Bart Preneel

List of Publications by Year in Descending Order

359 papers	6,271 citations	39 h-index	61 g-index
394 ext. papers	7,090 ext. citations	1.4 avg, IF	5.99 L-index

#	Paper	IF	Citations
359	A New Privacy Enhancing Beacon Scheme in V2X Communication. *Lecture Notes in Computer Science*, **2022**, 139-151	0.9	
358	A White-Box Speck Implementation Using Self-equivalence Encodings. *Lecture Notes in Computer Science*, **2022**, 771-791	0.9	1
357	Categorization of Faulty Nonce Misuse Resistant Message Authentication. *Lecture Notes in Computer Science*, **2021**, 520-550	0.9	1
356	Exploring the storj network **2021**,		3
355	Off-chain state channels in the energy domain **2021**,		2
354	Toward a Common Performance and Effectiveness Terminology for Digital Proximity Tracing Applications. *Frontiers in Digital Health*, **2021**, 3, 677929	2.3	4
353	On Self-equivalence Encodings in White-Box Implementations. *Lecture Notes in Computer Science*, **2021**, 639-669	0.9	2
352	Authenticated and auditable data sharing via smart contract **2020**,		2
351	Block-Anti-Circulant Unbalanced Oil and Vinegar. *Lecture Notes in Computer Science*, **2020**, 574-588	0.9	2
350	Improved Interpolation Attacks on Cryptographic Primitives of Low Algebraic Degree. *Lecture Notes in Computer Science*, **2020**, 171-193	0.9	4
349	The Fifth International Students Olympiad in cryptography NSUCRYPTO: Problems and their solutions. *Cryptologia*, **2020**, 44, 223-256	0.9	2
348	On the Difficulty of Using Patient's Physiological Signals in Cryptographic Protocols **2019**,		1
347	Reply to Lucas & Henneberg: Are human faces unique?. *Forensic Science International*, **2019**, 297, 217-220	2.6	
346	Problems and solutions from the fourth International Students Olympiad in Cryptography (NSUCRYPTO). *Cryptologia*, **2019**, 43, 138-174	0.9	2
345	**2019**,		18
344	SC2Share: Smart Contract for Secure Car Sharing **2019**,		4
343	A Collaborative Cybersecurity Education Program. *Advances in Information Security, Privacy, and Ethics Book Series*, **2019**, 181-200	0.3	2

342	Public Key Compression for Constrained Linear Signature Schemes. *Lecture Notes in Computer Science*, **2019**, 300-321	0.9	1
341	Survey of Security Aspect of V2X Standards and Related Issues **2019**,		4
340	Collateral damage of Facebook third-party applications: a comprehensive study. *Computers and Security*, **2018**, 77, 179-208	4.9	16
339	Private Mobile Pay-TV From Priced Oblivious Transfer. *IEEE Transactions on Information Forensics and Security*, **2018**, 13, 280-291	8	5
338	Privacy-preserving Biometric Authentication Model for e-Finance Applications **2018**,		4
337	Short Solutions to Nonlinear Systems of Equations. *Lecture Notes in Computer Science*, **2018**, 71-90	0.9	1
336	Optimal Forgeries Against Polynomial-Based MACs and GCM. *Lecture Notes in Computer Science*, **2018**, 445-467	0.9	7
335	Securing Wireless Neurostimulators **2018**,		9
334	A Privacy-Preserving Device Tracking System Using a Low-Power Wide-Area Network. *Lecture Notes in Computer Science*, **2018**, 347-369	0.9	1
333	De-pseudonymization of Smart Metering Data: Analysis and Countermeasures **2018**,		3
332	Publish or Perish: A Backward-Compatible Defense Against Selfish Mining in Bitcoin. *Lecture Notes in Computer Science*, **2017**, 277-292	0.9	39
331	SOFIA: Software and control flow integrity architecture. *Computers and Security*, **2017**, 68, 16-35	4.9	15
330	SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision. *Lecture Notes in Computer Science*, **2017**, 475-493	0.9	10
329	Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning **2017**,		41
328	Sancus 2.0. *ACM Transactions on Privacy and Security*, **2017**, 20, 1-33	2.9	25
327	STBC: Side Channel Attack Tolerant Balanced Circuit with Reduced Propagation Delay **2017**,		3
326	On the Necessity of a Prescribed Block Validity Consensus **2017**,		10
325	MQ Signatures for PKI. *Lecture Notes in Computer Science*, **2017**, 224-240	0.9	3

324	Field Lifting for Smaller UOV Public Keys. *Lecture Notes in Computer Science*, **2017**, 227-246	0.9	19
323	Towards Quantum Distance Bounding Protocols. *Lecture Notes in Computer Science*, **2017**, 151-162	0.9	1
322	Practical identity-based private sharing for online social networks. *Computer Communications*, **2016**, 73, 243-250	5.1	7
321	Efficient parallelizable hashing using small non-compressing primitives. *International Journal of Information Security*, **2016**, 15, 285-300	2.8	2
320	On the choice of the appropriate AES data encryption method for ZigBee nodes. *Security and Communication Networks*, **2016**, 9, 87-93	1.9	3
319	High Assurance Smart Metering **2016**,		5
318	Extension Field Cancellation: A New Central Trapdoor for Multivariate Quadratic Systems. *Lecture Notes in Computer Science*, **2016**, 182-196	0.9	22
317	SOFIA: Software and control flow integrity architecture **2016**,		15
316	Collateral Damage of Online Social Network Applications **2016**,		3
315	Forgery and Subkey Recovery on CAESAR Candidate iFeed. *Lecture Notes in Computer Science*, **2016**, 197-204		4
314	Collateral Damage of Facebook Apps: Friends, Providers, and Privacy Interdependence. *IFIP Advances in Information and Communication Technology*, **2016**, 194-208	0.5	4
313	A Privacy-Preserving Remote Healthcare System Offering End-to-End Security. *Lecture Notes in Computer Science*, **2016**, 237-250	0.9	6
312	An Efficient Entity Authentication Protocol with Enhanced Security and Privacy Properties. *Lecture Notes in Computer Science*, **2016**, 335-349	0.9	4
311	A Privacy-Preserving Model for Biometric Fusion. *Lecture Notes in Computer Science*, **2016**, 743-748	0.9	1
310	On the Influence of Message Length in PMAC□s Security Bounds. *Lecture Notes in Computer Science*, **2016**, 596-621	0.9	6
309	On the Feasibility of Cryptography for a Wireless Insulin Pump System **2016**,		20
308	On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them **2016**,		26
307	An Implementation of a High Assurance Smart Meter Using Protected Module Architectures. *Lecture Notes in Computer Science*, **2016**, 53-69	0.9	6

306	Keyless car sharing system: A security and privacy analysis **2016**,		7
305	A MAC Mode for Lightweight Block Ciphers. *Lecture Notes in Computer Science*, **2016**, 43-59	0.9	26
304	Two-permutation-based hashing with binary mixing. *Journal of Mathematical Cryptology*, **2015**, 9,	0.6	1
303	A Survey on Multimodal Biometrics and the Protection of Their Templates. *IFIP Advances in Information and Communication Technology*, **2015**, 169-184	0.5	6
302	Open problems in hash function security. *Designs, Codes, and Cryptography*, **2015**, 77, 611-631	1.2	17
301	Cryptography and Information Security in the Post-Snowden Era **2015**,		3
300	Anonymous Split E-Cash□oward Mobile Anonymous Payments. *Transactions on Embedded Computing Systems*, **2015**, 14, 1-25	1.8	7
299	On the XOR of Multiple Random Permutations. *Lecture Notes in Computer Science*, **2015**, 619-634	0.9	19
298	On the Impact of Known-Key Attacks on Hash Functions. *Lecture Notes in Computer Science*, **2015**, 59-84	0.9	3
297	Internal differential collision attacks on the reduced-round Gr□tl-0 hash function. *Designs, Codes, and Cryptography*, **2014**, 70, 251-271	1.2	
296	Toward a secure Kerberos key exchange with smart cards. *International Journal of Information Security*, **2014**, 13, 217-228	2.8	2
295	Censorship-resistant and privacy-preserving distributed web search **2014**,		5
294	Attacking a problem from the middle. *Communications of the ACM*, **2014**, 57, 97-97	2.5	
293	Practical privacy-preserving location-sharing based services with aggregate statistics **2014**,		4
292	VirtualFriendship: Hiding interactions on Online Social Networks **2014**,		5
291	Proper RFID Privacy: Model and Protocols. *IEEE Transactions on Mobile Computing*, **2014**, 13, 2888-2902	4.6	28
290	Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. *Lecture Notes in Computer Science*, **2014**, 306-323	0.9	76
289	AEGIS: A Fast Authenticated Encryption Algorithm. *Lecture Notes in Computer Science*, **2014**, 185-201	0.9	33

288	Two Attacks on a White-Box AES Implementation. *Lecture Notes in Computer Science*, **2014**, 265-285	0.9	43
287	Cryptanalysis of the Xiao Lai White-Box AES Implementation. *Lecture Notes in Computer Science*, **2013**, 34-49	0.9	42
286	End-To-End Security for Video Distribution: The Combination of Encryption, Watermarking, and Video Adaptation. *IEEE Signal Processing Magazine*, **2013**, 30, 97-107	9.4	36
285	Optimal sporadic location privacy preserving systems in presence of bandwidth constraints **2013**,		9
284	FPDetective **2013**,		136
283	Format-compliant encryption techniques for high efficiency video coding **2013**,		10
282	Friend in the Middle (FiM): Tackling de-anonymization in social networks **2013**,		10
281	For some eyes only **2013**,		14
280	Threshold-Based Location-Aware Access Control **2013**, 20-36		1
279	Protected Software Module Architectures **2013**, 241-251		12
278	Dedicated Hardware for Attribute-Based Credential Verification. *Lecture Notes in Computer Science*, **2013**, 50-65	0.9	
277	Flexible Design of a Modular Simultaneous Exponentiation Core for Embedded Platforms. *Lecture Notes in Computer Science*, **2013**, 115-121	0.9	1
276	Related-Key Boomerang and Rectangle Attacks: Theory and Experimental Analysis. *IEEE Transactions on Information Theory*, **2012**, 58, 4948-4966	2.8	18
275	A Practical Attack on KeeLoq. *Journal of Cryptology*, **2012**, 25, 136-157	2.1	9
274	Toward More Secure and Reliable Access Control. *IEEE Pervasive Computing*, **2012**, 11, 76-83	1.3	8
273	Robust Image Content Authentication with Tamper Location **2012**,		9
272	Evaluating Tag-Based Preference Obfuscation Systems. *IEEE Transactions on Knowledge and Data Engineering*, **2012**, 24, 1613-1623	4.2	1
271	Hash Functions Based on Three Permutations: A Generic Security Analysis. *Lecture Notes in Computer Science*, **2012**, 330-347	0.9	12

270	UNAF: A Special Set of Additive Differences with Application to the Differential Analysis of ARX. *Lecture Notes in Computer Science*, **2012**, 287-305	0.9	4
269	Interface Design for Mapping a Variety of RSA Exponentiation Algorithms on a HW/SW Co-design Platform **2012**,		4
268	Impossible Differential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT. *Lecture Notes in Computer Science*, **2012**, 117-137	0.9	30
267	A linux kernel cryptographic framework **2012**,		2
266	Criteria towards metrics for benchmarking template protection algorithms **2012**,		33
265	On security arguments of the second round SHA-3 candidates. *International Journal of Information Security*, **2012**, 11, 103-120	2.8	1
264	The parazoa family: generalizing the sponge hash functions. *International Journal of Information Security*, **2012**, 11, 149-165	2.8	11
263	A cross-protocol attack on the TLS protocol **2012**,		40
262	Security implications in Kerberos by the introduction of smart cards **2012**,		3
261	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	0.4	12
260	Practical Attacks on a Cryptosystem Proposed in Patent WO/2009/066313. *Lecture Notes in Computer Science*, **2012**, 1-12	0.9	1
259	Security Analysis and Comparison of the SHA-3 Finalists BLAKE, Gr□tl, JH, Keccak, and Skein. *Lecture Notes in Computer Science*, **2012**, 287-305	0.9	3
258	Soft Decision Error Correction for Compact Memory-Based PUFs Using a Single Enrollment. *Lecture Notes in Computer Science*, **2012**, 268-282	0.9	26
257	A Model for Structure Attacks, with Applications to PRESENT and Serpent. *Lecture Notes in Computer Science*, **2012**, 49-68	0.9	15
256	Robust Image Content Authentication Using Perceptual Hashing and Watermarking. *Lecture Notes in Computer Science*, **2012**, 315-326	0.9	6
255	DES Collisions Revisited. *Lecture Notes in Computer Science*, **2012**, 13-24	0.9	
254	. *IEEE Software*, **2011**, 28, 56-59	1.5	1
253	The Differential Analysis of S-Functions. *Lecture Notes in Computer Science*, **2011**, 36-56	0.9	17

252	Algebraic Techniques in Differential Cryptanalysis Revisited. *Lecture Notes in Computer Science*, **2011**, 120-141	0.9	7
251	Meet-in-the-Middle Attacks on Reduced-Round XTEA. *Lecture Notes in Computer Science*, **2011**, 250-267	0.9	18
250	A Privacy-Preserving Buyer–Seller Watermarking Protocol Based on Priced Oblivious Transfer. *IEEE Transactions on Information Forensics and Security*, **2011**, 6, 202-212	8	26
249	A taxonomy of self-modifying code for obfuscation. *Computers and Security*, **2011**, 30, 679-691	4.9	25
248	A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, **2011**, 16, 3-32	2.7	241
247	Practical Collisions for EnRUPT. *Journal of Cryptology*, **2011**, 24, 1-23	2.1	4
246	PriPAYD: Privacy-Friendly Pay-As-You-Drive Insurance. *IEEE Transactions on Dependable and Secure Computing*, **2011**, 8, 742-755	3.9	59
245	A Secure Perceptual Hash Algorithm for Image Content Authentication. *Lecture Notes in Computer Science*, **2011**, 108-121	0.9	12
244	Tripartite modular multiplication. *The Integration VLSI Journal*, **2011**, 44, 259-269	1.4	13
243	Equivalent keys in Multivariate uadratic public key systems. *Journal of Mathematical Cryptology*, **2011**, 4,	0.6	15
242	A New RFID Privacy Model. *Lecture Notes in Computer Science*, **2011**, 568-587	0.9	51
241	Improved Collision Attacks on the Reduced-Round Grøstl Hash Function. *Lecture Notes in Computer Science*, **2011**, 1-16	0.9	4
240	Security Reductions of the Second Round SHA-3 Candidates. *Lecture Notes in Computer Science*, **2011**, 39-53	0.9	18
239	The Additive Differential Probability of ARX. *Lecture Notes in Computer Science*, **2011**, 342-358	0.9	5
238	The NIST SHA-3 Competition: A Perspective on the Final Year. *Lecture Notes in Computer Science*, **2011**, 383-386	0.9	1
237	A Lightweight 256-Bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW. *Lecture Notes in Computer Science*, **2011**, 151-168	0.9	17
236	Radon Transform-Based Secure Image Hashing. *Lecture Notes in Computer Science*, **2011**, 186-193	0.9	2
235	A Privacy-Preserving ID-Based Group Key Agreement Scheme Applied in VPAN. *Lecture Notes in Computer Science*, **2011**, 214-225	0.9	

234	Finding Collisions for Reduced Luffa-256 v2 (Poster). *Lecture Notes in Computer Science*, **2011**, 423-427	0.9	
233	A Modular Test Platform for Evaluation of Security Protocols in NFC Applications. *Lecture Notes in Computer Science*, **2011**, 171-177	0.9	2
232	Image Distortion Estimation by Hash Comparison. *Lecture Notes in Computer Science*, **2011**, 62-72	0.9	1
231	MAA **2011**, 741-742		2
230	Threshold-Based Location-Aware Access Control. *International Journal of Handheld Computing Research*, **2011**, 2, 22-37		1
229	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	34
228	An embedded platform for privacy-friendly road charging applications **2010**,		3
227	Cryptanalysis of the ESSENCE Family of Hash Functions. *Lecture Notes in Computer Science*, **2010**, 15-34	0.9	
226	A novel video hash algorithm **2010**,		2
225	Speed Records for NTRU. *Lecture Notes in Computer Science*, **2010**, 73-88	0.9	27
224	A general model for hiding control flow **2010**,		15
223	The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition. *Lecture Notes in Computer Science*, **2010**, 1-14	0.9	22
222	Cryptography for Network Security: Failures, Successes and Challenges. *Lecture Notes in Computer Science*, **2010**, 36-54	0.9	4
221	State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures **2010**,		77
220	Reversing protected minutiae vicinities **2010**,		9
219	Galois geometries and applications. *Designs, Codes, and Cryptography*, **2010**, 56, 85-86	1.2	
218	Algebraic cryptanalysis of a small-scale version of stream cipher Lex. *IET Information Security*, **2010**, 4, 49	1.4	2
217	. *IEEE Transactions on Vehicular Technology*, **2010**, 59, 519-532	6.8	17

216	A Provably Secure Anonymous Buyer-Seller Watermarking Protocol. *IEEE Transactions on Information Forensics and Security*, **2010**, 5, 920-931	8	38
215	Security Properties of Domain Extenders for Cryptographic Hash Functions. *Journal of Information Processing Systems*, **2010**, 6, 453-480		7
214	From Image Hashing to Video Hashing. *Lecture Notes in Computer Science*, **2010**, 662-668	0.9	7
213	Revisiting Higher-Order DPA Attacks:. *Lecture Notes in Computer Science*, **2010**, 221-234	0.9	30
212	Parallel Shortest Lattice Vector Enumeration on Graphics Cards. *Lecture Notes in Computer Science*, **2010**, 52-68	0.9	14
211	Optimistic Fair Priced Oblivious Transfer. *Lecture Notes in Computer Science*, **2010**, 131-147	0.9	8
210	Anti-counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware. *Information Security and Cryptography*, **2010**, 237-257	3.6	10
209	On the Indifferentiability of the Grøstl Hash Function. *Lecture Notes in Computer Science*, **2010**, 88-105	0.9	19
208	Cryptanalysis of a Perturbated White-Box AES Implementation. *Lecture Notes in Computer Science*, **2010**, 292-310	0.9	43
207	Cryptographic Hash Functions: Theory and Practice. *Lecture Notes in Computer Science*, **2010**, 115-117	0.9	8
206	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
205	Cryptographic Hash Functions: Theory and Practice. *Lecture Notes in Computer Science*, **2010**, 1-3	0.9	3
204	Increased Resilience in Threshold Cryptography: Sharing a Secret with Devices That Cannot Store Shares. *Lecture Notes in Computer Science*, **2010**, 116-135	0.9	5
203	Shape-based features for image hashing **2009**,		7
202	Empirical comparison of side channel analysis distinguishers on DES in hardware **2009**,		3
201	Towards a cross-context identity management framework in e-health. *Online Information Review*, **2009**, 33, 422-442	2	12
200	Anonymous user communication for privacy protection in wireless metropolitan mesh networks **2009**,		2
199	. *IEEE Transactions on Information Forensics and Security*, **2009**, 4, 593-596	8	3

198	An efficient buyer-seller watermarking protocol based on composite signal representation **2009**,		33
197	nPAKE+: A Tree-Based Group Password-Authenticated Key Exchange Protocol Using Different Passwords. *Journal of Computer Science and Technology*, **2009**, 24, 138-151	1.7	1
196	Collisions and Other Non-random Properties for Step-Reduced SHA-256. *Lecture Notes in Computer Science*, **2009**, 276-293	0.9	22
195	The State of Hash Functions and the NIST SHA-3 Competition. *Lecture Notes in Computer Science*, **2009**, 1-11	0.9	1
194	Finding Collisions for a 45-Step Simplified HAS-V. *Lecture Notes in Computer Science*, **2009**, 206-225	0.9	5
193	Practical DPA attacks on MDPL **2009**,		10
192	Efficient implementation of anonymous credentials on Java Card smart cards **2009**,		25
191	**2009**,		91
190	Case Study : A class E power amplifier for ISO-14443A **2009**,		1
189	ARM: anonymous routing protocol for mobile ad hoc networks. *International Journal of Wireless and Mobile Computing*, **2009**, 3, 145	0.4	31
188	Offline NFC payments with electronic vouchers **2009**,		14
187	Universally Composable Adaptive Priced Oblivious Transfer. *Lecture Notes in Computer Science*, **2009**, 231-247	0.9	35
186	Practical Collisions for EnRUPT. *Lecture Notes in Computer Science*, **2009**, 246-259	0.9	11
185	A Three-Property-Secure Hash Function. *Lecture Notes in Computer Science*, **2009**, 228-244	0.9	9
184	A New Approach to Cryptanalysis of Block Ciphers. *Lecture Notes in Computer Science*, **2009**, 1-16	0.9	1
183	Towards Security Notions for White-Box Cryptography. *Lecture Notes in Computer Science*, **2009**, 49-58	0.9	15
182	Threshold Things That Think: Authorisation for Resharing. *IFIP Advances in Information and Communication Technology*, **2009**, 111-124	0.5	4
181	Practical Collisions for SHAMATA-256. *Lecture Notes in Computer Science*, **2009**, 1-15	0.9	1

180	Improved Distinguishing Attacks on HC-256. *Lecture Notes in Computer Science*, **2009**, 38-52	0.9	2
179	Threshold things that think **2009**,		3
178	Cryptanalysis of Dynamic SHA(2). *Lecture Notes in Computer Science*, **2009**, 415-432	0.9	1
177	Dependence of RFID Reader Antenna Design on Read Out Distance. *IEEE Transactions on Antennas and Propagation*, **2008**, 56, 3829-3837	4.9	25
176	Anonymous ID-Based Group Key Agreement for Wireless Networks **2008**,		16
175	Identity in federated electronic healthcare **2008**,		4
174	On Secure and Anonymous Buyer-Seller Watermarking Protocol **2008**,		15
173	Analysis of Grain Initialization Algorithm. *Lecture Notes in Computer Science*, **2008**, 276-289	0.9	35
172	A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks **2008**,		8
171	**2008**,		11
170	Attacks on Two Buyer-Seller Watermarking Protocols and an Improvement for Revocable Anonymity **2008**,		5
169	Hardware implementation of an elliptic curve processor over GF(p) with Montgomery modular multiplier. *International Journal of Embedded Systems*, **2008**, 3, 229	0.5	8
168	Reliable Key Establishment Scheme Exploiting Unidirectional Links in Wireless Sensor Networks **2008**,		5
167	Insights on identity documents based on the Belgian case study. *Information Security Technical Report*, **2008**, 13, 54-60		4
166	Remote attestation on legacy operating systems with trusted platform modules. *Science of Computer Programming*, **2008**, 74, 13-22	1.1	37
165	Revisiting a combinatorial approach toward measuring anonymity **2008**,		24
164	Improving secure long-term archival of digitally signed documents **2008**,		6
163	New Attacks on the Stream Cipher TPy6 and Design of New Ciphers the TPy6-A and the TPy6-B. *Lecture Notes in Computer Science*, **2008**, 127-141	0.9	0

162	A Framework for the Analysis of Mix-Based Steganographic File Systems. *Lecture Notes in Computer Science*, **2008**, 428-445	0.9	2
161	Embedded Trusted Computing with Authenticated Non-volatile Memory. *Lecture Notes in Computer Science*, **2008**, 60-74	0.9	20
160	Perfect Matching Disclosure Attacks. *Lecture Notes in Computer Science*, **2008**, 2-23	0.9	21
159	A Practical Attack on KeeLoq **2008**, 1-18		44
158	Towards Tamper Resistant Code Encryption: Practice and Experience. *Lecture Notes in Computer Science*, **2008**, 86-100	0.9	21
157	Mutual Information Analysis. *Lecture Notes in Computer Science*, **2008**, 426-442	0.9	282
156	Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms. *Lecture Notes in Computer Science*, **2008**, 144-161	0.9	54
155	A Secure Cross-Layer Protocol for Multi-hop Wireless Body Area Networks. *Lecture Notes in Computer Science*, **2008**, 94-107	0.9	16
154	Collisions for RC4-Hash. *Lecture Notes in Computer Science*, **2008**, 355-366	0.9	4
153	Public-Key Cryptography for RFID Tags and Applications **2008**, 317-348		3
152	Attacking Some Perceptual Image Hash Algorithms **2007**,		9
151	Key Establishment Using Secure Distance Bounding Protocols **2007**,		6
150	A Side-channel Attack Resistant Programmable PKC Coprocessor for Embedded Applications **2007**,		7
149	An introduction to modern cryptology **2007**, 565-592		
148	A survey of recent developments in cryptographic algorithms for smart cards. *Computer Networks*, **2007**, 51, 2223-2233	5.4	12
147	HW/SW co-design for public-key cryptosystems on the 8051 micro-controller. *Computers and Electrical Engineering*, **2007**, 33, 324-332	4.3	3
146	Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems. *Computers and Electrical Engineering*, **2007**, 33, 367-382	4.3	36
145	High-performance Public-key Cryptoprocessor for Wireless Mobile Applications. *Mobile Networks and Applications*, **2007**, 12, 245-258	2.9	13

144	**2007**,		16
143	Seven-Property-Preserving Iterated Hashing: ROX **2007**, 130-146		43
142	Efficient pipelining for modular multiplication architectures in prime fields **2007**,		11
141	Pripayd **2007**,		30
140	On Secure Image Hashing by Higher-Order Statistics **2007**,		3
139	Multicore Curve-Based Cryptoprocessor with Reconfigurable Modular Arithmetic Logic Units over GF(2^n). *IEEE Transactions on Computers*, **2007**, 56, 1269-1282	2.5	38
138	Reconfigurable modular arithmetic logic unit supporting high-performance RSA and ECC over GF(p). *International Journal of Electronics*, **2007**, 94, 501-514	1.2	18
137	New Weaknesses in the Keystream Generation Algorithms of the Stream Ciphers TPy and Py. *Lecture Notes in Computer Science*, **2007**, 249-262	0.9	4
136	Preimages for Reduced-Round Tiger. *Lecture Notes in Computer Science*, **2007**, 90-99	0.9	5
135	Electronic Voting in Belgium: Past and Future. *Lecture Notes in Computer Science*, **2007**, 76-87	0.9	2
134	Accountable Anonymous Communication **2007**, 239-253		8
133	Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy. *Lecture Notes in Computer Science*, **2007**, 276-290	0.9	11
132	Distance Bounding in Noisy Environments. *Lecture Notes in Computer Science*, **2007**, 101-115	0.9	54
131	Related-Key Rectangle Attacks on Reduced AES-192 and AES-256. *Lecture Notes in Computer Science*, **2007**, 225-241	0.9	36
130	Differential-Linear Attacks Against the Stream Cipher Phelix. *Lecture Notes in Computer Science*, **2007**, 87-100	0.9	14
129	MAME: A Compression Function with Reduced Hardware Requirements. *Lecture Notes in Computer Science*, **2007**, 148-165	0.9	17
128	Efficient Negative Databases from Cryptographic Hash Functions. *Lecture Notes in Computer Science*, **2007**, 423-436	0.9	9
127	Efficient Oblivious Augmented Maps: Location-Based Services with a Payment Broker **2007**, 77-94		12

126	Related-Key Attacks on the Py-Family of Ciphers and an Approach to Repair the Weaknesses **2007**, 58-72		2
125	Improved Meet-in-the-Middle Attacks on Reduced-Round DES **2007**, 86-100		21
124	nPAKE + : A Hierarchical Group Password-Authenticated Key Exchange Protocol Using Different Passwords. *Lecture Notes in Computer Science*, **2007**, 31-43	0.9	7
123	Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings **2007**, 264-277		54
122	Traffic Analysis Attacks on a Continuously-Observable Steganographic File System. *Lecture Notes in Computer Science*, **2007**, 220-236	0.9	3
121	Classification of cubic (n-4)-resilient Boolean functions. *IEEE Transactions on Information Theory*, **2006**, 52, 1670-1676	2.8	3
120	**2006**,		71
119	Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks. *Lecture Notes in Computer Science*, **2006**, 6-17	0.9	70
118	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	0.9	54
117	Extending the Selective MPEG Encryption Algorithm PVEA **2006**,		1
116	On the security of stepwise triangular systems. *Designs, Codes, and Cryptography*, **2006**, 40, 285-302	1.2	16
115	Improved Pairing Protocol for Bluetooth. *Lecture Notes in Computer Science*, **2006**, 252-265	0.9	2
114	A Weakness in Some Oblivious Transfer and Zero-Knowledge Protocols. *Lecture Notes in Computer Science*, **2006**, 348-363	0.9	
113	Update on Tiger. *Lecture Notes in Computer Science*, **2006**, 63-79	0.9	8
112	Blind Differential Cryptanalysis for Enhanced Power Attacks. *Lecture Notes in Computer Science*, **2006**, 163-173	0.9	12
111	Distinguishing Attacks on the Stream Cipher Py. *Lecture Notes in Computer Science*, **2006**, 405-421	0.9	11
110	Resynchronization Attacks on WG and LEX. *Lecture Notes in Computer Science*, **2006**, 422-432	0.9	16
109	Cryptanalysis of the Stream Cipher DECIM. *Lecture Notes in Computer Science*, **2006**, 30-40	0.9	6

108	Time-Memory Trade-Off Attack on FPGA Platforms: UNIX Password Cracking. *Lecture Notes in Computer Science*, **2006**, 323-334	0.9	8
107	On the (In)security of Stream Ciphers Based on Arrays and Modular Addition. *Lecture Notes in Computer Science*, **2006**, 69-83	0.9	16
106	Cryptanalysis of Reduced Variants of the FORK-256 Hash Function. *Lecture Notes in Computer Science*, **2006**, 85-100	0.9	5
105	Near Optimal Algorithms for Solving Differential Equations of Addition with Batch Queries. *Lecture Notes in Computer Science*, **2005**, 90-103	0.9	10
104	Cryptanalysis of the Two-Dimensional Circulation Encryption Algorithm. *Eurasip Journal on Advances in Signal Processing*, **2005**, 2005, 1	1.9	7
103	Efficient Cooperative Signatures: A Novel Authentication Scheme for Sensor Networks. *Lecture Notes in Computer Science*, **2005**, 86-100	0.9	5
102	Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192. *Lecture Notes in Computer Science*, **2005**, 368-383	0.9	44
101	Threat Modelling for Security Tokens in Web Applications. *International Federation for Information Processing*, **2005**, 183-193		7
100	Spectral characterization of cryptographic Boolean functions satisfying the (extended) propagation criterion of degree l and order k. *Information Processing Letters*, **2005**, 93, 25-28	0.8	2
99	Recent attacks on alleged SecurID and their practical implications. *Computers and Security*, **2005**, 24, 364-370	4.9	4
98	On the covering radii of binary Reed-Muller codes in the set of resilient Boolean functions. *IEEE Transactions on Information Theory*, **2005**, 51, 1182-1189	2.8	14
97	Solving Systems of Differential Equations of Addition. *Lecture Notes in Computer Science*, **2005**, 75-88	0.9	17
96	A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes. *Lecture Notes in Computer Science*, **2005**, 29-43	0.9	19
95	A Systematic Evaluation of Compact Hardware Implementations for the Rijndael S-Box. *Lecture Notes in Computer Science*, **2005**, 323-333	0.9	42
94	Classification of Boolean Functions of 6 Variables or Less with Respect to Some Cryptographic Properties. *Lecture Notes in Computer Science*, **2005**, 324-334	0.9	13
93	Probabilistic Algebraic Attacks. *Lecture Notes in Computer Science*, **2005**, 290-303	0.9	9
92	Normality of Vectorial Functions. *Lecture Notes in Computer Science*, **2005**, 186-200	0.9	1
91	On the Security of Encryption Modes of MD4, MD5 and HAVAL. *Lecture Notes in Computer Science*, **2005**, 147-158	0.9	7

90	Large Superfluous Keys in (mathcal{M})ultivariate (mathcal{Q})uadratic Asymmetric Systems. *Lecture Notes in Computer Science*, **2005**, 275-287	0.9	16
89	Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC. *Lecture Notes in Computer Science*, **2005**, 294-309	0.9	26
88	Non-randomness of the Full 4 and 5-Pass HAVAL. *Lecture Notes in Computer Science*, **2005**, 324-336	0.9	7
87	Equivalent Keys in HFE, C*, and Variations. *Lecture Notes in Computer Science*, **2005**, 33-49	0.9	18
86	A Randomised Algorithm for Checking The Normality of Cryptographic Boolean Functions **2004**, 51-66		
85	Taxonomy of Mixes and Dummy Traffic **2004**, 217-232		22
84	On Boolean Functions with Generalized Cryptographic Properties. *Lecture Notes in Computer Science*, **2004**, 120-135	0.9	11
83	The Biryukov-Demirci Attack on Reduced-Round Versions of IDEA and MESH Ciphers. *Lecture Notes in Computer Science*, **2004**, 98-109	0.9	10
82	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	0.9	66
81	Reasoning About the Anonymity Provided by Pool Mixes That Generate Dummy Traffic. *Lecture Notes in Computer Science*, **2004**, 309-325	0.9	23
80	Higher Order Universal One-Way Hash Functions. *Lecture Notes in Computer Science*, **2004**, 201-213	0.9	6
79	The MESH Block Ciphers. *Lecture Notes in Computer Science*, **2004**, 458-473	0.9	10
78	E03: A new systolic architecture for multiplication in GF(2n). *IFAC Postprint Volumes IPPV / International Federation of Automatic Control*, **2004**, 37, 461-466		
77	Robust Metering Schemes for General Access Structures. *Lecture Notes in Computer Science*, **2004**, 53-65	0.9	
76	Cryptanalysis of the Alleged SecurID Hash Function. *Lecture Notes in Computer Science*, **2004**, 130-144	0.9	4
75	Trends in Cryptology Research **2004**, 51-58		1
74	Power Analysis Attacks Against FPGA Implementations of the DES. *Lecture Notes in Computer Science*, **2004**, 84-94	0.9	18
73	On Feistel Ciphers Using Optimal Diffusion Mappings Across Multiple Rounds. *Lecture Notes in Computer Science*, **2004**, 1-15	0.9	10

72	Extending the Resynchronization Attack. *Lecture Notes in Computer Science*, **2004**, 19-38	0.9	15
71	Revocable anonymous access to the Internet?. *Internet Research*, **2003**, 13, 242-258	4.8	21
70	On Multiplicative Linear Secret Sharing Schemes. *Lecture Notes in Computer Science*, **2003**, 135-147	0.9	5
69	A Note on Weak Keys of PES, IDEA, and Some Extended Variants. *Lecture Notes in Computer Science*, **2003**, 267-279	0.9	1
68	A new inequality in discrete Fourier theory. *IEEE Transactions on Information Theory*, **2003**, 49, 2038-2040	2.8	6
67	Towards a framework for evaluating certificate status information mechanisms. *Computer Communications*, **2003**, 26, 1839-1850	5.1	25
66	Hardware architectures for public key cryptography. *The Integration VLSI Journal*, **2003**, 34, 1-64	1.4	47
65	Power-Analysis Attacks on an FPGA First Experimental Results. *Lecture Notes in Computer Science*, **2003**, 35-50	0.9	35
64	Towards Measuring Anonymity. *Lecture Notes in Computer Science*, **2003**, 54-68	0.9	199
63	Pseudorandomness of Basic Structures in the Block Cipher KASUMI. *ETRI Journal*, **2003**, 25, 89-100	1.4	1
62	Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator. *Lecture Notes in Computer Science*, **2003**, 52-67	0.9	19
61	Cryptanalysis of Sober-t32. *Lecture Notes in Computer Science*, **2003**, 111-128	0.9	7
60	A Concrete Security Analysis for 3GPP-MAC. *Lecture Notes in Computer Science*, **2003**, 154-169	0.9	6
59	Cryptanalysis of 3-Pass HAVAL. *Lecture Notes in Computer Science*, **2003**, 228-245	0.9	18
58	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	0.9	9
57	On a Resynchronization Weakness in a Class of Combiners with Memory. *Lecture Notes in Computer Science*, **2003**, 164-173	0.9	2
56	A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms. *Lecture Notes in Computer Science*, **2003**, 33-50	0.9	72
55	Combining World Wide Web and Wireless Security. *IFIP Advances in Information and Communication Technology*, **2002**, 153-171	0.5	3

54	. *IEEE Transactions on Information Theory*, **2002**, 48, 2524-2539	2.8	19
53	On the Security of Today's Online Electronic Banking Systems. *Computers and Security*, **2002**, 21, 253-265	4.9	42
52	New Weak-Key Classes of IDEA. *Lecture Notes in Computer Science*, **2002**, 315-326	0.9	30
51	A Tangled World Wide Web of Security Issues. *First Monday*, **2002**, 7,		5
50	NESSIE: A European Approach to Evaluate Cryptographic Algorithms. *Lecture Notes in Computer Science*, **2002**, 267-276	0.9	
49	On Unconditionally Secure Distributed Oblivious Transfer. *Lecture Notes in Computer Science*, **2002**, 395-408	0.9	10
48	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	0.9	3
47	Improved Square Attacks against Reduced-Round Hierocrypt. *Lecture Notes in Computer Science*, **2002**, 165-173	0.9	8
46	Producing Collisions for PANAMA. *Lecture Notes in Computer Science*, **2002**, 37-51	0.9	6
45	A New Keystream Generator MUGI. *Lecture Notes in Computer Science*, **2002**, 179-194	0.9	29
44	On Securely Scheduling a Meeting. *IFIP Advances in Information and Communication Technology*, **2001**, 183-198	0.5	2
43	Cryptography on smart cards. *Computer Networks*, **2001**, 36, 423-435	5.4	14
42	Linear Cryptanalysis of Reduced-Round Versions of the SAFER Block Cipher Family. *Lecture Notes in Computer Science*, **2001**, 244-261	0.9	9
41	New (Two-Track-)MAC Based on the Two Trails of RIPEMD. *Lecture Notes in Computer Science*, **2001**, 314-324	0.9	3
40	Secure Meeting Scheduling with Agenta. *IFIP Advances in Information and Communication Technology*, **2001**, 327-338	0.5	2
39	Authentication and payment in future mobile systems. *Journal of Computer Security*, **2000**, 8, 183-207	0.8	14
38	Evaluating certificate status information mechanisms **2000**,		13
37	Equivalent Keys of HPC. *Lecture Notes in Computer Science*, **1999**, 29-42	0.9	4

36	The State of Cryptographic Hash Functions. *Lecture Notes in Computer Science*, **1999**, 158-182	0.9	25
35	On the Security of Double and 2-Key Triple Modes of Operation. *Lecture Notes in Computer Science*, **1999**, 215-230	0.9	6
34	State-of-the-art ciphers for commercial applications. *Computers and Security*, **1999**, 18, 67-74	4.9	1
33	CNN Algorithms for Video Authentication and Copyright Protection. *Journal of Signal Processing Systems*, **1999**, 23, 449-463		1
32	On the security of iterated message authentication codes. *IEEE Transactions on Information Theory*, **1999**, 45, 188-199	2.8	54
31	Linear Cryptanalysis of RC5 and RC6. *Lecture Notes in Computer Science*, **1999**, 16-30	0.9	17
30	Attack on Six Rounds of CRYPTON. *Lecture Notes in Computer Science*, **1999**, 46-59	0.9	17
29	Software Performance of Universal Hash Functions. *Lecture Notes in Computer Science*, **1999**, 24-41	0.9	31
28	Attacks on Fast Double Block Length Hash Functions. *Journal of Cryptology*, **1998**, 11, 59-72	2.1	50
27	Cryptographic Primitives for Information Authentication State of the Art. *Lecture Notes in Computer Science*, **1998**, 49-104	0.9	13
26	MacDES: MAC algorithm based on DES. *Electronics Letters*, **1998**, 34, 871	1.1	18
25	Authentication and payment in future mobile systems. *Lecture Notes in Computer Science*, **1998**, 277-293	0.9	45
24	An Introduction to Cryptology. *Lecture Notes in Computer Science*, **1998**, 204-221	0.9	1
23	Recent Developments in the Design of Conventional Cryptographic Algorithms. *Lecture Notes in Computer Science*, **1998**, 105-130	0.9	8
22	Analysis Methods for (Alleged) RC4. *Lecture Notes in Computer Science*, **1998**, 327-341	0.9	52
21	A family of trapdoor ciphers. *Lecture Notes in Computer Science*, **1997**, 139-148	0.9	25
20	Fast and secure hashing based on codes. *Lecture Notes in Computer Science*, **1997**, 485-498	0.9	27
19	MACs and hash functions: State of the art. *Information Security Technical Report*, **1997**, 2, 33-43		1

18	On Weaknesses of Non□urjective Round Functions. *Designs, Codes, and Cryptography*, **1997**, 12, 253-266	1.2	14
17	Security analysis of the message authenticator algorithm (MAA). *European Transactions on Telecommunications*, **1997**, 8, 455-470		9
16	Key recovery attack on ANSI X9.19 retail MAC. *Electronics Letters*, **1996**, 32, 1568	1.1	22
15	Hash functions based on block ciphers and quaternary codes. *Lecture Notes in Computer Science*, **1996**, 77-90	0.9	14
14	The cipher SHARK. *Lecture Notes in Computer Science*, **1996**, 99-111	0.9	82
13	RIPEMD-160: A strengthened version of RIPEMD. *Lecture Notes in Computer Science*, **1996**, 71-82	0.9	180
12	The Newton channel. *Lecture Notes in Computer Science*, **1996**, 151-156	0.9	15
11	On the Security of Two MAC Algorithms. *Lecture Notes in Computer Science*, **1996**, 19-32	0.9	41
10	MDx-MAC and Building Fast MACs from Hash Functions. *Lecture Notes in Computer Science*, **1995**, 1-14	0.9	45
9	Improved characteristics for differential cryptanalysis of hash functions based on block ciphers. *Lecture Notes in Computer Science*, **1995**, 242-248	0.9	9
8	Hash functions based on block ciphers: a synthetic approach **1993**, 368-378		189
7	Information authentication: Hash functions and digital signatures. *Lecture Notes in Computer Science*, **1993**, 87-131	0.9	3
6	Cryptanalysis of the CFB mode of the DES with a reduced number of rounds **1993**, 212-223		10
5	On the power of memory in the design of collision resistant hash functions. *Lecture Notes in Computer Science*, **1993**, 105-121	0.9	10
4	Propagation Characteristics of Boolean Functions. *Lecture Notes in Computer Science*, **1991**, 161-173	0.9	81
3	Cryptanalysis of a fast cryptographic checksum algorithm. *Computers and Security*, **1990**, 9, 257-262	4.9	5
2	A Chosen Text Attack on The Modified Cryptographic Checksum Algorithm of Cohen and Huang **1989**, 154-163		3
1	Revisiting a Methodology for Efficient CNN Architectures in Profiling Attacks. *Iacr Transactions on Cryptographic Hardware and Embedded Systems*,147-168		13