Bart Preneel

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/8141430/publications.pdf

Version: 2024-02-01

370 papers	8,603 citations	70961 41 h-index	95083 68 g-index
394 all docs	394 docs citations	394 times ranked	3859 citing authors

#	Article	IF	Citations
1	Mutual Information Analysis. Lecture Notes in Computer Science, 2008, , 426-442.	1.0	383
2	A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering, 2011, 16, 3-32.	2.1	360
3	RIPEMD-160: A strengthened version of RIPEMD. Lecture Notes in Computer Science, 1996, , 71-82.	1.0	280
4	Hash functions based on block ciphers: a synthetic approach. , 1993, , 368-378.		204
5	FPDetective. , 2013, , .		174
6	Propagation Characteristics of Boolean Functions. Lecture Notes in Computer Science, 1991, , 161-173.	1.0	133
7	The cipher SHARK. Lecture Notes in Computer Science, 1996, , 99-111.	1.0	124
8	Privacy Weaknesses in Biometric Sketches. , 2009, , .		114
9	Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. Lecture Notes in Computer Science, 2014, , 306-323.	1.0	113
10	State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures. , 2010, , .		101
11	A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher. Lecture Notes in Computer Science, 2004, , 245-259.	1.0	90
12	A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms. Lecture Notes in Computer Science, 2003, , 33-50.	1.0	87
13	FPGA Vendor Agnostic True Random Number Generator. , 2006, , .		83
14	Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning. , 2017, , .		79
15	Analysis Methods for (Alleged) RC4. Lecture Notes in Computer Science, 1998, , 327-341.	1.0	76
16	PriPAYD: Privacy-Friendly Pay-As-You-Drive Insurance. IEEE Transactions on Dependable and Secure Computing, 2011, 8, 742-755.	3.7	74
17	Power-Analysis Attacks on an FPGA â€“ First Experimental Results. Lecture Notes in Computer Science, 2003, , 35-50.	1.0	72
18	On the security of iterated message authentication codes. IEEE Transactions on Information Theory, 1999, 45, 188-199.	1.5	70

#	Article	IF	Citations
19	MDx-MAC and Building Fast MACs from Hash Functions. Lecture Notes in Computer Science, 1995, , 1-14.	1.0	69
20	Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms. Lecture Notes in Computer Science, 2008, , 144-161.	1.0	69
21	Hardware architectures for public key cryptography. The Integration VLSI Journal, 2003, 34, 1-64.	1.3	68
22	Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings. , 2007, , 264-277.		68
23	Authentication and payment in future mobile systems. Lecture Notes in Computer Science, 1998, , 277-293.	1.0	65
24	On the Security of Todayâ€™s Online Electronic Banking Systems. Computers and Security, 2002, 21, 253-265.	4.0	65
25	A New RFID Privacy Model. Lecture Notes in Computer Science, 2011, , 568-587.	1.0	65
26	On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (Extended Abstract). Lecture Notes in Computer Science, 2006, , 242-256.	1.0	63
27	A Systematic Evaluation of Compact Hardware Implementations for the Rijndael S-Box. Lecture Notes in Computer Science, 2005, , 323-333.	1.0	61
28	Sancus 2.0. ACM Transactions on Privacy and Security, 2017, 20, 1-33.	2.2	61
29	ARM: anonymous routing protocol for mobile ad hoc networks. International Journal of Wireless and Mobile Computing, 2009, 3, 145.	0.1	60
30	Attacks on Fast Double Block Length Hash Functions. Journal of Cryptology, 1998, 11, 59-72.	2.1	59
31	Publish or Perish: A Backward-Compatible Defense Against Selfish Mining in Bitcoin. Lecture Notes in Computer Science, 2017, , 277-292.	1.0	56
32	AEGIS: A Fast Authenticated Encryption Algorithm. Lecture Notes in Computer Science, 2014, , 185-201.	1.0	56
33	Distance Bounding in Noisy Environments. Lecture Notes in Computer Science, 2007, , 101-115.	1.0	54
34	Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192. Lecture Notes in Computer Science, 2005, , 368-383.	1.0	53
35	Remote attestation on legacy operating systems with trusted platform modules. Science of Computer Programming, 2008, 74, 13-22.	1.5	53
36	A Practical Attack on KeeLoq. , 2008, , 1-18.		53

#	Article	IF	Citations
37	Two Attacks on a White-Box AES Implementation. Lecture Notes in Computer Science, 2014, , 265-285.	1.0	52
38	Related-Key Rectangle Attacks on Reduced AES-192 and AES-256. Lecture Notes in Computer Science, 2007, , 225-241.	1.0	51
39	Cryptanalysis of a Perturbated White-Box AES Implementation. Lecture Notes in Computer Science, 2010, , 292-310.	1.0	51
40	A Provably Secure Anonymous Buyerâ€"Seller Watermarking Protocol. IEEE Transactions on Information Forensics and Security, 2010, 5, 920-931.	4.5	50
41	Efficient Isolation of Trusted Subsystems in Embedded Systems. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 344-361.	0.2	48
42	A cross-protocol attack on the TLS protocol. , 2012, , .		48
43	Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols' Security. , 2019, , .		47
44	Multicore Curve-Based Cryptoprocessor with Reconfigurable Modular Arithmetic Logic Units over GF(2^n). IEEE Transactions on Computers, 2007, 56, 1269-1282.	2.4	46
45	Revisiting Higher-Order DPA Attacks:. Lecture Notes in Computer Science, 2010, , 221-234.	1.0	45
46	Seven-Property-Preserving Iterated Hashing: ROX. , 2007, , 130-146.		44
47	An efficient buyer-seller watermarking protocol based on composite signal representation. , 2009, , .		44
48	End-To-End Security for Video Distribution: The Combination of Encryption, Watermarking, and Video Adaptation. IEEE Signal Processing Magazine, 2013, 30, 97-107.	4.6	44
49	On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. , 2016, , .		44
50	Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems. Computers and Electrical Engineering, 2007, 33, 367-382.	3.0	42
51	Analysis of Grainâ€™s Initialization Algorithm. Lecture Notes in Computer Science, 2008, , 276-289.	1.0	42
52	Criteria towards metrics for benchmarking template protection algorithms. , 2012, , .		42
53	The State of Cryptographic Hash Functions. Lecture Notes in Computer Science, 1999, , 158-182.	1.0	40
54	New Weak-Key Classes of IDEA. Lecture Notes in Computer Science, 2002, , 315-326.	1.0	40

#	Article	IF	Citations
55	Universally Composable Adaptive Priced Oblivious Transfer. Lecture Notes in Computer Science, 2009, , 231-247.	1.0	40
56	Dependence of RFID Reader Antenna Design on Read Out Distance. IEEE Transactions on Antennas and Propagation, 2008, 56, 3829-3837.	3.1	39
57	Impossible Differential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT. Lecture Notes in Computer Science, 2012, , 117-137.	1.0	39
58	Revisiting a Methodology for Efficient CNN Architectures in Profiling Attacks. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 147-168.	0.0	39
59	Authentication and payment in future mobile systems. Journal of Computer Security, 2000, 8, 183-207.	0.5	38
60	Pripayd. , 2007, , .		38
61	A MAC Mode for Lightweight Block Ciphers. Lecture Notes in Computer Science, 2016, , 43-59.	1.0	38
62	A taxonomy of self-modifying code for obfuscation. Computers and Security, 2011, 30, 679-691.	4.0	37
63	Software Performance of Universal Hash Functions. Lecture Notes in Computer Science, 1999, , 24-41.	1.0	36
64	Speed Records for NTRU. Lecture Notes in Computer Science, 2010, , 73-88.	1.0	35
65	A New Keystream Generator MUGI. Lecture Notes in Computer Science, 2002, , 179-194.	1.0	33
66	Power Analysis Attacks Against FPGA Implementations of the DES. Lecture Notes in Computer Science, 2004, , 84-94.	1.0	33
67	Perfect Matching Disclosure Attacks. Lecture Notes in Computer Science, 2008, , 2-23.	1.0	33
68	Soft Decision Error Correction for Compact Memory-Based PUFs Using a Single Enrollment. Lecture Notes in Computer Science, 2012, , 268-282.	1.0	33
69	Revisiting a combinatorial approach toward measuring anonymity. , 2008, , .		33
70	A family of trapdoor ciphers. Lecture Notes in Computer Science, 1997, , 139-148.	1.0	32
71	Proper RFID Privacy: Model and Protocols. IEEE Transactions on Mobile Computing, 2014, 13, 2888-2902.	3.9	32
72	Towards a framework for evaluating certificate status information mechanisms. Computer Communications, 2003, 26, 1839-1850.	3.1	31

#	Article	IF	Citations
73	Taxonomy of Mixes and Dummy Traffic. , 2004, , 217-232.		31
74	Efficient implementation of anonymous credentials on Java Card smart cards. , 2009, , .		31
75	A Privacy-Preserving Buyerâ€"Seller Watermarking Protocol Based on Priced Oblivious Transfer. IEEE Transactions on Information Forensics and Security, 2011, 6, 202-212.	4.5	31
76	Reasoning About the Anonymity Provided by Pool Mixes That Generate Dummy Traffic. Lecture Notes in Computer Science, 2004, , 309-325.	1.0	30
77	The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition. Lecture Notes in Computer Science, 2010, , 1-14.	1.0	30
78	SOFIA: Software and control flow integrity architecture. Computers and Security, 2017, 68, 16-35.	4.0	30
79	Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC. Lecture Notes in Computer Science, 2005, , 294-309.	1.0	30
80	Fast and secure hashing based on codes. Lecture Notes in Computer Science, 1997, , 485-498.	1.0	28
81	Collisions and Other Non-random Properties for Step-Reduced SHA-256. Lecture Notes in Computer Science, 2009, , 276-293.	1.0	28
82	Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator. Lecture Notes in Computer Science, 2003, , 52-67.	1.0	28
83	SOFIA: Software and Control Flow Integrity Architecture. , 2016, , .		28
84	Revocable anonymous access to the Internet?. Internet Research, 2003, 13, 242-258.	2.7	27
85	Improved Meet-in-the-Middle Attacks on Reduced-Round DES. , 2007, , 86-100.		27
86	A Secure Perceptual Hash Algorithm for Image Content Authentication. Lecture Notes in Computer Science, 2011, , 108-121.	1.0	26
87	Key recovery attack on ANSI X9.19 retail MAC. Electronics Letters, 1996, 32, 1568.	0.5	25
88	MacDES: MAC algorithm based on DES. Electronics Letters, 1998, 34, 871.	0.5	25
89	A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes. Lecture Notes in Computer Science, 2005, , 29-43.	1.0	25
90	Linear Cryptanalysis of RC5 and RC6. Lecture Notes in Computer Science, 1999, , 16-30.	1.0	25

#	Article	IF	Citations
91	Field Lifting for Smaller UOV Public Keys. Lecture Notes in Computer Science, 2017, , 227-246.	1.0	25
92	Cryptography on smart cards. Computer Networks, 2001, 36, 423-435.	3.2	24
93	Construction of secure and fast hash functions using nonbinary error-correcting codes. IEEE Transactions on Information Theory, 2002, 48, 2524-2539.	1.5	24
94	Public-Key Cryptography on the Top of a Needle. , 2007, , .		24
95	Related-Key Boomerang and Rectangle Attacks: Theory and Experimental Analysis. IEEE Transactions on Information Theory, 2012, 58, 4948-4966.	1.5	24
96	Extension Field Cancellation: A New Central Trapdoor for Multivariate Quadratic Systems. Lecture Notes in Computer Science, 2016, , 182-196.	1.0	24
97	On the Feasibility of Cryptography for a Wireless Insulin Pump System. , 2016, , .		23
98	Attack on Six Rounds of CRYPTON. Lecture Notes in Computer Science, 1999, , 46-59.	1.0	23
99	Embedded Trusted Computing with Authenticated Non-volatile Memory. Lecture Notes in Computer Science, 2008, , 60-74.	1.0	23
100	Evaluating certificate status information mechanisms. , 2000, , .		22
101	On Secure and Anonymous Buyer-Seller Watermarking Protocol. , 2008, , .		22
102	Equivalent Keys in HFE, C*, and Variations. Lecture Notes in Computer Science, 2005, , 33-49.	1.0	22
103	Towards Tamper Resistant Code Encryption: Practice and Experience. Lecture Notes in Computer Science, 2008, , 86-100.	1.0	22
104	Tripartite modular multiplication. The Integration VLSI Journal, 2011, 44, 259-269.	1.3	21
105	Collateral damage of Facebook third-party applications: a comprehensive study. Computers and Security, 2018, 77, 179-208.	4.0	21
106	Parallel Shortest Lattice Vector Enumeration on Graphics Cards. Lecture Notes in Computer Science, 2010, , 52-68.	1.0	21
107	On the Indifferentiability of the GrÃ¸stl Hash Function. Lecture Notes in Computer Science, 2010, , 88-105.	1.0	21
108	A Lightweight 256-Bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW. Lecture Notes in Computer Science, 2011, , 151-168.	1.0	21

#	Article	IF	Citations
109	Offline NFC payments with electronic vouchers. , 2009, , .		21
110	On Weaknesses of Nonâ€"surjective Round Functions. Designs, Codes, and Cryptography, 1997, 12, 253-266.	1.0	20
111	Reconfigurable modular arithmetic logic unit supporting high-performance RSA and ECC over GF(p). International Journal of Electronics, 2007, 94, 501-514.	0.9	20
112	Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks. IEEE Transactions on Vehicular Technology, 2010, 59, 519-532.	3.9	20
113	The Differential Analysis of S-Functions. Lecture Notes in Computer Science, 2011, , 36-56.	1.0	20
114	For some eyes only. , 2013, , .		20
115	SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision. Lecture Notes in Computer Science, 2017, , 475-493.	1.0	20
116	Resynchronization Attacks on WG and LEX. Lecture Notes in Computer Science, 2006, , 422-432.	1.0	20
117	On the XOR of Multiple Random Permutations. Lecture Notes in Computer Science, 2015, , 619-634.	1.0	20
118	Security Reductions of the Second Round SHA-3 Candidates. Lecture Notes in Computer Science, 2011, , 39-53.	1.0	20
119	On the Covering Radii of Binary Reedâ€"Muller Codes in the Set of Resilient Boolean Functions. IEEE Transactions on Information Theory, 2005, 51, 1182-1189.	1.5	19
120	Meet-in-the-Middle Attacks on Reduced-Round XTEA. Lecture Notes in Computer Science, 2011, , 250-267.	1.0	19
121	Open problems in hash function security. Designs, Codes, and Cryptography, 2015, 77, 611-631.	1.0	19
122	On Feistel Ciphers Using Optimal Diffusion Mappings Across Multiple Rounds. Lecture Notes in Computer Science, 2004, , 1-15.	1.0	19
123	Cryptanalysis of 3-Pass HAVAL. Lecture Notes in Computer Science, 2003, , 228-245.	1.0	19
124	MAME: A Compression Function with Reduced Hardware Requirements. Lecture Notes in Computer Science, 2007, , 148-165.	1.0	19
125	On the security of stepwise triangular systems. Designs, Codes, and Cryptography, 2006, 40, 285-302.	1.0	18
126	The Newton channel. Lecture Notes in Computer Science, 1996, , 151-156.	1.0	18

#	Article	IF	Citations
127	Large Superfluous Keys in $mathcal{M}$ ultivariate $mathcal{Q}$ uadratic Asymmetric Systems. Lecture Notes in Computer Science, 2005, , 275-287.	1.0	18
128	Towards Security Notions for White-Box Cryptography. Lecture Notes in Computer Science, 2009, , 49-58.	1.0	18
129	On Boolean Functions with Generalized Cryptographic Properties. Lecture Notes in Computer Science, 2004, , 120-135.	1.0	17
130	Classification of Boolean Functions of 6 Variables or Less with Respect to Some Cryptographic Properties. Lecture Notes in Computer Science, 2005, , 324-334.	1.0	17
131	Towards a crossâ€context identity management framework in eâ€health. Online Information Review, 2009, 33, 422-442.	2.2	17
132	An AES Based 256-bit Hash Function for Lightweight Applications: Lesamnta-LW. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A, 89-99.	0.2	17
133	Keyless car sharing system: A security and privacy analysis. , 2016, , .		17
134	On the (In)security of Stream Ciphers Based on Arrays and Modular Addition. Lecture Notes in Computer Science, 2006, , 69-83.	1.0	17
135	Efficient Oblivious Augmented Maps: Location-Based Services with a Payment Broker. , 2007, , 77-94.		17
136	Hash functions based on block ciphers and quaternary codes. Lecture Notes in Computer Science, 1996, , 77-90.	1.0	16
137	Efficient pipelining for modular multiplication architectures in prime fields. , 2007, , .		16
138	A survey of recent developments in cryptographic algorithms for smart cards. Computer Networks, 2007, 51, 2223-2233.	3.2	16
139	High-performance Public-key Cryptoprocessor for Wireless Mobile Applications. Mobile Networks and Applications, 2007, 12, 245-258.	2.2	16
140	Anonymous ID-Based Group Key Agreement for Wireless Networks. , 2008, , .		16
141	A general model for hiding control flow. , 2010, , .		16
142	Equivalent keys in â„³ultivariate uadratic public key systems. Journal of Mathematical Cryptology, 2011, 4, .	0.4	16
143	Format-compliant encryption techniques for high efficiency video coding. , 2013, , .		16
144	Differential-Linear Attacks Against the Stream Cipher Phelix. Lecture Notes in Computer Science, 2007, , 87-100.	1.0	16

#	Article	IF	Citations
145	The parazoa family: generalizing the sponge hash functions. International Journal of Information Security, 2012, 11, 149-165.	2.3	15
146	Time-Memory Trade-Off Attack on FPGA Platforms: UNIX Password Cracking. Lecture Notes in Computer Science, 2006, , 323-334.	1.0	15
147	Cryptanalysis of the CFB mode of the DES with a reduced number of rounds. , 1993, , 212-223.		15
148	Extending the Resynchronization Attack. Lecture Notes in Computer Science, 2004, , 19-38.	1.0	15
149	Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy. Lecture Notes in Computer Science, 2007, , 276-290.	1.0	15
150	Blind Differential Cryptanalysis for Enhanced Power Attacks. Lecture Notes in Computer Science, 2006, , 163-173.	1.0	15
151	A Model for Structure Attacks, with Applications to PRESENT and Serpent. Lecture Notes in Computer Science, 2012, , 49-68.	1.0	15
152	The Biryukov-Demirci Attack on Reduced-Round Versions of IDEA and MESH Ciphers. Lecture Notes in Computer Science, 2004, , 98-109.	1.0	14
153	The MESH Block Ciphers. Lecture Notes in Computer Science, 2004, , 458-473.	1.0	14
154	Secure and Privacy-Friendly Logging for eGovernment Services. , 2008, , .		14
155	Hash Functions Based on Three Permutations: A Generic Security Analysis. Lecture Notes in Computer Science, 2012, , 330-347.	1.0	14
156	A Practical Attack on KeeLoq. Journal of Cryptology, 2012, 25, 136-157.	2.1	14
157	Securing Wireless Neurostimulators. , 2018, , .		14
158	Distinguishing Attacks on the Stream Cipher Py. Lecture Notes in Computer Science, 2006, , 405-421.	1.0	14
159	Protected Software Module Architectures. , 2013, , 241-251.		14
160	SC2Share: Smart Contract for Secure Car Sharing. , 2019, , .		14
161	Cryptographic Primitives for Information Authentication â€" State of the Art. Lecture Notes in Computer Science, 1998, , 49-104.	1.0	13
162	Attacking Some Perceptual Image Hash Algorithms. , 2007, , .		13

#	Article	IF	Citations
163	Practical DPA attacks on MDPL. , 2009, , .		13
164	Friend in the Middle (FiM): Tackling de-anonymization in social networks. , 2013, , .		13
165	On Unconditionally Secure Distributed Oblivious Transfer. Lecture Notes in Computer Science, 2002, , 395-408.	1.0	13
166	Improved characteristics for differential cryptanalysis of hash functions based on block ciphers. Lecture Notes in Computer Science, 1995, , 242-248.	1.0	13
167	A Three-Property-Secure Hash Function. Lecture Notes in Computer Science, 2009, , 228-244.	1.0	13
168	Robust Image Content Authentication with Tamper Location. , 2012, , .		12
169	Optimal sporadic location privacy preserving systems in presence of bandwidth constraints. , 2013, , .		12
170	Linear Cryptanalysis of Reduced-Round Versions of the SAFER Block Cipher Family. Lecture Notes in Computer Science, 2001, , 244-261.	1.0	12
171	Anti-counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware. Information Security and Cryptography, 2010, , 237-257.	0.2	12
172	Security analysis of the message authenticator algorithm (MAA). European Transactions on Telecommunications, 1997, 8, 455-470.	1.2	11
173	On the Security of Double and 2-Key Triple Modes of Operation. Lecture Notes in Computer Science, 1999, , 215-230.	1.0	11
174	A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks. , 2008, , .		11
175	Anonymous user communication for privacy protection in wireless metropolitan mesh networks. , 2009, , .		11
176	On the Necessity of a Prescribed Block Validity Consensus. , 2017, , .		11
177	Recent Developments in the Design of Conventional Cryptographic Algorithms. Lecture Notes in Computer Science, 1998, , 105-130.	1.0	11
178	Cryptanalysis of Sober-t32. Lecture Notes in Computer Science, 2003, , 111-128.	1.0	11
179	Practical Collisions for EnRUPT. Lecture Notes in Computer Science, 2009, , 246-259.	1.0	11
180	Threat Modelling for Security Tokens in Web Applications. International Federation for Information Processing, 2005, , 183-193.	0.4	10

#	Article	IF	Citations
181	Probabilistic Algebraic Attacks. Lecture Notes in Computer Science, 2005, , 290-303.	1.0	10
182	Key Establishment Using Secure Distance Bounding Protocols. , 2007, , .		10
183	Reversing protected minutiae vicinities. , 2010, , .		10
184	Toward More Secure and Reliable Access Control. IEEE Pervasive Computing, 2012, 11, 76-83.	1.1	10
185	Practical identity-based private sharing for online social networks. Computer Communications, 2016, 73, 243-250.	3.1	10
186	Toward a Common Performance and Effectiveness Terminology for Digital Proximity Tracing Applications. Frontiers in Digital Health, 2021, 3, 677929.	1.5	10
187	Improved Square Attacks against Reduced-Round Hierocrypt. Lecture Notes in Computer Science, 2002, , 165-173.	1.0	10
188	Efficient Negative Databases from Cryptographic Hash Functions. Lecture Notes in Computer Science, 2007, , 423-436.	1.0	10
189	Related-Key Attacks on the Py-Family of Ciphers and an Approach to Repair the Weaknesses. , 2007, , 58-72.		10
190	nPAKEâ€‰+â€‰: A Hierarchical Group Password-Authenticated Key Exchange Protocol Using Different Passwords. Lecture Notes in Computer Science, 2007, , 31-43.	1.0	10
191	Optimistic Fair Priced Oblivious Transfer. Lecture Notes in Computer Science, 2010, , 131-147.	1.0	10
192	Higher Order Universal One-Way Hash Functions. Lecture Notes in Computer Science, 2004, , 201-213.	1.0	9
193	Hardware implementation of an elliptic curve processor over GF(p) with Montgomery modular multiplier. International Journal of Embedded Systems, 2008, 3, 229.	0.2	9
194	Algebraic Techniques in Differential Cryptanalysis Revisited. Lecture Notes in Computer Science, 2011, , 120-141.	1.0	9
195	Practical privacy-preserving location-sharing based services with aggregate statistics. , 2014, , .		9
196	Survey of Security Aspect of V2X Standards and Related Issues. , 2019, , .		9
197	Exploring the storj network. , 2021, , .		9
198	A Privacy-Preserving Remote Healthcare System Offering End-to-End Security. Lecture Notes in Computer Science, 2016, , 237-250.	1.0	9

#	Article	IF	Citations
199	Multi-party Computation from Any Linear Secret Sharing Scheme Unconditionally Secure against Adaptive Adversary: The Zero-Error Case. Lecture Notes in Computer Science, 2003, , 1-15.	1.0	9
200	From Image Hashing to Video Hashing. Lecture Notes in Computer Science, 2010, , 662-668.	1.0	9
201	Anonymous Split E-Cashâ€"Toward Mobile Anonymous Payments. Transactions on Embedded Computing Systems, 2015, 14, 1-25.	2.1	9
202	Cryptanalysis of the Two-Dimensional Circulation Encryption Algorithm. Eurasip Journal on Advances in Signal Processing, 2005, 2005, 1.	1.0	8
203	Recent attacks on alleged SecurID and their practical implications. Computers and Security, 2005, 24, 364-370.	4.0	8
204	A Survey on Multimodal Biometrics and the Protection of Their Templates. IFIP Advances in Information and Communication Technology, 2015, , 169-184.	0.5	8
205	Private Mobile Pay-TV From Priced Oblivious Transfer. IEEE Transactions on Information Forensics and Security, 2018, 13, 280-291.	4.5	8
206	Producing Collisions for PANAMA. Lecture Notes in Computer Science, 2002, , 37-51.	1.0	8
207	Optimal Forgeries Against Polynomial-Based MACs and GCM. Lecture Notes in Computer Science, 2018, , 445-467.	1.0	8
208	A Concrete Security Analysis for 3GPP-MAC. Lecture Notes in Computer Science, 2003, , 154-169.	1.0	8
209	Accountable Anonymous Communication. , 2007, , 239-253.		8
210	Cryptographic Hash Functions: Theory and Practice. Lecture Notes in Computer Science, 2010, , 115-117.	1.0	8
211	Security Properties of Domain Extenders for Cryptographic Hash Functions. Journal of Information Processing Systems, 2010, 6, 453-480.	1.0	8
212	Cryptanalysis of the Alleged SecurID Hash Function. Lecture Notes in Computer Science, 2004, , 130-144.	1.0	8
213	A new inequality in discrete fourier theory. IEEE Transactions on Information Theory, 2003, 49, 2038-2040.	1.5	7
214	A Side-channel Attack Resistant Programmable PKC Coprocessor for Embedded Applications. , 2007, , .		7
215	Shape-based features for image hashing. , 2009, , .		7
216	Censorship-resistant and privacy-preserving distributed web search. , 2014, , .		7

#	Article	IF	Citations
217	Improved Interpolation Attacks on Cryptographic Primitives of Low Algebraic Degree. Lecture Notes in Computer Science, 2020, , 171-193.	1.0	7
218	Non-randomness of the Full 4 and 5-Pass HAVAL. Lecture Notes in Computer Science, 2005, , 324-336.	1.0	7
219	Improving secure long-term archival of digitally signed documents. , 2008, , .		7
220	On the Security of Encryption Modes of MD4, MD5 and HAVAL. Lecture Notes in Computer Science, 2005, , 147-158.	1.0	7
221	Cryptanalysis of a fast cryptographic checksum algorithm. Computers and Security, 1990, 9, 257-262.	4.0	6
222	Combining World Wide Web and Wireless Security. IFIP Advances in Information and Communication Technology, 2002, , 153-171.	0.5	6
223	Classification of cubic (n-4)-resilient Boolean functions. IEEE Transactions on Information Theory, 2006, 52, 1670-1676.	1.5	6
224	Identity in federated electronic healthcare. , 2008, , .		6
225	Attacks on Two Buyer-Seller Watermarking Protocols and an Improvement for Revocable Anonymity. , 2008, , .		6
226	Cryptography for Network Security: Failures, Successes and Challenges. Lecture Notes in Computer Science, 2010, , 36-54.	1.0	6
227	On Distributed Key Distribution Centers and Unconditionally Secure Proactive Verifiable Secret Sharing Schemes Based on General Access Structure. Lecture Notes in Computer Science, 2002, , 422-435.	1.0	6
228	Collateral Damage of Facebook Apps: Friends, Providers, and Privacy Interdependence. IFIP Advances in Information and Communication Technology, 2016, , 194-208.	0.5	6
229	Robust Image Content Authentication Using Perceptual Hashing and Watermarking. Lecture Notes in Computer Science, 2012, , 315-326.	1.0	6
230	On the Influence of Message Length in PMACâ€™s Security Bounds. Lecture Notes in Computer Science, 2016, , 596-621.	1.0	6
231	A Tangled World Wide Web of Security Issues. First Monday, 2002, 7, .	0.6	6
232	Privacy-preserving Biometric Authentication Model for e-Finance Applications. , 2018, , .		6
233	Increased Resilience in Threshold Cryptography: Sharing a Secret with Devices That Cannot Store Shares. Lecture Notes in Computer Science, 2010, , 116-135.	1.0	6
234	Equivalent Keys of HPC. Lecture Notes in Computer Science, 1999, , 29-42.	1.0	5

#	Article	IF	Citations
235	On Multiplicative Linear Secret Sharing Schemes. Lecture Notes in Computer Science, 2003, , 135-147.	1.0	5
236	Insights on identity documents based on the Belgian case study. Information Security Technical Report, 2008, 13, 54-60.	1.3	5
237	Reliable Key Establishment Scheme Exploiting Unidirectional Links in Wireless Sensor Networks. , 2008, , .		5
238	Finding Collisions for a 45-Step Simplified HAS-V. Lecture Notes in Computer Science, 2009, , 206-225.	1.0	5
239	Practical Collisions for EnRUPT. Journal of Cryptology, 2011, 24, 1-23.	2.1	5
240	VirtualFriendship: Hiding interactions on Online Social Networks. , 2014, , .		5
241	On the choice of the appropriate AES data encryption method for ZigBee nodes. Security and Communication Networks, 2016, 9, 87-93.	1.0	5
242	High Assurance Smart Metering. , 2016, , .		5
243	De-pseudonymization of Smart Metering Data: Analysis and Countermeasures. , 2018, , .		5
244	On the Difficulty of Using Patient's Physiological Signals in Cryptographic Protocols. , 2019, , .		5
245	Problems and solutions from the fourth International Studentsâ€™ Olympiad in Cryptography (NSUCRYPTO). Cryptologia, 2019, 43, 138-174.	0.4	5
246	A Chosen Text Attack on The Modified Cryptographic Checksum Algorithm of Cohen and Huang. , 1989, , 154-163.		5
247	Cryptanalysis of Reduced Variants of the FORK-256 Hash Function. Lecture Notes in Computer Science, 2006, , 85-100.	1.0	5
248	An Efficient Entity Authentication Protocol with Enhanced Security and Privacy Properties. Lecture Notes in Computer Science, 2016, , 335-349.	1.0	5
249	MQ Signatures for PKI. Lecture Notes in Computer Science, 2017, , 224-240.	1.0	5
250	Collisions for RC4-Hash. Lecture Notes in Computer Science, 2008, , 355-366.	1.0	5
251	Improved Collision Attacks on the Reduced-Round GrÃ¸stl Hash Function. Lecture Notes in Computer Science, 2011, , 1-16.	1.0	5
252	Security Analysis and Comparison of the SHA-3 Finalists BLAKE, GrÃ¸stl, JH, Keccak, and Skein. Lecture Notes in Computer Science, 2012, , 287-305.	1.0	5

#	Article	IF	Citations
253	Threshold things that think. , 2009, , .		5
254	Authenticated and auditable data sharing via smart contract. , 2020, , .		5
255	New Weaknesses in the Keystream Generation Algorithms of the Stream Ciphers TPy and Py. Lecture Notes in Computer Science, 2007, , 249-262.	1.0	5
256	Preimages for Reduced-Round Tiger. Lecture Notes in Computer Science, 2007, , 90-99.	1.0	5
257	CNN Algorithms for Video Authentication and Copyright Protection. Journal of Signal Processing Systems, 1999, 23, 449-463.	1.0	4
258	On Secure Image Hashing by Higher-Order Statistics. , 2007, , .		4
259	HW/SW co-design for public-key cryptosystems on the 8051 micro-controller. Computers and Electrical Engineering, 2007, 33, 324-332.	3.0	4
260	An embedded platform for privacy-friendly road charging applications. , 2010, , .		4
261	Security implications in Kerberos by the introduction of smart cards. , 2012, , .		4
262	UNAF: A Special Set of Additive Differences with Application to the Differential Analysis of ARX. Lecture Notes in Computer Science, 2012, , 287-305.	1.0	4
263	Interface Design for Mapping a Variety of RSA Exponentiation Algorithms on a HW/SW Co-design Platform. , 2012, , .		4
264	A linux kernel cryptographic framework. , 2012, , .		4
265	Cryptography and Information Security in the Post-Snowden Era. , 2015, , .		4
266	STBC: Side Channel Attack Tolerant Balanced Circuit with Reduced Propagation Delay. , 2017, , .		4
267	The Fifth International Studentsâ€™ Olympiad in cryptographyâ€"NSUCRYPTO: Problems and their solutions. Cryptologia, 2020, 44, 223-256.	0.4	4
268	Off-chain state channels in the energy domain. , 2021, , .		4
269	On Self-equivalence Encodings inÂWhite-Box Implementations. Lecture Notes in Computer Science, 2021, , 639-669.	1.0	4
270	HERMES: Scalable, Secure, and Privacy-Enhancing Vehicular Sharing-Access System. IEEE Internet of Things Journal, 2022, 9, 129-151.	5.5	4

#	Article	IF	Citations
271	Public-Key Cryptography for RFID Tags and Applications. , 2008, , 317-348.		4
272	Forgery and Subkey Recovery on CAESAR Candidate iFeed. Lecture Notes in Computer Science, 2016, , 197-204.	1.0	4
273	AES Data Encryption in a ZigBee Network: Software or Hardware?. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 163-173.	0.2	4
274	Radon Transform-Based Secure Image Hashing. Lecture Notes in Computer Science, 2011, , 186-193.	1.0	4
275	Collateral Damage of Online Social Network Applications. , 2016, , .		4
276	Extending the Selective MPEG Encryption Algorithm PVEA. , 2006, , .		3
277	Empirical comparison of side channel analysis distinguishers on DES in hardware. , 2009, , .		3
278	Guest Editorial Special Issue on Electronic Voting. IEEE Transactions on Information Forensics and Security, 2009, 4, 593-596.	4.5	3
279	The State of Hash Functions and the NIST SHA-3 Competition. Lecture Notes in Computer Science, 2009, , 1-11.	1.0	3
280	Case Study : A class E power amplifier for ISO-14443A. , 2009, , .		3
281	Algebraic cryptanalysis of a small-scale version of stream cipher Lex. IET Information Security, 2010, 4, 49.	1.1	3
282	New (Two-Track-)MAC Based on the Two Trails of RIPEMD. Lecture Notes in Computer Science, 2001, , 314-324.	1.0	3
283	Traffic Analysis Attacks on a Continuously-Observable Steganographic File System. Lecture Notes in Computer Science, 2007, , 220-236.	1.0	3
284	On the Impact of Known-Key Attacks on Hash Functions. Lecture Notes in Computer Science, 2015, , 59-84.	1.0	3
285	Improved Pairing Protocol for Bluetooth. Lecture Notes in Computer Science, 2006, , 252-265.	1.0	3
286	Improved Distinguishing Attacks on HC-256. Lecture Notes in Computer Science, 2009, , 38-52.	1.0	3
287	Cryptanalysis of Dynamic SHA(2). Lecture Notes in Computer Science, 2009, , 415-432.	1.0	3
288	Information authentication: Hash functions and digital signatures. Lecture Notes in Computer Science, 1993, , 87-131.	1.0	3

#	Article	IF	Citations
289	Block-Anti-Circulant Unbalanced Oil and Vinegar. Lecture Notes in Computer Science, 2020, , 574-588.	1.0	3
290	Categorization of Faulty Nonce Misuse Resistant Message Authentication. Lecture Notes in Computer Science, 2021, , 520-550.	1.0	3
291	MACs and hash functions: State of the art. Information Security Technical Report, 1997, 2, 33-43.	1.3	2
292	Spectral characterization of cryptographic Boolean functions satisfying the (extended) propagation criterion of degree l and order k. Information Processing Letters, 2005, 93, 25-28.	0.4	2
293	nPAKE+: A Tree-Based Group Password-Authenticated Key Exchange Protocol Using Different Passwords. Journal of Computer Science and Technology, 2009, 24, 138-151.	0.9	2
294	A novel video hash algorithm. , 2010, , .		2
295	On security arguments of the second round SHA-3 candidates. International Journal of Information Security, 2012, 11, 103-120.	2.3	2
296	Toward a secure Kerberos key exchange with smart cards. International Journal of Information Security, 2014, 13, 217-228.	2.3	2
297	Provoking security: Spoofing attacks against crypto-biometric systems. , 2015, , .		2
298	Post-Snowden Threat Models. , 2015, , .		2
299	Efficient parallelizable hashing using small non-compressing primitives. International Journal of Information Security, 2016, 15, 285-300.	2.3	2
300	SCM. , 2017, , .		2
301	A Privacy-Preserving Device Tracking System Using a Low-Power Wide-Area Network. Lecture Notes in Computer Science, 2018, , 347-369.	1.0	2
302	On a Resynchronization Weakness in a Class of Combiners with Memory. Lecture Notes in Computer Science, 2003, , 164-173.	1.0	2
303	Hash Functions. , 2011, , 543-553.		2
304	The NIST SHA-3 Competition: A Perspective on the Final Year. Lecture Notes in Computer Science, 2011, , 383-386.	1.0	2
305	Electronic Voting in Belgium: Past and Future. Lecture Notes in Computer Science, 2007, , 76-87.	1.0	2
306	A Framework for the Analysis of Mix-Based Steganographic File Systems. Lecture Notes in Computer Science, 2008, , 428-445.	1.0	2

#	Article	IF	Citations
307	A Modular Test Platform for Evaluation of Security Protocols in NFC Applications. Lecture Notes in Computer Science, 2011, , 171-177.	1.0	2
308	Image Distortion Estimation by Hash Comparison. Lecture Notes in Computer Science, 2011, , 62-72.	1.0	2
309	MAA. , 2011, , 741-742.		2
310	Flexible Design of a Modular Simultaneous Exponentiation Core for Embedded Platforms. Lecture Notes in Computer Science, 2013, , 115-121.	1.0	2
311	An Introduction to Cryptology. Lecture Notes in Computer Science, 1998, , 204-221.	1.0	2
312	A Collaborative Cybersecurity Education Program. Advances in Information Security, Privacy, and Ethics Book Series, 2019, , 181-200.	0.4	2
313	A White-Box Speck Implementation Using Self-equivalence Encodings. Lecture Notes in Computer Science, 2022, , 771-791.	1.0	2
314	State-of-the-art ciphers for commercial applications. Computers and Security, 1999, 18, 67-74.	4.0	1
315	Security Model for a Shared Multimedia Archive. , 2007, , .		1
316	An introduction to modern cryptology. , 2007, , 565-592.		1
317	Delegation and digital mandates: Legal requirements and security objectives. Computer Law and Security Review, 2009, 25, 415-431.	1.3	1
318	Point/Counterpoint. IEEE Software, 2011, 28, 56-59.	2.1	1
319	Disparity guided exhibition watermarking for 3D stereo images. , 2011, , .		1
320	Evaluating Tag-Based Preference Obfuscation Systems. IEEE Transactions on Knowledge and Data Engineering, 2012, 24, 1613-1623.	4.0	1
321	Two-permutation-based hashing with binary mixing. Journal of Mathematical Cryptology, 2015, 9, .	0.4	1
322	Binary decision diagram to design balanced secure logic styles. , 2016, , .		1
323	Editorial: Special issue on recent trends in cryptography. Cryptography and Communications, 2018, 10, 1-3.	0.9	1
324	Reply to Lucas &amp; Henneberg: Are human faces unique?. Forensic Science International, 2019, 297, 217-220.	1.3	1

#	Article	IF	Citations
325	Modes of Operation of a Block Cipher. , 2011, , 789-794.		1
326	Public Key Compression for Constrained Linear Signature Schemes. Lecture Notes in Computer Science, 2019, , 300-321.	1.0	1
327	A Privacy-Preserving Model for Biometric Fusion. Lecture Notes in Computer Science, 2016, , 743-748.	1.0	1
328	Trends in Cryptology Research. , 2004, , 51-58.		1
329	A New Approach to Ï‡ 2 Cryptanalysis of Block Ciphers. Lecture Notes in Computer Science, 2009, , 1-16.	1.0	1
330	Practical Collisions for SHAMATA-256. Lecture Notes in Computer Science, 2009, , 1-15.	1.0	1
331	Practical Attacks on a Cryptosystem Proposed in Patent WO/2009/066313. Lecture Notes in Computer Science, 2012, , 1-12.	1.0	1
332	Threshold-Based Location-Aware Access Control. , 2013, , 20-36.		1
333	Pseudorandomness of Basic Structures in the Block Cipher KASUMI. ETRI Journal, 2003, 25, 89-100.	1.2	1
334	Normality of Vectorial Functions. Lecture Notes in Computer Science, 2005, , 186-200.	1.0	1
335	Second Preimage Resistance. , 2011, , 1093-1093.		1
336	Threshold-Based Location-Aware Access Control. International Journal of Handheld Computing Research, 2011, 2, 22-37.	0.4	1
337	Towards Quantum Distance Bounding Protocols. Lecture Notes in Computer Science, 2017, , 151-162.	1.0	1
338	Short Solutions to Nonlinear Systems of Equations. Lecture Notes in Computer Science, 2018, , 71-90.	1.0	1
339	A Randomised Algorithm for Checking The Normality of Cryptographic Boolean Functions. , 2004, , 51-66.		0
340	E03: A new systolic architecture for multiplication in GF(2n). IFAC Postprint Volumes IPPV / International Federation of Automatic Control, 2004, 37, 461-466.	0.4	0
341	Side-channel resistant system-level design flow for public-key cryptography. , 2007, , .		0
342	Galois geometries and applications. Designs, Codes, and Cryptography, 2010, 56, 85-86.	1.0	0

#	Article	IF	Citations
343	Cryptanalysis of the ESSENCE Family of Hash Functions. Lecture Notes in Computer Science, 2010, , 15-34.	1.0	0
344	Challenging the increased resistance of regular hash functions against birthday attacks. Journal of Mathematical Cryptology, 2012, 6, .	0.4	0
345	Message from ACS Workshop Chairs. , 2012, , .		0
346	It's Not My Fault - On Fault Attacks on Symmetric Cryptography. , 2012, , .		0
347	Advanced theory and practice for cryptography and future security. Mathematical and Computer Modelling, 2012, 55, 1-2.	2.0	0
348	The SHA-3 competition. , 2013, , .		0
349	Attacking a problem from the middle. Communications of the ACM, 2014, 57, 97-97.	3.3	0
350	Internal differential collision attacks on the reduced-round GrÃ¸stl-0 hash function. Designs, Codes, and Cryptography, 2014, 70, 251-271.	1.0	0
351	Software Security: Squaring the Circle?. , 2015, , .		0
352	Are You Really My Friend? Efficient and Secure Friend-Matching in Mobile Social Networks. , 2017, , .		0
353	Robust Metering Schemes for General Access Structures. Lecture Notes in Computer Science, 2004, , 53-65.	1.0	0
354	A Weakness in Some Oblivious Transfer and Zero-Knowledge Protocols. Lecture Notes in Computer Science, 2006, , 348-363.	1.0	0
355	The Future of Cryptographic Algorithms. Lecture Notes in Computer Science, 2009, , 1-2.	1.0	0
356	Collision Attack. , 2011, , 220-221.		0
357	MAC Algorithms. , 2011, , 742-748.		0
358	Preimage Resistance. , 2011, , 952-953.		0
359	Collision Resistance. , 2011, , 221-222.		0
360	HMAC. , 2011, , 559-560.		0

#	Article	IF	Citations
361	A Privacy-Preserving ID-Based Group Key Agreement Scheme Applied in VPAN. Lecture Notes in Computer Science, 2011, , 214-225.	1.0	0
362	Finding Collisions for Reduced Luffa-256Âv2 (Poster). Lecture Notes in Computer Science, 2011, , 423-427.	1.0	0
363	GMAC. , 2011, , 513-514.		0
364	NESSIE Project. , 2011, , 831-836.		0
365	DES Collisions Revisited. Lecture Notes in Computer Science, 2012, , 13-24.	1.0	0
366	Dedicated Hardware for Attribute-Based Credential Verification. Lecture Notes in Computer Science, 2013, , 50-65.	1.0	0
367	Mathematicians Discuss the Snowden Revelations. Notices of the American Mathematical Society, 2015, 62, 400-403.	0.1	0
368	A Bimodal Verification Cryptosystem as a Framework against Spoofing Attacks. International Journal of Intelligent Computing Research, 2015, 6, 540-549.	0.5	0
369	Verification Schemes of Multi-SIM Devices in Mobile Communication Systems. , 2020, , .		0
370	Big Data against Corona: Mass Surveillance or Privacy by Design? Keynote. , 2020, , .		0