , 851-880.	1.0	2
880	Describing and Simulating Concurrent Quantum Systems. Lecture Notes in Computer Science, 2020, , 271-277.	1.0	1
882	Mind the Composition: Birthday Bound Attacks on EWCDMD and SoKAC21. Lecture Notes in Computer Science, 2020, , 203-220.	1.0	9
883	Information-Theoretic Security of Cryptographic Channels. Lecture Notes in Computer Science, 2020, , 295-311.	1.0	0
884	Introduction and Preliminaries. Indian Statistical Institute Series, 2020, , 1-29.	0.1	0
885	BBB Secure Nonce Based MAC Using Public Permutations. Lecture Notes in Computer Science, 2020, , 172-191.	1.0	5
886	Pythia: Intellectual Property Verification in Zero-Knowledge. , 2020, , .		4
887	Quantum Key Distribution Networks. Advances in Information Security, Privacy, and Ethics Book Series, 0, , 61-96.	0.4	1
888	Quantum Cryptography. Advances in Information Security, Privacy, and Ethics Book Series, 0, , 260-292.	0.4	0
889	A Construction for One Way Hash Functions and Pseudorandom Bit Generators. , 1991, , 431-445.		1
890	Two Improved Range-Efficient Algorithms for F 0 Estimation. , 2007, , 659-669.		1
891	Multilane HMACâ€" Security beyond the Birthday Limit. , 2007, , 18-32.		15
892	Saving Private Randomness in One-Way Functions and Pseudorandom Generators. , 2008, , 607-625.		5
895	Equivalence of Three Classical Algorithms With Quantum Side Information: Privacy Amplification, Error Correction, and Data Compression. IEEE Transactions on Information Theory, 2022, 68, 1016-1031.	1.5	5
896	Differential properties of authenticated encryption mode based on universal hash function (XTSMAC). , 2021, , .		0
897	Hybrid Encryption in Correlated Randomness Model. , 2021, , .		0
898	Deployment-Ready Quantum Key Distribution Over a Classical Network Infrastructure in Padua. Journal of Lightwave Technology, 2022, 40, 1658-1663.	2.7	7
899	Categorization of Faulty Nonce Misuse Resistant Message Authentication. Lecture Notes in Computer Science, 2021, , 520-550.	1.0	3

#	Article	IF	Citations
900	Long-Term Secure Distributed Storage Using Quantum Key Distribution Network With Third-Party Verification. IEEE Transactions on Quantum Engineering, 2022, 3, 1-11.	2.9	4
901	Digital Signatures with Quantum Candies. Entropy, 2022, 24, 207.	1.1	0
902	Practical quantum multiparty signatures using quantum-key-distribution networks. Physical Review A, 2022, 105, .	1.0	5
903	Memory-Saving and High-Speed Privacy Amplification Algorithm Using LFSR-Based Hash Function for Key Generation. Electronics (Switzerland), 2022, 11, 377.	1.8	4
904	Secure List Decoding and its Application to Bit-String Commitment. IEEE Transactions on Information Theory, 2022, 68, 3620-3642.	1.5	2
905	Quantum-Inspired Secure Wireless Communication Protocol Under Spatial and Local Gaussian Noise Assumptions. IEEE Access, 2022, 10, 29040-29068.	2.6	3
906	Multi-user Security of the Elephant v2 Authenticated Encryption Mode. Lecture Notes in Computer Science, 2022, , 155-178.	1.0	3
907	Quantum Identity Authentication Based on Round Robin Differencial Phase Shift Communication Line. International Journal of Theoretical Physics, 2022, 61, 1.	0.5	2
908	Authentication of variable length messages in quantum key distribution. EPJ Quantum Technology, 2022, 9, 8.	2.9	5
909	Quantum key distribution using universal hash functions over finite fields. Quantum Information Processing, 2022, 21, 1.	1.0	2
910	Two-way unclonable encryption with a vulnerable sender. International Journal of Quantum Information, 2022, 20, .	0.6	0
911	Can't touch this: unconditional tamper evidence from short keys. Quantum Information and Computation, 2022, 22, 361-384.	0.1	0
912	Secure Physical Layer Network Coding versus Secure Network Coding. Entropy, 2022, 24, 47.	1.1	1
913	Resource-Aware Cryptography: An Analysis of Lightweight Cryptographic Primitives. SN Computer Science, 2022, 3, 1.	2.3	1
915	Quantum Communication Using Semiconductor Quantum Dots. Advanced Quantum Technologies, 2022, 5, .	1.8	64
916	Scalable Authentication and Optimal Flooding in a Quantum Network. PRX Quantum, 2022, 3, .	3.5	6
918	Lazy structure sharing for query optimization. Acta Informatica, 1995, 32, 255-270.	0.5	0
919	BP-MAC: Fast Authentication for Short Messages. , 2022, , .		7

#	Article	IF	Citations
920	Multi-user BBB security of public permutations based MAC. Cryptography and Communications, 2022, 14, 1145-1177.	0.9	4
921	Fair and Efficient Robust Secret Sharing Scheme against Rushing Adversaries. Security and Communication Networks, 2022, 2022, 1-12.	1.0	0
922	Analyzing the Security of Three-State Protocols Using Information-Theoretic. SSRN Electronic Journal, 0, , .	0.4	0
923	On the robustness of information-theoretic authentication in quantum cryptography. Laser Physics Letters, 2022, 19, 075203.	0.6	3
924	Authenticated QKD Based on Orthogonal States. International Journal of Theoretical Physics, 2022, 61, .	0.5	0
926	Entropy-Learned Hashing: Constant Time Hashing with Controllable Uniformity. , 2022, , .		1
927	A Modified Key Sifting Scheme With Artificial Neural Network Based Key Reconciliation Analysis in Quantum Cryptography. IEEE Access, 2022, 10, 72743-72757.	2.6	4
928	Security in quantum cryptography. Reviews of Modern Physics, 2022, 94, .	16.4	74
929	Open-Source Hardware Memory Protection Engine Integrated With NVMM Simulator. IEEE Computer Architecture Letters, 2022, 21, 77-80.	1.0	0
930	Authentication of smart grid communications using quantum key distribution. Scientific Reports, 2022, 12, .	1.6	7
931	Mitigating 5G security challenges for next-gen industry using quantum computing. Journal of King Saud University - Computer and Information Sciences, 2023, 35, 101334.	2.7	6
935	Quantum key distribution. , 2022, , 215-272.		0
936	Fundamentals of Quantum Key Distribution. , 2022, , 1-28.		3
937	Perfectly Secure Message Transmission Against Rational Adversaries. IEEE Journal on Selected Areas in Information Theory, 2022, 3, 390-404.	1.9	1
938	Randomized First-Order Monitoring withÂHashing. Lecture Notes in Computer Science, 2022, , 3-24.	1.0	1
939	Cryptography in the Quantum Era. , 2022, , .		3
940	Review of OFC 2022 Optical Networks and Communications Conference Hybrid (Virtual/In-Person) Conference: 6â€“10 March 2022, San Diego, CA. Fiber and Integrated Optics, 0, , 1-20.	1.7	0
941	Hybrid Cryptosystem Ensuring CIA Triad. International Journal of Engineering and Advanced Technology, 2022, 12, 50-53.	0.2	0

#	Article	IF	Citations
942	The Gap Is Sensitive to Size of Preimages: Collapsing Property Doesnâ€™t Go Beyond Quantum Collision-Resistance for Preimages Bounded Hash Functions. Lecture Notes in Computer Science, 2022, , 564-595.	1.0	2
943	Harm-DoS: Hash Algorithm Replacement for Mitigating Denial-of-Service Vulnerabilities in Binary Executables. , 2022, , .		1
944	Secure secondary utilization system of genomic data using quantum secure cloud. Scientific Reports, 2022, 12, .	1.6	2
945	Quantum and Post-Quantum Cybersecurity Challenges and Finance Organizations Readiness. Advances in Information Security, Privacy, and Ethics Book Series, 2022, , 314-337.	0.4	0
946	Computational indistinguishability and boson sampling. Physica Scripta, 0, , .	1.2	0
947	A short review on quantum identity authentication protocols: how would Bob know that he is talking with Alice?. Quantum Information Processing, 2022, 21, .	1.0	14
948	Private Randomness Agreement and its Application in Quantum Key Distribution Networks. IEEE Communications Letters, 2023, 27, 477-481.	2.5	0
949	Unconditional Proofs-of-Work and Other Possibilities of Thermodynamic Cryptography. , 2022, , .		0
950	Controlled secure direct quantum communication inspired scheme for quantum identity authentication. Quantum Information Processing, 2023, 22, .	1.0	15
951	QKD parameter estimation by two-universal hashing. Quantum - the Open Journal for Quantum Science, 0, 7, 894.	0.0	0
952	No Repetition. Proceedings of the VLDB Endowment, 2022, 15, 3989-4001.	2.1	1
953	On the Security of Offloading Post-Processing for Quantum Key Distribution. Entropy, 2023, 25, 226.	1.1	1
954	Quantum Attacks onÂPRFs Based onÂPublic Random Permutations. Lecture Notes in Computer Science, 2022, , 566-591.	1.0	1
955	Security of device-independent quantum key distribution protocols: a review. Quantum - the Open Journal for Quantum Science, 0, 7, 932.	0.0	11
956	Post-quantum Security for the Extended Access Control Protocol. Lecture Notes in Computer Science, 2023, , 22-52.	1.0	0
957	Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together. , 0, 2, .		0
958	Wireless-Channel Key Exchange. Lecture Notes in Computer Science, 2023, , 672-699.	1.0	0
959	Commitment Capacity of Classical-Quantum Channels. IEEE Transactions on Information Theory, 2023, 69, 5083-5099.	1.5	0

#	Article	IF	Citations
961	Crypto-agile Design and Testbed for QKD-Networks. , 2023, , .		0
962	Subversion-Resilient Authenticated Encryption Without Random Oracles. Lecture Notes in Computer Science, 2023, , 460-483.	1.0	1
964	A Critical Analysis ofÂClassifier Selection inÂLearned Bloom Filters: The Essentials. Communications in Computer and Information Science, 2023, , 47-61.	0.4	0
967	Multi-instance Secure Public-Key Encryption. Lecture Notes in Computer Science, 2023, , 336-367.	1.0	0
968	Universal Hashing Based onÂField Multiplication andÂ(Near-)MDS Matrices. Lecture Notes in Computer Science, 2023, , 129-150.	1.0	0
970	On theÂSecurity ofÂKeyed Hashing Based onÂPublic Permutations. Lecture Notes in Computer Science, 2023, , 607-627.	1.0	0
971	Key Management Systems for Large-Scale Quantum Key Distribution Networks. , 2023, , .		0
974	Îµ-Almost Collision-Flat Universal Hash Functions Motivated by Information-Theoretic Security. , 2023, , .		1
975	Describing and Animating Quantum Protocols. Outstanding Contributions To Logic, 2023, , 447-473.	0.2	0
981	Forgery Attacks onÂSeveral Beyond-Birthday-Bound Secure MACs. Lecture Notes in Computer Science, 2023, , 169-189.	1.0	0
985	Quantum Key Distribution and Authentication in the Cloud for Internet of Things. Advances in Information Security, Privacy, and Ethics Book Series, 2024, , 48-65.	0.4	0