Probabilistic encryption

DOI: 10.1016/0022-0000(84)90070-9
Journal of Computer and System Sciences, 1984, 28, 270-299.

#	Paper	IF	Citations
2294	IEEE Standard for Identity-Based Cryptographic Techniques using Pairings.		1
2293	.		1
2292	How to Generate Cryptographically Strong Sequences of Pseudorandom Bits. **1984**, 13, 850-864		770
2291	RSA/Rabin Bits are 1/2 + 1 / Poly (Log N) Secure. **1984**,		14
2290	Complexity Measures For Public-Key Cryptosystems.		13
2289	A "Paradoxical" Solution To The Signature Problem. **1984**,		36
2288	An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information. **1984**, 289-299		94
2287	An Update on Quantum Cryptography. **1984**, 475-480		37
2286	Verifiable secret sharing and achieving simultaneity in the presence of faults. **1985**,		332
2285	Origins of randomness in physical systems. **1985**, 55, 449-452		88
2284	Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. **1986**,		236
2283	The NP-completeness column: An ongoing guide. **1986**, 7, 584-601		12
2282	Random sequence generation by cellular automata. **1986**, 7, 123-169		275
2281	Authentication: A concise survey. **1986**, 5, 243-250		2
2280	How to Reduce your Enemyâ Information (extended abstract). **1985**, 468-476		19
2279	Information theoretic reductions among disclosure problems. **1986**,		76
2278	. **1986**,		5

2277	On the cunning power of cheating verifiers: Some observations about zero knowledge proofs. **1987**,		36
2276	Computer Algebra Algorithms. **1987**, 2, 91-118		4
2275	A practical scheme for non-interactive verifiable secret sharing. **1987**,		463
2274	Interactive proof systems: Provers that never fail and random selection. **1987**,		17
2273	Open Problems in Number Theoretic Complexity. **1987**, 237-262		5
2272	One way functions and pseudorandom generators. **1987**, 7, 357-363		181
2271	One-way permutations in NC0. **1987**, 26, 153-155		23
2270	The NP-completeness column: An ongoing guide. **1988**, 9, 426-444		22
2269	Partial information in public key cryptography. **1988**, 20, 261-263		
2268	Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, **1988**, 37, 156-189	1	540
2267	. **1988**,		60
2266	Non-Interactive Zero-Knowledge Proof Systems. *Lecture Notes in Computer Science*, **1988**, 52-72	0.9	48
2265	. **1988**, 34, 901-909		118
2264	The Notion of Security for Probabilistic Cryptosystems. **1988**, 17, 412-426		94
2263	RSA and Rabin Functions: Certain Parts are as Hard as the Whole. **1988**, 17, 194-209		199
2262	A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. **1988**, 17, 281-308		1676
2261	Complexity Measures for Public-Key Cryptosystems. **1988**, 17, 309-335		195
2260	Solving Simultaneous Modular Equations of Low Degree. **1988**, 17, 336-341		104

2259	. **1988**,		27
2258	How to sign given any trapdoor function. **1988**,		17
2257	Advances in Cryptology â EUROCRYPT â 88. *Lecture Notes in Computer Science*, **1988**,	0.9	2
2256	Simple constant-time consensus protocols in realistic failure models. **1989**, 36, 591-614		32
2255	Some consequences of the existence of pseudorandom generators. *Journal of Computer and System Sciences*, **1989**, 39, 101-124	1	19
2254	. **1989**,		168
2253	The Knowledge Complexity of Interactive Proof Systems. **1989**, 18, 186-208		1685
2252	Minimum-Knowledge Interactive Proofs for Decision Problems. **1989**, 18, 711-739		37
2251	A note on computational indistinguishability. **1990**, 34, 277-281		38
2250	Secure circuit evaluation. *Journal of Cryptology*, **1990**, 2, 1-12	2.1	81
2249	An efficient probabilistic encryption scheme. **1990**, 34, 123-129		6
2248	Security, veriflability, and universality in distributed computing. **1990**, 11, 492-521		6
2247	Cryptography. **1990**, 717-755		31
2246	.		56
2245	How to Break the Direct RSA-Implementation of Mixes. **1989**, 373-381		32
2244	Advances in Cryptology â CRYPTOâ 88. *Lecture Notes in Computer Science*, **1990**,	0.9	16
2243	Everything Provable is Provable in Zero-Knowledge. *Lecture Notes in Computer Science*, **1990**, 37-56	0.9	80
2242	Cryptography Based Data Security. **1990**, 30, 171-222		1

2241	Flipping Persuasively in Constant Time. **1990**, 19, 472-499		15
2240	Noninteractive Zero-Knowledge. **1991**, 20, 1084-1118		242
2239	.		2
2238	.		1
2237	Pseudorandom bits for constant depth circuits. **1991**, 11, 63-70		111
2236	Practical zero-knowledge proofs: Giving hints and using deficiencies. *Journal of Cryptology*, **1991**, 4, 185-206		33
2235	How to time-stamp a digital document. *Journal of Cryptology*, **1991**, 3, 99-111	2.1	462
2234	Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. **1991**, 38, 690-728		612
2233	.		5
2232	Advances in Cryptology âEUROCRYPT â90. *Lecture Notes in Computer Science*, **1991**,	0.9	4
2231	How to sign given any trapdoor permutation. **1992**, 39, 214-233		36
2230	Systematic Design of Two-Party Authentication Protocols. **1991**, 44-61		36
2229	. **1992**,		73
2228	Advances in Cryptology âCRYPTO â91. *Lecture Notes in Computer Science*, **1992**,	0.9	1
2227	Foundations of Secure Interactive Computing. **1991**, 377-391		89
2226	. **1992**,		3
2225	.		3
2224	A zero knowledge probabilistic login protocol. **1992**, 11, 733-745		1

2223	The discrete logarithm modulo a composite hides 0(n) Bits. *Journal of Computer and System Sciences*, **1993**, 47, 376-404	1	40
2222	Mathematical problems in cryptology. **1993**, 67, 3373-3406		
2221	On the communication complexity of zero-knowledge proofs. *Journal of Cryptology*, **1993**, 6, 65-85	2.1	6
2220	A perfect zero-knowledge proof system for a problem equivalent to the discrete logarithm. *Journal of Cryptology*, **1993**, 6, 97-116	2.1	21
2219	A uniform-complexity treatment of encryption and zero-knowledge. *Journal of Cryptology*, **1993**, 6, 21-53	2.1	72
2218	On the Existence of Pseudorandom Generators. **1993**, 22, 1163-1175		71
2217	Random-Self-Reducibility of Complete Sets. **1993**, 22, 994-1005		87
2216	. **1993**, 11, 715-724		38
2215	Computer security by redefining what a computer is. **1993**,		26
2214	Advances in Cryptology âEUROCRYPT â93. *Lecture Notes in Computer Science*, **1994**,	0.9	14
2213	Secure distributed computing: Theory and practice. *Lecture Notes in Computer Science*, **1994**, 53-73	0.9	
2212	Chapter 38 Game-theoretic aspects of computing. **1994**, 2, 1339-1395		11
2211	On randomization in sequential and distributed algorithms. **1994**, 26, 7-86		33
2210	.		7
2209	The knowledge complexity of quadratic residuosity languages. **1994**, 132, 291-317		24
2208	Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, **1994**, 7, 1-32	2.1	325
2207	The power of adaptiveness and additional queries in random-self-reductions. **1994**, 4, 158-174		7
2206	Hardness vs randomness. *Journal of Computer and System Sciences*, **1994**, 49, 149-167	1	480

2205	Number Theory and Cryptography. **1994**, 211-236		
2204	Distance-Bounding Protocols. **1993**, 344-359		309
2203	Fast generation of prime numbers and secure public-key cryptographic parameters. *Journal of Cryptology*, **1995**, 8, 123-155	2.1	54
2202	Subquadratic zero-knowledge. **1995**, 42, 1169-1193		8
2201	Optimal asymmetric encryption. *Lecture Notes in Computer Science*, **1995**, 92-111	0.9	451
2200	Proactive Secret Sharing Or: How to Cope With Perpetual Leakage. *Lecture Notes in Computer Science*, **1995**, 339-352	0.9	217
2199	.		
2198	Synthesizers and their application to the parallel construction of pseudo-random functions.		12
2197	Efficient cryptographic schemes provably as secure as subset sum. *Journal of Cryptology*, **1996**, 9, 199-216	2.1	96
2196	Joint encryption and message-efficient secure computation. *Journal of Cryptology*, **1996**, 9, 217-232	2.1	30
2195	Software protection and simulation on oblivious RAMs. **1996**, 43, 431-473		820
2194	On the Composition of Zero-Knowledge Proof Systems. **1996**, 25, 169-192		240
2193	SKEME: a versatile secure key exchange mechanism for Internet.		59
2192	Multisymbol majority vote and hard core. **1996**, 58, 285-292		
2191	Towards a formal system-to-system authentication protocol. **1996**, 19, 954-961		6
2190	â€Indirect discourse proofsâ€Achieving efficient Fair Off-Line e-cash. *Lecture Notes in Computer Science*, **1996**, 286-300	0.9	69
2189	Incoercible multiparty computation.		18
2188	Information Systems Security. **1996**,		1

2187	Does parallel repetition lower the error in computationally sound protocols?.		31
2186	Positive applications of lattices to cryptography. *Lecture Notes in Computer Science*, **1997**, 44-51	0.9	3
2185	The prevalence of kleptographic attacks on discrete-log based cryptosystems. *Lecture Notes in Computer Science*, **1997**, 264-276	0.9	45
2184	Sliding encryption: A cryptographic tool for mobile agents. *Lecture Notes in Computer Science*, **1997**, 230-241	0.9	15
2183	On the foundations of modern cryptography. *Lecture Notes in Computer Science*, **1997**, 46-74	0.9	17
2182	Proactive RSA. *Lecture Notes in Computer Science*, **1997**, 440-454	0.9	73
2181	An information-theoretic treatment of random-self-reducibility. *Lecture Notes in Computer Science*, **1997**, 523-534	0.9	1
2180	âPseudo-randomâ number generation within cryptographic algorithms: The DDS case. *Lecture Notes in Computer Science*, **1997**, 277-291	0.9	42
2179	Provable security for cryptographic protocols-exact analysis and engineering applications.		3
2178	Minimizing the use of random oracles in authenticated encryption schemes. *Lecture Notes in Computer Science*, **1997**, 1-16	0.9	30
2177	New directions in cryptography: twenty some years later (or cryptograpy and complexity theory: a match made in heaven).		5
2176	Replication is not needed: single database, computationally-private information retrieval.		198
2175	Optimal-resilience proactive public-key cryptosystems.		71
2174	Public-key cryptosystems from lattice reduction problems. *Lecture Notes in Computer Science*, **1997**, 112-131	0.9	206
2173	Number-theoretic constructions of efficient pseudo-random functions.		71
2172	Plug and play encryption. *Lecture Notes in Computer Science*, **1997**, 75-89	0.9	41
2171	An Optimal Probabilistic Protocol for Synchronous Byzantine Agreement. **1997**, 26, 873-933		119
2170	A concrete security treatment of symmetric encryption.		220

2169	ATM cell encryption and key update synchronization. **1997**, 7, 391-408		1
2168	On the Clark-Jacob version of SPLICE/AS. **1997**, 62, 251-254		3
2167	A formal framework for evaluating heuristic programs. **1998**, 22, 193-206		1
2166	Statistical secrecy and multibit commitments. **1998**, 44, 1143-1151		29
2165	Secret sharing with public reconstruction. **1998**, 44, 1887-1896		10
2164	Secret Sharing With Public Reconstruction. **1998**, 44, 1887-1896		20
2163	Computational indistinguishability: Algorithms vs. circuits. **1998**, 191, 215-218		4
2162	A confused document encrypting scheme and its implementation. **1998**, 17, 543-551		4
2161	Many-to-one trapdoor functions and their relation to public-key cryptosystems. *Lecture Notes in Computer Science*, **1998**, 283-298	0.9	34
2160	Computational indistinguishability: a sample hierarchy.		
2159	.		
2158	Randomness vs. time: de-randomization under a uniform assumption.		18
2157	On enabling secure applications through off-line biometric identification.		163
2156	Stop- and- Go-MIXes Providing Probabilistic Anonymity in an Open System. *Lecture Notes in Computer Science*, **1998**, 83-98	0.9	130
2155	A new public key cryptosystem based on higher residues. **1998**,		162
2154	The Decision Diffie-Hellman problem. *Lecture Notes in Computer Science*, **1998**, 48-63	0.9	368
2153	Fast digital identity revocation. *Lecture Notes in Computer Science*, **1998**, 137-152	0.9	53
2152	Information Hiding. *Lecture Notes in Computer Science*, **1998**,	0.9	11

2151	On Software Protection via Function Hiding. *Lecture Notes in Computer Science*, **1998**, 111-123	0.9	40
2150	Public-key cryptography and password protocols. **1998**,		48
2149	Testing problems with sub-learning sample complexity. **1998**,		5
2148	Practice-oriented provable-security. *Lecture Notes in Computer Science*, **1998**, 221-231	0.9	25
2147	A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. *Lecture Notes in Computer Science*, **1998**, 13-25	0.9	693
2146	On the security of ElGamal based encryption. *Lecture Notes in Computer Science*, **1998**, 117-134	0.9	144
2145	NTRU: A ring-based public key cryptosystem. *Lecture Notes in Computer Science*, **1998**, 267-288	0.9	663
2144	.		3
2143	Finite-state analysis of security protocols. *Lecture Notes in Computer Science*, **1998**, 71-76	0.9	8
2142	Advances in Cryptology âASIACRYPTâ98. *Lecture Notes in Computer Science*, **1998**,	0.9	7
2141	Relations among notions of security for public-key encryption schemes. *Lecture Notes in Computer Science*, **1998**, 26-45	0.9	435
2140	Concurrent zero-knowledge: Reducing the need for timing constraints. *Lecture Notes in Computer Science*, **1998**, 442-457	0.9	30
2139	An efficient discrete log pseudo random generator. *Lecture Notes in Computer Science*, **1998**, 304-317	0.9	32
2138	Entity authentication and authenticated key transport protocols employing asymmetric techniques. *Lecture Notes in Computer Science*, **1998**, 137-158	0.9	26
2137	Sequential iteration of interactive arguments and an efficient zero-knowledge argument for NP. *Lecture Notes in Computer Science*, **1998**, 772-783	0.9	7
2136	Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible. *Lecture Notes in Computer Science*, **1998**, 266-280	0.9	47
2135	Generic constructions for secure and efficient confirmer signature schemes. *Lecture Notes in Computer Science*, **1998**, 406-421	0.9	27
2134	A practical mix. *Lecture Notes in Computer Science*, **1998**, 448-461	0.9	87

2133	Zero-knowledge proofs for finite field arithmetic, or: Can zero-knowledge be for free?. *Lecture Notes in Computer Science*, **1998**, 424-441	0.9	79
2132	Provable security for cryptographic protocols â exact analysis and engineering applications. **1998**, 6, 23-52		
2131	Public-key cryptography and password protocols. **1999**,		26
2130	Efficient private bidding and auctions with an oblivious third party. **1999**,		135
2129	Enhancing privacy and trust in electronic communities. **1999**,		83
2128	One-way functions are essential for single-server private information retrieval. **1999**,		24
2127	Secure computation with honest-looking parties (extended abstract). **1999**,		14
2126	Pseudorandom generators without the XOR Lemma (extended abstract). **1999**,		29
2125	Uniform-distribution attribute noise learnability. **1999**,		4
2124	Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries. *Lecture Notes in Computer Science*, **1999**, 165-179	0.9	69
2123	Non-malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization. *Lecture Notes in Computer Science*, **1999**, 519-536	0.9	68
2122	Public-key cryptography and password protocols. **1999**, 2, 230-268		157
2121	Construction of extractors using pseudo-random generators (extended abstract). **1999**,		36
2120	Public Key Cryptography. *Lecture Notes in Computer Science*, **1999**,	0.9	1
2119	Two Party RSA Key Generation. *Lecture Notes in Computer Science*, **1999**, 116-129	0.9	79
2118	Linear complexity of the x2 mod p orbits. **1999**, 72, 3-7		2
2117	Divertible and Subliminal-Free Zero-Knowledge Proofs for Languages. *Journal of Cryptology*, **1999**, 12, 197-223	2.1	9
2116	Cryptographic distinguishability measures for quantum-mechanical states. **1999**, 45, 1216-1227		398

2115	Synthesizers and Their Application to the Parallel Construction of Pseudo-Random Functions. *Journal of Computer and System Sciences*, **1999**, 58, 336-375	1	64
2114	Computational Indistinguishability: A Sample Hierarchy. *Journal of Computer and System Sciences*, **1999**, 59, 253-269	1	1
2113	Non-interactive cryptocomputing for NC/sup 1/.		29
2112	Comparing entropies in statistical zero knowledge with applications to the structure of SZK.		24
2111	Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security.		91
2110	Magic functions.		20
2109	A Pseudorandom Generator from any One-way Function. **1999**, 28, 1364-1396		876
2108	Multiple NonInteractive Zero Knowledge Proofs Under General Assumptions. **1999**, 29, 1-28		204
2107	On the Security Properties of OAEP as an All-or-Nothing Transform. *Lecture Notes in Computer Science*, **1999**, 503-518	0.9	38
2106	Efficient Communication-Storage Tradeoffs for Multicast Encryption. *Lecture Notes in Computer Science*, **1999**, 459-474	0.9	88
2105	On the statistical properties of Diffie-Hellman distributions. **2000**, 120, 23-46		46
2104	Testing Problems with Sublearning Sample Complexity. *Journal of Computer and System Sciences*, **2000**, 61, 428-456	1	24
2103	New Efficient and Secure Protocols for Verifiable Signature Sharing and Other Applications. *Journal of Computer and System Sciences*, **2000**, 61, 51-80	1	1
2102	On the Limits of Nonapproximability of Lattice Problems. *Journal of Computer and System Sciences*, **2000**, 60, 540-563	1	88
2101	On secret set schemes. **2000**, 74, 243-251		4
2100	Secure distributed storage and retrieval. **2000**, 243, 363-389		44
2099	Information Security, Mathematics, and Public-Key Cryptography. **2000**, 19, 77-99		5
2098	Short Non-Interactive Cryptographic Proofs. *Journal of Cryptology*, **2000**, 13, 449-472	2.1	25

2097	Maintaining Authenticated Communication in the Presence of Break-Ins. *Journal of Cryptology*, **2000**, 13, 61-105	2.1	22
2096	Security and Composition of Multiparty Cryptographic Protocols. *Journal of Cryptology*, **2000**, 13, 143-202	2.1	733
2095	Provably Secure Length-Saving Public-Key Encryption Scheme under the Computational Diffie-Hellman Assumption. **2000**, 22, 25-31		4
2094	A Note on Security Proofs in the Generic Model. *Lecture Notes in Computer Science*, **2000**, 458-469	0.9	20
2093	Information Security and Privacy. *Lecture Notes in Computer Science*, **2000**,	0.9	2
2092	Advances in Cryptology â ASIACRYPT 2000. *Lecture Notes in Computer Science*, **2000**,	0.9	7
2091	A Cryptographic Solution to a Game Theoretic Problem. *Lecture Notes in Computer Science*, **2000**, 112-130	0.9	51
2090	Optimistic Fair Secure Computation. *Lecture Notes in Computer Science*, **2000**, 93-111	0.9	52
2089	Complete characterization of security notions for probabilistic private-key encryption. **2000**,		43
2088	Funkspiel schemes. **2000**,		9
2087	A protocol to achieve independence in constant rounds. **2000**, 11, 636-647		9
2086	Advances in Cryptology â CRYPTO 2000. *Lecture Notes in Computer Science*, **2000**,	0.9	44
2085	Quantum Public-Key Cryptosystems. *Lecture Notes in Computer Science*, **2000**, 147-165	0.9	48
2084	Pseudonym Systems. *Lecture Notes in Computer Science*, **2000**, 184-199	0.9	198
2083	Selected Areas in Cryptography. *Lecture Notes in Computer Science*, **2000**,	0.9	4
2082	REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. *Lecture Notes in Computer Science*, **2000**, 159-174	0.9	106
2081	Nonmalleable Cryptography. **2000**, 30, 391-437		526
2080	STACS 2000. *Lecture Notes in Computer Science*, **2000**,	0.9	

2079	A Survey of Number Theory and Cryptography. **2000**, 217-239		6
2078	IEEE Standard Specifications for Public-Key Cryptography.		14
2077	The relationship between public key encryption and oblivious transfer.		47
2076	.		
2075	Extracting randomness from samplable distributions.		67
2074	.		58
2073	. **2000**, 18, 593-610		232
2072	On the (Im)possibility of Obfuscating Programs. *Lecture Notes in Computer Science*, **2001**, 1-18	0.9	519
2071	Trusted Information. **2001**,		0
2070	Universal Exponentiation Algorithm A First Step towards Provable SPA-Resistance. *Lecture Notes in Computer Science*, **2001**, 300-308	0.9	52
2069	The Exact Security of ECIES in the Generic Group Model. *Lecture Notes in Computer Science*, **2001**, 73-84	0.9	27
2068	On the impossibility of basing trapdoor functions on trapdoor predicates. **2001**,		50
2067	The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?). *Lecture Notes in Computer Science*, **2001**, 310-331	0.9	140
2066	A Cost-Effective Pay-Per-Multiplication Comparison Method for Millionaires. *Lecture Notes in Computer Science*, **2001**, 457-471	0.9	65
2065	Probabilistic polynomial-time process calculus and security protocol analysis.		2
2064	Universally composable security: a new paradigm for cryptographic protocols. **2001**,		1222
2063	Strong Forward Security. **2001**, 109-121		3
2062	A fair and efficient solution to the socialist millionairesâ problem. **2001**, 111, 23-36		98

2061	A Probabilistic Polynomial-time Calculus For Analysis of Cryptographic Protocols: (Preliminary Report). **2001**, 45, 280-310		21
2060	Pseudorandom Generators without the XOR Lemma. *Journal of Computer and System Sciences*, **2001**, 62, 236-266	1	175
2059	A lattice-based McEliece scheme for encryption and signature. **2001**, 6, 402-411		2
2058	Self-Scrambling Anonymizers. *Lecture Notes in Computer Science*, **2001**, 259-275	0.9	26
2057	The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES. *Lecture Notes in Computer Science* , **2001**, 143-158	0.9	226
2056	Cryptography and Coding. *Lecture Notes in Computer Science*, **2001**,	0.9	1
2055	Cryptographic Hardware and Embedded Systems â CHES 2001. *Lecture Notes in Computer Science*, **2001**,	0.9	4
2054	Extractors and pseudorandom generators. **2001**, 48, 860-879		185
2053	Paillier's cryptosystem revisited. **2001**,		42
2052	Financial Cryptography. *Lecture Notes in Computer Science*, **2001**,	0.9	3
2051	Advances in Cryptology â EUROCRYPT 2001. *Lecture Notes in Computer Science*, **2001**,	0.9	13
2050	Advances in Cryptology â ASIACRYPT 2001. *Lecture Notes in Computer Science*, **2001**,	0.9	5
2049	An optimally robust hybrid mix network. **2001**,		45
2048	Selective private function evaluation with applications to private statistics. **2001**,		47
2047	OCB. **2001**,		135
2046	Provably authenticated group Diffie-Hellman key exchange. **2001**,		152
2045	Mobile values, new names, and secure communication. **2001**,		302
2044	A model for asynchronous reactive systems and its application to secure message transmission.		92

2043	Mobile values, new names, and secure communication. **2001**, 36, 104-115		170
2042	Public Key Cryptography. *Lecture Notes in Computer Science*, **2001**,	0.9	3
2041	Improving Lattice Based Cryptosystems Using the Hermite Normal Form. *Lecture Notes in Computer Science*, **2001**, 126-145	0.9	66
2040	Public Key Cryptography. *Lecture Notes in Computer Science*, **2002**,	0.9	2
2039	Multi-recipient Public-Key Encryption with Shortened Ciphertext. *Lecture Notes in Computer Science* , **2002**, 48-63	0.9	73
2038	2-round zero knowledge and proof auditors. **2002**,		12
2037	Authenticated encryption in SSH. **2002**,		33
2036	Tight security proofs for the bounded-storage model. **2002**,		21
2035	Authenticated-encryption with associated-data. **2002**,		159
2034	Universally composable two-party and multi-party secure computation. **2002**,		261
2033	Concurrent zero-knowledge with timing, revisited. **2002**,		22
2032	Receipt-freeness in Large-scale Elections without Untappable Channels. **2001**, 683-693		11
2031	Homomorphic Signature Schemes. *Lecture Notes in Computer Science*, **2002**, 244-262	0.9	230
2030	Towards secure IFF: preventing mafia fraud attacks.		4
2029	Number Theory for Computing. **2002**,		66
2028	Introduction to Cryptography. **2002**,		80
2027	Information Security and Cryptology â□CISC 2001. *Lecture Notes in Computer Science*, **2002**,	0.9	13
2026	Graph Nonisomorphism Has Subexponential Size Proofs Unless the Polynomial-Time Hierarchy Collapses. **2002**, 31, 1501-1526		118

2025	Everlasting security in the bounded storage model. **2002**, 48, 1668-1680		75
2024	Reconciling Two Views of Cryptography (The Computational Soundness of Formal Encryption)*. *Journal of Cryptology*, **2002**, 15, 103-127	2.1	203
2023	OAEP Reconsidered. *Journal of Cryptology*, **2002**, 15, 223-249	2.1	93
2022	Compliant cryptologic protocols. **2002**, 1, 189-202		
2021	Buses for Anonymous Message Delivery. *Journal of Cryptology*, **2003**, 16, 25-39	2.1	74
2020	On the one-wayness against chosen-plaintext attacks of the Loidreau's modified McEliece PKC. **2003**, 49, 3160-3168		9
2019	On the freedom of decryption. **2003**, 86, 329-333		20
2018	Dynamical analysis of a class of Euclidean algorithms. **2003**, 297, 447-486		19
2017	Secrecy types for asymmetric communication. **2003**, 298, 387-415		30
2016	On the implementation of huge random objects.		5
2015	Privacy Enhancing Technologies. *Lecture Notes in Computer Science*, **2003**,	0.9	5
2014	The Impact of Decryption Failures on the Security of NTRU Encryption. *Lecture Notes in Computer Science*, **2003**, 226-246	0.9	55
2013	Encryption-Scheme Security in the Presence of Key-Dependent Messages. *Lecture Notes in Computer Science*, **2003**, 62-75	0.9	128
2012	OCB. **2003**, 6, 365-403		186
2011	An IND-CPA cryptosystem from Demytko's primitive.		1
2010	Identity-Based Encryption from the Weil Pairing. **2003**, 32, 586-615		1408
2009	Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. *Lecture Notes in Computer Science*, **2003**, 614-629	0.9	342
2008	Nonmalleable Cryptography. **2003**, 45, 727-784		39

2007	Proving hard-core predicates using list decoding.		27
2006	Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. *Lecture Notes in Computer Science*, **2003**,	0.9	1
2005	Randomness Re-use in Multi-recipient Encryption Schemeas. *Lecture Notes in Computer Science*, **2003**, 85-99	0.9	62
2004	Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack. **2003**, 33, 167-226		576
2003	A computational analysis of the Needham-Schroeder-(Lowe) protocol.		15
2002	A Two-Server, Sealed-Bid Auction Protocol. *Lecture Notes in Computer Science*, **2003**, 72-86	0.9	48
2001	Trust, Reputation, and Security: Theories and Practice. *Lecture Notes in Computer Science*, **2003**,	0.9	2
2000	Topics in Cryptology âCT-RSA 2003. *Lecture Notes in Computer Science*, **2003**,	0.9	4
1999	Selected Areas in Cryptography. *Lecture Notes in Computer Science*, **2003**,	0.9	
1998	Future Directions in Distributed Computing. *Lecture Notes in Computer Science*, **2003**,	0.9	6
1997	Cryptographically Sound and Machine-Assisted Verification of Security Protocols. *Lecture Notes in Computer Science*, **2003**, 675-686	0.9	21
1996	A complete problem for statistical zero knowledge. **2003**, 50, 196-249		88
1995	Lower bounds on the efficiency of encryption and digital signature schemes. **2003**,		16
1994	Hiding Information in Image Mosaics. **2003**, 46, 202-212		4
1993	Efficient revocation and threshold pairing based cryptosystems. **2003**,		60
1992	A composable cryptographic library with nested operations. **2003**,		129
1991	A Tweakable Enciphering Mode. *Lecture Notes in Computer Science*, **2003**, 482-499	0.9	121
1990	Automatic generation of two-party computations. **2003**,		17

1989	Secure and private sequence comparisons. **2003**,		115
1988	Privacy preserving database application testing. **2003**,		7
1987	Universal Designated-Verifier Signatures. *Lecture Notes in Computer Science*, **2003**, 523-542	0.9	100
1986	A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications. *Lecture Notes in Computer Science*, **2003**, 37-54	0.9	131
1985	Magic Functions. **2003**, 50, 852-921		72
1984	Relaxing Chosen-Ciphertext Security. *Lecture Notes in Computer Science*, **2003**, 565-582	0.9	145
1983	A Cryptographically Sound Security Proof of the Needham-Schroeder-Lowe Public-Key Protocol. *Lecture Notes in Computer Science*, **2003**, 1-12	0.9	22
1982	Mental Poker Revisited. *Lecture Notes in Computer Science*, **2003**, 370-383	0.9	18
1981	Nonce-Based Symmetric Encryption. *Lecture Notes in Computer Science*, **2004**, 348-358	0.9	124
1980	Accountable Ring Signatures: A Smart Card Approach. **2004**, 271-286		19
1979	Algorithmic Tamper-Proof (ATP) Security: Theoretical Foundations for Security against Hardware Tampering. *Lecture Notes in Computer Science*, **2004**, 258-277	0.9	113
1978	About the Security of Ciphers (Semantic Security and Pseudo-Random Permutations). *Lecture Notes in Computer Science*, **2004**, 182-197	0.9	35
1977	Universal Re-encryption for Mixnets. *Lecture Notes in Computer Science*, **2004**, 163-178	0.9	164
1976	Towards Plaintext-Aware Public-Key Encryption Without Random Oracles. *Lecture Notes in Computer Science*, **2004**, 48-62	0.9	66
1975	EME*: Extending EME to Handle Arbitrary-Length Messages with Associated Data. *Lecture Notes in Computer Science*, **2004**, 315-327	0.9	51
1974	The security of all RSA and discrete log bits. **2004**, 51, 187-230		21
1973	Asynchronous group key exchange with failures. **2004**,		14
1972	Defending email communication against profiling attacks. **2004**,		2

1971	Concurrent zero-knowledge. **2004**, 51, 851-898		86
1970	A user-centric anonymous authorisation framework in e-commerce environment. **2004**,		1
1969	Number-theoretic constructions of efficient pseudo-random functions. **2004**, 51, 231-262		198
1968	Privacy-preserving data mining on data grids in the presence of malicious participants.		4
1967	The random oracle methodology, revisited. **2004**, 51, 557-594		486
1966	Breaking and provably repairing the SSH authenticated encryption scheme. **2004**, 7, 206-241		67
1965	Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. *Lecture Notes in Computer Science*, **2004**, 16-31	0.9	208
1964	A Cryptographically Sound Dolev-Yao Style Security Proof of the Otway-Rees Protocol. *Lecture Notes in Computer Science*, **2004**, 89-108	0.9	21
1963	Selected Areas in Cryptography. *Lecture Notes in Computer Science*, **2004**,	0.9	3
1962	Trust and Privacy in Digital Business. *Lecture Notes in Computer Science*, **2004**,	0.9	
1961	Chosen-Ciphertext Security from Identity-Based Encryption. *Lecture Notes in Computer Science*, **2004**, 207-222	0.9	438
1960	The dual receiver cryptosystem and its applications. **2004**,		15
1959	Uncoercible e-Bidding Games. **2004**, 4, 113-125		5
1958	Two-party generation of DSA signatures. **2004**, 2, 218-239		20
1957	Protocols useful on the Internet from distributed signature schemes. **2004**, 3, 61-69		4
1956	An operational model and language support for securing XML documents. **2004**, 23, 498-529		15
1955	Private authentication. **2004**, 322, 427-476		70
1954	RSA-OAEP Is Secure under the RSA Assumption. *Journal of Cryptology*, **2004**, 17, 81-104	2.1	85

1953	Cryptography in NC/sup 0/.		18
1952	Leak-free group signatures with immediate revocation. **2004**,		8
1951	.		1
1950	Privacy-preserving association rule mining in large-scale distributed systems.		7
1949	A theory of dictionary attacks and its complexity.		10
1948	Introduction to Cryptography. **2004**,		55
1947	A cryptographically sound security proof of the Needham-Schroeder-Lowe public-key protocol. **2004**, 22, 2075-2086		18
1946	On the Security of Cryptosystems with All-or-Nothing Transform. *Lecture Notes in Computer Science* , **2004**, 76-90	0.9	3
1945	Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. *Lecture Notes in Computer Science*, **2004**, 371-388	0.9	223
1944	A Survey of Public-Key Cryptosystems. **2004**, 46, 599-634		24
1943	Public Key Encryption with Keyword Search. *Lecture Notes in Computer Science*, **2004**, 506-522	0.9	1092
1942	Specifying confidentiality. **2004**, 35, 72-83		
1941	Enhancing anonymity via market competition. **2004**,		
1940	An Uninstantiable Random-Oracle-Model Scheme for a Hybrid-Encryption Problem. *Lecture Notes in Computer Science*, **2004**, 171-188	0.9	121
1939	On the Minimal Assumptions of Group Signature Schemes. *Lecture Notes in Computer Science*, **2004**, 1-13	0.9	19
1938	RECENT DEVELOPMENTS IN EXPLICIT CONSTRUCTIONS OF EXTRACTORS. **2004**, 189-228		13
1937	Bibliography. **2004**, 321-332		
1936	A computational analysis of the Needhamâ5chroederâ(Lowe) protocol. **2005**, 13, 565-591		5

1935	Universally Composable Password-Based Key Exchange. *Lecture Notes in Computer Science*, **2005**, 404-421	0.9	144
1934	Public-Key Steganography with Active Attacks. *Lecture Notes in Computer Science*, **2005**, 210-226	0.9	28
1933	On Tolerant Cryptographic Constructions. *Lecture Notes in Computer Science*, **2005**, 172-190	0.9	24
1932	The design of a secure and fair sealed-bid auction service. **2005**, 41, 973-985		7
1931	Analysing Password Protocol Security Against Off-line Dictionary Attacks. **2005**, 121, 47-63		23
1930	Secure distributed constraint satisfaction: reaching agreement without revealing private information. **2005**, 161, 229-245		23
1929	Oblivious signature-based envelope. **2005**, 17, 293-302		26
1928	FujisakiâOkamoto hybrid encryption revisited. **2005**, 4, 228-241		4
1927	Public-key cryptography and invariant theory. **2005**, 126, 1152-1157		1
1926	On non-Abelian homomorphic public-key cryptosystems. **2005**, 126, 1158-1166		1
1925	Signcryption with Non-interactive Non-repudiation. **2005**, 37, 81-109		11
1924	Computational Indistinguishability Between Quantum States and Its Cryptographic Application. *Lecture Notes in Computer Science*, **2005**, 268-284	0.9	16
1923	Bibliography. **2005**, 504-509		
1922	Correcting errors without leaking partial information. **2005**,		82
1921	New and improved constructions of non-malleable cryptographic protocols. **2005**,		71
1920	Programming Languages and Systems. *Lecture Notes in Computer Science*, **2005**,	0.9	4
1919	Hierarchical Group Signatures. *Lecture Notes in Computer Science*, **2005**, 446-458	0.9	24
1918	On the Design of Provably Secure Identity-Based Authentication and Key Exchange Protocol for Heterogeneous Wireless Access. *Lecture Notes in Computer Science*, **2005**, 972-981	0.9	6

1917	Practical Cryptography in High Dimensional Tori. *Lecture Notes in Computer Science*, **2005**, 234-250	0.9	17
1916	New approaches for deniable authentication. **2005**,		24
1915	Anonymity-preserving data collection. **2005**,		36
1914	Security analysis of cryptographically controlled access to XML documents. **2005**,		3
1913	Collusion-free protocols. **2005**,		34
1912	Privacy Preserving Clustering. *Lecture Notes in Computer Science*, **2005**, 397-417	0.9	83
1911	Computationally private randomizing polynomials and their applications (extended abstract).		10
1910	.		1
1909	Secrecy types for a simulatable cryptographic library. **2005**,		33
1908	Concurrent non-malleable commitments.		40
1907	Security in Communication Networks. *Lecture Notes in Computer Science*, **2005**,	0.9	1
1906	.		61
1905	Information Security. *Lecture Notes in Computer Science*, **2005**,	0.9	5
1904	A Formal Treatment of Onion Routing. *Lecture Notes in Computer Science*, **2005**, 169-187	0.9	70
1903	Foundations of Security Analysis and Design III. *Lecture Notes in Computer Science*, **2005**,	0.9	3
1902	Adaptive Security of Symbolic Encryption. *Lecture Notes in Computer Science*, **2005**, 169-187	0.9	27
1901	Optimal secure data retrieval using an oblivious transfer scheme.		1
1900	On the Power of Nonlinear Secret-Sharing. **2005**, 19, 258-280		16

1899	Bounds on the Efficiency of Generic Cryptographic Constructions. **2005**, 35, 217-246		75
1898	Information Security and Cryptology. *Lecture Notes in Computer Science*, **2005**,	0.9	4
1897	A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount of Data. **2005**,		13
1896	How to play almost any mental game over the net - concurrent composition via super-polynomial simulation.		27
1895	Security analysis on Chinese wireless LAN standard and its solution.		0
1894	Secure Authentication Protocols Used for Low Power Wireless Sensor Networks. **2005**,		1
1893	Rational secure computation and ideal mechanism design.		38
1892	A lightweight approach to authenticated Web caching.		4
1891	Unconditionally secure signatures and its related schemes.		
1890	Computational and information-theoretic soundness and completeness of formal encryption.		8
1889	A cryptographically sound Dolev-Yao style security proof of an electronic payment system.		5
1888	Deciding knowledge in security protocols under (many more) equational theories.		6
1887	On Session Identifiers in Provably Secure Protocols. *Lecture Notes in Computer Science*, **2005**, 351-366	0.9	17
1886	Provable Security for Public Key Schemes. **2005**, 133-190		14
1885	Relating symbolic and cryptographic secrecy. **2005**, 2, 109-123		26
1884	Security of public-key cryptosystems based on Chebyshev polynomials. **2005**, 52, 1382-1393		190
1883	Computer Security âESORICS 2005. *Lecture Notes in Computer Science*, **2005**,	0.9	4
1882	Private Searching on Streaming Data. *Lecture Notes in Computer Science*, **2005**, 223-240	0.9	63

1881	Cryptography and Coding. *Lecture Notes in Computer Science*, **2005**,	0.9	2
1880	Randomness in cryptography. **2006**, 4, 64-67		22
1879	Computer Security âŒESORICS 2006. *Lecture Notes in Computer Science*, **2006**,	0.9	1
1878	Cryptographically Sound Security Proofs for Basic and Public-Key Kerberos. *Lecture Notes in Computer Science*, **2006**, 362-383	0.9	20
1877	Group key exchange over combined wired and wireless networks. **2006**, 8, 461-474		
1876	Kleptographic Weaknesses in Benaloh-Tuinstra Protocol. **2006**,		1
1875	Automated Security Proofs with Sequences of Games. *Lecture Notes in Computer Science*, **2006**, 537-554	0.9	37
1874	FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science. *Lecture Notes in Computer Science*, **2006**,	0.9	5
1873	Information Security. *Lecture Notes in Computer Science*, **2006**,	0.9	1
1872	Parallel repetition of zero-knowledge proofs and the possibility of basing cryptography on NP-hardness.		8
1871	Computationally sound compositional logic for key exchange protocols.		25
1870	Cryptography in NC^0. **2006**, 36, 845-888		109
1869	Public-key cryptography using paraunitary matrices. **2006**, 54, 3489-3504		11
1868	What is cryptography?. **2006**, 4, 70-73		23
1867	A Study on the Security of Privacy Homomorphism. **2006**,		4
1866	Improved proxy re-encryption schemes with applications to secure distributed storage. **2006**, 9, 1-30		678
1865	Provably-secure time-bound hierarchical key assignment schemes. **2006**,		41
1864	. **2006**,		2

1863	Searchable symmetric encryption. **2006**,		824
1862	A survey of algebraic properties used in cryptographic protocols. **2006**, 14, 1-43		97
1861	Relations among Notions of Security for Identity Based Encryption Schemes. **2006**, 2, 465-477		
1860	Deciding knowledge in security protocols under equational theories. **2006**, 367, 2-32		88
1859	Towards a Theory of Software Protection (Extended Abstract). **1986**, 426-439		5
1858	Developing the concept of one-way functions for cryptographic security systems using achievements in chaotic dynamics. **2006**, 42, 884-891		
1857	Decision Procedures for the Security of Protocols with Probabilistic Encryption against Offline Dictionary Attacks. **2006**, 36, 85-124		5
1856	Reducing The Seed Length In The Nisan-Wigderson Generator*. **2006**, 26, 647-681		10
1855	A secure distributed framework for achieving k-anonymity. **2006**, 15, 316-333		104
1854	Characterization of Security Notions for Probabilistic Private-Key Encryption. *Journal of Cryptology*, **2006**, 19, 67-95	2.1	41
1853	Session-Key Generation Using Human Passwords Only. *Journal of Cryptology*, **2006**, 19, 241-340	2.1	35
1852	Protecting against key-exposure: strongly key-insulated encryption with optimal threshold. **2006**, 16, 379-396		25
1851	Homomorphic Public-Key Cryptosystems and Encrypting Boolean Circuits. **2006**, 17, 239-255		9
1850	A probabilistic polynomial-time process calculus for the analysis of cryptographic protocols. **2006**, 353, 118-164		50
1849	Real-or-random Key Secrecy of the Otway-Rees Protocol via a Symbolic Security Proof. **2006**, 155, 111-145		1
1848	Public key cryptography based on ergodic matrices over finite field. **2006**, 11, 1525-1528		5
1847	. *IEEE Transactions on Information Forensics and Security*, **2006**, 1, 524-531	8	1
1846	. **2006**, 52, 1130-1140		19

1845	Security and composition of cryptographic protocols. **2006**, 37, 67-92		31
1844	Digitally signed document sanitizing scheme based on bilinear maps. **2006**,		57
1843	Securing wireless systems via lower layer enforcements. **2006**,		102
1842	Stateful public-key cryptosystems. **2006**,		29
1841	Secure multiparty computation of approximations. **2006**, 2, 435-472		61
1840	Towards security and QoS optimization in real-time embedded systems. **2006**, 3, 29-34		6
1839	A Classical Introduction to Cryptography. **2006**,		1
1838	Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret (Extended Abstract). **1986**, 251-260		104
1837	NIS05-6: A Non-Commutative Generalization of ElGamal Key Exchange using Polycyclic Groups. **2006**,		5
1836	Quantum Computation and Information. **2006**,		11
1835	Progress in Cryptology - VIETCRYPT 2006. *Lecture Notes in Computer Science*, **2006**,	0.9	1
1834	Public Key Cryptography Sans Certificates in Ad Hoc Networks. *Lecture Notes in Computer Science*, **2006**, 375-389	0.9	5
1833	Public Key Cryptography - PKC 2006. *Lecture Notes in Computer Science*, **2006**,	0.9	10
1832	Encoding-Free ElGamal Encryption Without Random Oracles. *Lecture Notes in Computer Science*, **2006**, 91-104	0.9	18
1831	Public Key Cryptography â PKC 2007. *Lecture Notes in Computer Science*, **2007**,	0.9	2
1830	How to Build a Hash Function from Any Collision-Resistant Function. **2007**, 147-163		11
1829	Fast, Secure Encryption for Indexing in a Column-Oriented DBMS. **2007**,		30
1828	A Proof of Revised Yahalom Protocol in the Bellare and Rogaway (1993) Model. **2007**, 50, 591-601		10

1827	Security under key-dependent inputs. **2007**,		32
1826	An efficient parallel repetition theorem for Arthur-Merlin games. **2007**,		21
1825	Single-bit re-encryption with applications to distributed proof systems. **2007**,		
1824	Cryptographic Hardware and Embedded Systems - CHES 2007. *Lecture Notes in Computer Science*, **2007**,	0.9	8
1823	D-S Theory-based Trust Model FIRE^+ in Multi-agent Systems. **2007**,		1
1822	Provably secure authenticated group Diffie-Hellman key exchange. **2007**, 10, 10		28
1821	Robust computational secret sharing and a unified account of classical secret-sharing goals. **2007**,		40
1820	Securing RFID Tags: Authentication Protocols with Completeness, Soundness, and Non-Traceability. **2007**,		
1819	Security, Privacy, and Trust in Modern Data Management. **2007**,		12
1818	FPGA Intrinsic PUFs and Their Use for IP Protection. *Lecture Notes in Computer Science*, **2007**, 63-80	0.9	446
1817	Deterministic and Efficiently Searchable Encryption. **2007**, 535-552		358
1816	Public Key Encryption That Allows PIR Queries. *Lecture Notes in Computer Science*, **2007**, 50-67	0.9	107
1815	Protection and Retrieval of Encrypted Multimedia Content: When Cryptography Meets Signal Processing. **2007**, 2007, 1-20		48
1814	Another look at automated theorem-proving. **2007**, 1,		2
1813	The unified theory of pseudorandomness. **2007**, 38, 39-54		13
1812	A Survey of Homomorphic Encryption for Nonspecialists. **2007**, 2007, 1-10		130
1811	Oblivious Neural Network Computing via Homomorphic Encryption. **2007**, 2007, 1-11		27
1810	JDGC. **2007**, 3, 190-204		

1809	Zaps and Their Applications. **2007**, 36, 1513-1543		59
1808	Chosen-Ciphertext Security from Identity-Based Encryption. **2007**, 36, 1301-1328		174
1807	MiniSec: A Secure Sensor Network Communication Architecture. **2007**,		39
1806	Public Key Infrastructure. *Lecture Notes in Computer Science*, **2007**,	0.9	3
1805	Computer Algebra in Scientific Computing. *Lecture Notes in Computer Science*, **2007**,	0.9	2
1804	Mobile and Wireless Network Security and Privacy. **2007**,		3
1803	Introduction to Cryptography. **2007**,		66
1802	Information Security. *Lecture Notes in Computer Science*, **2007**,	0.9	1
1801	Applied Cryptography and Network Security. *Lecture Notes in Computer Science*, **2007**,	0.9	7
1800	Efficient Arguments without Short PCPs. **2007**,		63
1799	Privacy preserving error resilient dna searching through oblivious automata. **2007**,		87
1798	Secure Anonymous Broadcasting in Vehicular Networks. **2007**,		11
1797	Quantifying Privacy for Privacy Preserving Data Mining. **2007**,		2
1796	Gradual Release: Unifying Declassification, Encryption and Key Release Policies. **2007**,		85
1795	A First Step to Provable Security in Block Ciphers against Side Channel Attacks. **2007**,		
1794	Verifying Delivered QoS in Multihop Wireless Networks. **2007**, 6, 1370-1383		3
1793	Compositional Security for Task-PIOAs. **2007**,		2
1792	Protocol Engineering Principles for Cryptographic Protocols Design. **2007**,		

1791	On the Undecidability of Quasi-Private-Key-Encryption Statistical Indistinguishability. **2007**,		
1790	Key-dependent Message Security under Active Attacks--BRSIM/UC-Soundness of Symbolic Encryption with Key Cycles. **2007**,		16
1789	An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks. **2007**, 6, 888-902		49
1788	Anonymous Fingerprinting with Robust QIM Watermarking Techniques. **2007**, 2007, 1-13		18
1787	Selected Areas in Cryptography. *Lecture Notes in Computer Science*, **2007**,	0.9	1
1786	Computational Soundness of Symbolic Analysis for Protocols Using Hash Functions. **2007**, 186, 121-139		2
1785	Privacy-preserving algorithms for distributed mining of frequent itemsets. **2007**, 177, 490-503		53
1784	How to construct secure proxy cryptosystem. **2007**, 177, 4095-4108		5
1783	Resource-aware protocols for authenticated group key exchange in integrated wired and wireless networks. **2007**, 177, 5441-5467		8
1782	Explicit Randomness is not Necessary when Modeling Probabilistic Encryption. **2007**, 186, 49-65		4
1781	Chaotic block iterating method for pseudo-random sequence generator. **2007**, 14, 45-48		5
1780	How to signcrypt a message to designated group. **2007**, 14, 57-63		1
1779	The reactive simulatability (RSIM) framework for asynchronous systems. **2007**, 205, 1685-1720		58
1778	Multirecipient Encryption Schemes: How to Save on Bandwidth and Computation Without Sacrificing Security. **2007**, 53, 3927-3943		35
1777	Formal Proofs for the Security of Signcryption. *Journal of Cryptology*, **2007**, 20, 203-235	2.1	88
1776	Protecting data privacy through hard-to-reverse negative databases. **2007**, 6, 403-415		36
1775	A New Public-Key Encryption Scheme. *Journal of Computer Science and Technology*, **2007**, 22, 95-102	1.7	4
1774	A Protocol for a Private Set-Operation. *Journal of Computer Science and Technology*, **2007**, 22, 822-829	1.7	

1773	On the possibility of practically obfuscating programs towards a unified perspective of code protection. **2007**, 3, 3-21		34
1772	Survey of information security. **2007**, 50, 273-298		38
1771	Sound and complete computational interpretation of symbolic hashes in the standard model. **2008**, 394, 112-133		8
1770	A new framework for the design and analysis of identity-based identification schemes. **2008**, 407, 370-388		10
1769	Semantic security for the McEliece cryptosystem without random oracles. **2008**, 49, 289-305		66
1768	Simpler Session-Key Generation from Short Random Passwords. *Journal of Cryptology*, **2008**, 21, 52-96	2.1	10
1767	Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. *Journal of Cryptology*, **2008**, 21, 469-491	2.1	196
1766	Novel protocols for NP. **2008**, 51, 40-52		
1765	Attribute-based re-encryption scheme in the standard model. **2008**, 13, 621-625		18
1764	Cycling attacks against homomorphic cryptosystems. **2008**, 13, 727-732		
1763	On the security of public key cryptosystems with a double decryption mechanism. **2008**, 108, 279-283		8
1762	Privacy-preserving collaborative data mining. *IEEE Computational Intelligence Magazine*, **2008**, 3, 31-41	5.6	20
1761	Cryptographic Hardness Based on the Decoding of Reedâ€Solomon Codes. **2008**, 54, 2752-2769		20
1760	A cryptographic approach to securely share and query genomic sequences. **2008**, 12, 606-17		86
1759	Private Data Analysis via Output Perturbation. **2008**, 383-414		3
1758	Applied Cryptography and Network Security. *Lecture Notes in Computer Science*, **2008**,	0.9	1
1757	Privacy, Security, and Trust in KDD. **2008**,		2
1756	A Brief History of Provably-Secure Public-Key Encryption. **2008**, 357-370		2

1755	Cryptography and Game Theory: Designing Protocols for Exchanging Information. **2008**, 320-339		82
1754	On the Computational Security of a Distributed Key Distribution Scheme. **2008**, 57, 1087-1097		2
1753	Concurrent Nonmalleable Commitments. **2008**, 37, 1891-1925		24
1752	New and Improved Constructions of Nonmalleable Cryptographic Protocols. **2008**, 38, 702-752		32
1751	A Java Crypto implementation of DNAProvider featuring complexity in theory and practice. **2008**,		3
1750	A forward secure identity based encryption scheme with master key update. **2008**,		
1749	Efficient signature schemes supporting redaction, pseudonymization, and data deidentification. **2008**,		40
1748	Group-based Cryptography. **2008**,		2
1747	Information Hiding. *Lecture Notes in Computer Science*, **2008**,	0.9	1
1746	Provable security of digital signatures in the tamper-proof device model. **2008**, 18,		1
1745	Cryptanalytic Attacks on RSA. **2008**,		1
1744	Formal certification of code-based cryptographic proofs. **2008**,		54
1743	Composition attacks and auxiliary information in data privacy. **2008**,		153
1742	Security analysis of cryptographically controlled access to XML documents. **2008**, 55, 1-29		9
1741	Key-dependent message security under active attacks âBRSIM/UC-soundness of DolevâYao-style encryption with key cycles. **2008**, 16, 497-530		16
1740	Differential Privacy: A Survey of Results. **2008**, 1-19		1056
1739	Generalized ElGamal Public Key Cryptosystem Based on a New Diffie-Hellman Problem. *Lecture Notes in Computer Science*, **2008**, 1-21	0.9	2
1738	Trustworthy Global Computing. *Lecture Notes in Computer Science*, **2008**,	0.9	

1737 A searching-based probabilistic cipher. **2008**, 2008, P11016 1

1736 Deleting index entries from compliance storage. **2008**, 1

1735 Security and Cryptography for Networks. *Lecture Notes in Computer Science*, **2008**, 0.9

1734 An efficient partial key pre-distribution scheme for chain oriented sensor networks. **2008**,

1733 A New ElGamal-Based Algebraic Homomorphism and Its Application. **2008**, 3

1732 The layered games framework for specifications and analysis of security protocols. **2008**, 1, 144 1

1731 Password-based authenticated key establishment for wireless group communications in an ad-hoc mode. **2008**, 1, 398 1

1730 Bibliography. 566-571

1729 Combining Public Key Encryption with Keyword Search and Public Key Encryption. **2009**, E92-D, 888-896 15

1728 Provable Security. *Lecture Notes in Computer Science*, **2009**, 0.9 1

1727 k-Anonymization with Minimal Loss of Information. **2009**, 21, 206-219 54

1726 Techniques for policy enforcement on encrypted network traffic. **2009**,

1725 Provable security of the modified encrypting file system for Microsoft Windows. **2009**,

1724 Cryptography. **2009**, 731

1723 (0)-Secure Message Transmission. **2009**,

1722 Efficient linear filtering of encrypted signals via composite representation. **2009**, 2

1721 A Data Privacy-Oriented Multi-parities Location Collect Scheme in Location Based Services. **2009**, 2

1720 On anonymity in an electronic society. **2009**, 42, 1-35 63

1719	Secure Arithmetic Computation with No Honest Majority. *Lecture Notes in Computer Science*, **2009**, 294-314	0.9	80
1718	Privacy Preserving Risk Assessment of Credit Securities. **2009**,		0
1717	Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima. *Lecture Notes in Computer Science*, **2009**, 1-20	0.9	120
1716	Securing Emerging Wireless Systems. **2009**,		9
1715	Perfect Subliminal Channel in a Paring-Based Digital Signature. **2009**,		
1714	An Efficient Homomorphic Coercion Resistant Voting Scheme Using Hierarchical Binary Search Tree. **2009**,		1
1713	Secure anonymous database search. **2009**,		49
1712	HICCUPS. **2009**,		12
1711	Efficient zero-knowledge identification schemes which respect privacy. **2009**,		11
1710	Inaccessible entropy. **2009**,		19
1709	A unified framework for concurrent security. **2009**,		55
1708	Non-malleability amplification. **2009**,		41
1707	A Complete Public-Key Cryptosystem. **2009**, 1, 1-12		9
1706	Generic Case Complexity and One-Way Functions. **2009**, 1,		
1705	Formal to Practical Security. *Lecture Notes in Computer Science*, **2009**,	0.9	
1704	Leak-free mediated group signatures1. **2009**, 17, 489-514		3
1703	Using Decision Problems in Public Key Cryptography. **2009**, 1,		4
1702	Format-Preserving Encryption. *Lecture Notes in Computer Science*, **2009**, 295-312	0.9	111

1701	A simple construction for public-key encryption with revocable anonymity. **2009**,		1
1700	One-Wayness Equivalent to General Factoring. **2009**, 55, 4249-4262		3
1699	On the Implementation of the Discrete Fourier Transform in the Encrypted Domain. *IEEE Transactions on Information Forensics and Security*, **2009**, 4, 86-97	8	96
1698	Computationally sound implementations of equational theories against passive adversaries. **2009**, 207, 496-520		11
1697	An application of index forms in cryptography. **2009**, 58, 35-45		
1696	Entropic security in quantum cryptography. **2009**, 8, 331-345		10
1695	Cryptography with Constant Input Locality. *Journal of Cryptology*, **2009**, 22, 429-469	2.1	26
1694	New Approaches for Deniable Authentication. *Journal of Cryptology*, **2009**, 22, 572-615	2.1	27
1693	When is a key establishment protocol correct?. *Security and Communication Networks*, **2009**, 2, n/a-n/a	1.9	
1692	Private multiparty sampling and approximation of vector combinations. **2009**, 410, 1730-1745		2
1691	User-private information retrieval based on a peer-to-peer community. **2009**, 68, 1237-1252		44
1690	k-Anonymous data collection. **2009**, 179, 2948-2963		22
1689	Probabilistic Encryption--A Comparative Analysis against RSA and ECC. **2009**,		2
1688	Lattice-based Cryptography. **2009**, 147-191		245
1687	Authentication without Elision: Partially Specified Protocols, Associated Data, and Cryptographic Models Described by Code. **2009**,		9
1686	Chosen-Ciphertext Security via Correlated Products. *Lecture Notes in Computer Science*, **2009**, 419-436	0.9	89
1685	Public-key cryptosystems from the worst-case shortest vector problem. **2009**,		412
1684	Guide to Wireless Sensor Networks. **2009**,		28

1683	Formally Certifying the Security of Digital Signature Schemes. **2009**,		8
1682	Public Key Cryptography âPKC 2009. *Lecture Notes in Computer Science*, **2009**,	0.9	3
1681	Efficient and provably secure aggregation of encrypted data in wireless sensor networks. **2009**, 5, 1-36		194
1680	Financial Cryptography and Data Security. *Lecture Notes in Computer Science*, **2009**,	0.9	2
1679	On the complexity of differentially private data release. **2009**,		144
1678	Cryptology and Network Security. *Lecture Notes in Computer Science*, **2009**,	0.9	
1677	Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs. **2009**, 20, 158-170		24
1676	Improved Group-Oriented Encryption for Group Communication. **2009**,		2
1675	Universally Composable Symmetric Encryption. **2009**,		14
1674	Sender-Side Public Key Deniable Encryption Scheme. **2009**,		6
1673	Bit Encryption Is Complete. **2009**,		38
1672	Protecting RSA against Fault Attacks: The Embedding Method. **2009**,		14
1671	Strengthening Class1 Gen2 RFID tags. **2009**,		
1670	Error-Tolerant Searchable Encryption. **2009**,		32
1669	Secure IP-block distribution for hardware devices. **2009**,		5
1668	A privacy preserving Jaccard similarity function for mining encrypted data. **2009**,		9
1667	h(k)-private information retrieval from privacy-uncooperative queryable databases. **2009**, 33, 720-744		71
1666	Provably Secure Access Authentication Protocol under Universal Network. **2009**,		

1665	Concealed Data Aggregation for Wireless Sensor Networks. **2009**,		1
1664	CCA-Secure Public Key Encryption without Group-Dependent Hash Functions. **2009**, E92-D, 967-970		
1663	Encrypted Domain DCT Based on Homomorphic Cryptosystems. **2009**, 2009, 1-12		12
1662	Formal certification of code-based cryptographic proofs. **2009**, 44, 90-101		57
1661	eSketch. **2010**,		34
1660	Chosen-Ciphertext Security via Correlated Products. **2010**, 39, 3058-3088		25
1659	Fundamental quantitative security in quantum key generation. **2010**, 82,		13
1658	Obfuscation for Cryptographic Purposes. *Journal of Cryptology*, **2010**, 23, 121-168	2.1	26
1657	Efficient privacy-preserving similar document detection. **2010**, 19, 457-475		51
1656	A new hardware-assisted PIR with O(n) shuffle cost. **2010**, 9, 237-252		7
1655	An efficient conversion scheme for enhancing security of Diffie-Hellman-based encryption. **2010**, 15, 415-421		1
1654	Cryptographic transformations of non-shannon sources of information. **2010**, 46, 813-819		1
1653	On server trust in private proxy auctions. **2010**, 10, 291-311		1
1652	Reversible Image Watermarking Using Interpolation Technique. *IEEE Transactions on Information Forensics and Security*, **2010**, 5, 187-193	8	424
1651	Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals. *IEEE Transactions on Information Forensics and Security*, **2010**, 5, 180-187	8	69
1650	A Provably Secure Anonymous BuyerâSeller Watermarking Protocol. *IEEE Transactions on Information Forensics and Security*, **2010**, 5, 920-931	8	38
1649	Quantum Entropic Security and Approximate Quantum Encryption. **2010**, 56, 3455-3464		11
1648	. **2010**, 8, 66-69		6

1647	Towards trustworthy e-voting using paper receipts. **2010**, 32, 305-311		3
1646	Variations on a theme by Akl and Taylor: Security and tradeoffs. **2010**, 411, 213-227		20
1645	Bounds on the efficiency of black-box commitment schemes. **2010**, 411, 1251-1260		1
1644	Effective watermarking scheme in the encrypted domain for buyerâseller watermarking protocol. **2010**, 180, 4672-4684		21
1643	Improvement of one quantum encryption scheme. **2010**,		
1642	Computational indistinguishability logic. **2010**,		20
1641	. **2010**,		4
1640	Cryptanalysis of a fast encryption scheme for databases. **2010**,		
1639	Security analysis for privacy preserving search of multimedia. **2010**,		29
1638	. **2010**,		0
1637	AN EFFICIENT SEVENTH POWER RESIDUE SYMBOL ALGORITHM. **2010**, 06, 1831-1853		6
1636	Information Security and Privacy. *Lecture Notes in Computer Science*, **2010**,	0.9	1
1635	Compressed-encrypted domain JPEG2000 image watermarking. **2010**,		9
1634	Probabilistic Public Key Encryption with Equality Test. *Lecture Notes in Computer Science*, **2010**, 119-131	0.9	103
1633	Secure Data Management. *Lecture Notes in Computer Science*, **2010**,	0.9	
1632	Cryptanalysis of a convertible authenticated encryption scheme based on the ElGamal cryptosystem. **2010**, 27, 266		2
1631	Calibrating the power of schedulers for probabilistic polynomial-time calculus. **2010**, 18, 265-316		
1630	Deciding security properties for cryptographic protocols. application to key cycles. **2010**, 11, 1-42		22

1629	Analysis Techniques for Information Security. **2010**, 2, 1-164		0
1628	Public-key cryptography from different assumptions. **2010**,		50
1627	Computing arbitrary functions of encrypted data. **2010**, 53, 97-105		306
1626	. **2010**, 9, 168-174		84
1625	Financial Cryptography and Data Security. *Lecture Notes in Computer Science*, **2010**,	0.9	0
1624	Topics in Cryptology - CT-RSA 2010. *Lecture Notes in Computer Science*, **2010**,	0.9	3
1623	Resettable Public-Key Encryption: How to Encrypt on a Virtual Machine. *Lecture Notes in Computer Science*, **2010**, 41-56	0.9	23
1622	Information and Communications Security. *Lecture Notes in Computer Science*, **2010**,	0.9	1
1621	How to Take Advantage of Distrusted Parties or Secure Auxiliary Computations for Every Language in NP. **2010**, 19, 160-174		
1620	Toward nanoworld-based secure encryption for enduring data storage. **2010**, 35, 2421-3		2
1619	Secure Routing in Wireless Sensor Networks. **2010**, 553-578		
1618	On the Implementation of Huge Random Objects. **2010**, 39, 2761-2822		16
1617	On the Security of Public-Key Algorithms Based on Chebyshev Polynomials over the Finite Field Z_N. **2010**, 59, 1392-1401		20
1616	Efficient Authentication for Mobile and Pervasive Computing. *Lecture Notes in Computer Science*, **2010**, 186-202	0.9	8
1615	Fully Homomorphic Encryption over the Integers. *Lecture Notes in Computer Science*, **2010**, 24-43	0.9	657
1614	Digital Signatures. **2010**,		52
1613	Information Security and Cryptology. *Lecture Notes in Computer Science*, **2010**,	0.9	
1612	A New Sampling Protocol and Applications to Basing Cryptographic Primitives on the Hardness of NP. **2010**,		9

1611	Provably Secure Nested One-Time Secret Mechanisms for Fast Mutual Authentication and Key Exchange in Mobile Communications. **2010**, 18, 996-1009		9
1610	Robustness Guarantees for Anonymity. **2010**,		1
1609	Secure Information Processing with Privacy Assurance - standard based design and development for biometric applications. **2010**,		0
1608	Design of strong cryptographic schemes based on Latin Squares. **2010**, 13, 233-256		5
1607	Multi-party k-Means Clustering with Privacy Consideration. **2010**,		14
1606	Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions. **2010**,		57
1605	Security for Key Management Interfaces. **2011**,		13
1604	An arbitrary encryption scheme for homomorphic data Migration. **2011**,		
1603	Index based symmetric block encryption. **2011**,		
1602	Computing Blindfolded: New Developments in Fully Homomorphic Encryption. **2011**,		53
1601	Key based bit level genetic cryptographic technique (KBGCT). **2011**,		8
1600	Careful with Composition: Limitations of the Indifferentiability Framework. *Lecture Notes in Computer Science*, **2011**, 487-506	0.9	87
1599	Information Security and Cryptology. *Lecture Notes in Computer Science*, **2011**,	0.9	
1598	Symmetric Searchable Encryption for Database Applications. **2011**,		4
1597	Towards Privacy-Preserving XML Transformation. **2011**,		3
1596	Towards a Game Theoretic View of Secure Computation. *Lecture Notes in Computer Science*, **2011**, 426-445	0.9	43
1595	One-Way Property Proof In Public Key Cryptography Based On Ohnn. **2011**, 15, 1812-1816		1
1594	A New Spin on Quantum Cryptography: Avoiding Trapdoors and Embracing Public Keys. *Lecture Notes in Computer Science*, **2011**, 255-274	0.9	4

1593	A security framework for privacy-preserving data aggregation in wireless sensor networks. **2011**, 7, 1-45		24
1592	A firm foundation for private data analysis. **2011**, 54, 86-95		408
1591	The Promise of Differential Privacy: A Tutorial on Algorithmic Techniques. **2011**,		16
1590	Privacy-preserving activity scheduling on mobile devices. **2011**,		5
1589	Lossy Trapdoor Functions and Their Applications. **2011**, 40, 1803-1844		89
1588	An Overview on Privacy Preserving Biometrics. **2011**,		5
1587	sSCADA: securing SCADA infrastructure communications. **2011**, 6, 59		15
1586	Efficient provably-secure hierarchical key assignment schemes. **2011**, 412, 5684-5699		22
1585	Provable Security in the Real World. **2011**, 9, 33-41		19
1584	$hbox{EP}^{2}hbox{DF}$: An Efficient Privacy-Preserving Data-Forwarding Scheme for Service-Oriented Vehicular Ad Hoc Networks. **2011**, 60, 580-591		17
1583	A Privacy-Preserving Buyerâ Seller Watermarking Protocol Based on Priced Oblivious Transfer. *IEEE Transactions on Information Forensics and Security*, **2011**, 6, 202-212	8	26
1582	On the Security of Randomized Arithmetic Codes Against Ciphertext-Only Attacks. *IEEE Transactions on Information Forensics and Security*, **2011**, 6, 19-27	8	19
1581	. **2011**, 57, 6428-6443		244
1580	Efficient defence against misbehaving TCP receiver DoS attacks. **2011**, 55, 3904-3914		4
1579	Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting. *Lecture Notes in Computer Science*, **2011**, 543-560	0.9	48
1578	More on Average Case vs Approximation Complexity. **2011**, 20, 755-786		21
1577	A general and efficient countermeasure to relation attacks in mix-based e-voting. **2011**, 10, 49-60		8
1576	Cryptographically sound security proofs for basic and public-key Kerberos. **2011**, 10, 107-134		7

1575	Universally Composable Symbolic Security Analysis. *Journal of Cryptology*, **2011**, 24, 83-147	2.1	14
1574	Short Undeniable Signatures Based on Group Homomorphisms. *Journal of Cryptology*, **2011**, 24, 545-587	2.1	4
1573	Securely Obfuscating Re-Encryption. *Journal of Cryptology*, **2011**, 24, 694-719	2.1	35
1572	Message-aimed side channel and fault attacks against public key cryptosystems with homomorphic properties. **2011**, 1, 283-292		3
1571	Identification with encrypted biometric data. *Security and Communication Networks*, **2011**, 4, 548-562	1.9	29
1570	An efficient and provably secure public key encryption scheme based on coding theory. *Security and Communication Networks*, **2011**, 4, 1440-1447	1.9	5
1569	Privacy preservation with X.509 standard certificates. **2011**, 181, 2906-2921		14
1568	Discrete logarithm based additively homomorphic encryption and secure data aggregation. **2011**, 181, 3308-3322		16
1567	k-out-of-n oblivious transfer based on homomorphic encryption and solvability of linear equations. **2011**,		3
1566	Extracting and verifying cryptographic models from C protocol code by symbolic execution. **2011**,		22
1565	Implementation of the discrete wavelet transform and multiresolution analysis in the encrypted domain. **2011**,		14
1564	Relations among privacy notions. **2011**, 14, 1-24		15
1563	. **2011**,		1
1562	Learning Whom to Trust in a Privacy-Friendly Way. **2011**,		3
1561	A Secure Multi-Party Protocol for Sharing Valuable Information in Public Safety Networks. **2011**,		
1560	On Constructing Homomorphic Encryption Schemes from Coding Theory. *Lecture Notes in Computer Science*, **2011**, 23-40	0.9	7
1559	Privacy preservation schemes for querying wireless sensor networks. **2011**,		5
1558	Security notions for information theoretically secure encryptions. **2011**,		9

1557	Secret Sharing in the Encrypted Domain with Secure Comparison. **2011**,		1
1556	A new proxy signcryption scheme using warrants. **2011**, 1, 309		2
1555	Functional Encryption: Definitions and Challenges. *Lecture Notes in Computer Science*, **2011**, 253-273	0.9	426
1554	A New Paradigm to Approximate Oblivious Data Processing (ODP) for Data Confidentiality in Cloud Computing. **2011**,		2
1553	A privacy-preserving broadcast encryption scheme with revocability. **2011**,		
1552	Efficiently computing private recommendations. **2011**,		18
1551	From Chaos to Secret Key Agreement. **2011**,		
1550	Key dependent message security. **2011**,		2
1549	Non-interactive distributed encryption. **2011**,		4
1548	Verified security of redundancy-free encryption from Rabin and RSA. **2012**,		4
1547	A Parallel Repetition Theorem for Constant-Round Arthur-Merlin Proofs. **2012**, 4, 1-22		4
1546	Pseudorandomness and derandomization. **2012**, 18, 27-31		1
1545	IMPROVEMENT OF ONE QUANTUM ENCRYPTION SCHEME. **2012**, 10, 1250076		2
1544	Computational verification of C protocol implementations by symbolic execution. **2012**,		16
1543	Collusion-resistant outsourcing of private set intersection. **2012**,		25
1542	Practical yet universally composable two-server password-authenticated secret sharing. **2012**,		29
1541	On beating the hybrid argument. **2012**,		2
1540	Privacy-aware personalization for mobile advertising. **2012**,		26

1539	Characterizing pseudoentropy and simplifying pseudorandom generator constructions. **2012**,		24
1538	Homomorphism Encryption Algorithm for Elementary Operations over Real Number Domain. **2012**,		1
1537	A novel self-certified security access authentication protocol in the space network. **2012**,		
1536	Efficient anonymous message submission. **2012**,		
1535	Characterizing pseudoentropy. **2012**,		4
1534	Cloud Storage-oriented Secure Information Gateway. **2012**,		1
1533	Foundations and Practice of Security. *Lecture Notes in Computer Science*, **2012**,	0.9	3
1532	Automation in Computer-Aided Cryptography: Proofs, Attacks and Designs. *Lecture Notes in Computer Science*, **2012**, 7-8	0.9	1
1531	PRIVACY-PRESERVING OLAP FOR ACCURATE ANSWER. **2012**, 21, 1250009		1
1530	Probabilistic Relational Hoare Logics for Computer-Aided Security Proofs. *Lecture Notes in Computer Science*, **2012**, 1-6	0.9	8
1529	Symbolic Analysis of Cryptographic Protocols Containing Bilinear Pairings. **2012**,		8
1528	A special purpose integer factorization algorithm. **2012**,		0
1527	A Network Identity Authentication Protocol Based on Fingerprint and Probabilistic Encryption of RSA. **2012**, 241-244, 2471-2474		
1526	References. **2012**, 420-454		
1525	WITHDRAWN: The 2010 Benjamin franklin medal in computer and cognitive science present to Shafrira Goldwasser. **2012**,		
1524	Survey of Key Dependent Message (KDM) Security. **2012**, 6, 26-36		
1523	Deterministic Public Key Encryption and Identity-Based Encryption from Lattices in the Auxiliary-Input Setting. *Lecture Notes in Computer Science*, **2012**, 1-18	0.9	18
1522	Public-Key Cryptosystems Resilient to Key Leakage. **2012**, 41, 772-814		59

1521	On detecting pollution attacks in inter-session network coding. **2012**,		11
1520	Encryption algorithm based on higher degree residues oriented to semantic security. **2012**,		
1519	Risk assessment of credit securities: The notion and the issues. **2012**,		
1518	Cryptanalysis and Improvement of an Efficient CCA Secure PKE Scheme. **2012**,		
1517	Privacy-preserving path-inclusion protocol through oblivious automata. **2012**,		2
1516	Deniably Information-Hiding Encryptions Secure against Adaptive Chosen Ciphertext Attack. **2012**,		2
1515	A CCA2 Secure Variant of the McEliece Cryptosystem. **2012**, 58, 6672-6680		17
1514	A secure and privacy-preserving communication scheme for Advanced Metering Infrastructure. **2012**,		6
1513	Cryptographic framework for analyzing the privacy of recommender algorithms. **2012**,		2
1512	PCLA: A new public-key cryptosystem based on logarithmic approach. **2012**,		1
1511	Semantic Security for the Wiretap Channel. *Lecture Notes in Computer Science*, **2012**, 294-311	0.9	69
1510	Secure Identity-Based Encryption in the Quantum Random Oracle Model. *Lecture Notes in Computer Science*, **2012**, 758-775	0.9	81
1509	Black-Box Constructions of Composable Protocols without Set-Up. *Lecture Notes in Computer Science*, **2012**, 461-478	0.9	26
1508	. **2012**, 14, 703-716		73
1507	Tightly Secure Signatures and Public-Key Encryption. *Lecture Notes in Computer Science*, **2012**, 590-607	0.9	101
1506	Lossy trapdoor functions from homomorphic reproducible encryption. **2012**, 112, 794-798		3
1505	An efficient IND-CCA2 secure Paillier-based cryptosystem. **2012**, 112, 885-888		13
1504	Pseudorandomness. **2012**, 7, 1-336		118

1503	Mechanism design and communication networks. **2012**, 7, 489-533		7
1502	Introduction of Cryptographic Protocols. **2012**, 1-12		1
1501	Engineering Principles for Security Design of Protocols. **2012**, 41-81		
1500	Computer-Aided Cryptographic Proofs. *Lecture Notes in Computer Science*, **2012**, 11-27	0.9	7
1499	A commutative encryption scheme based on ElGamal encryption. **2012**,		14
1498	Usable, Secure, Private Search. **2012**, 10, 53-60		19
1497	Information Security and Cryptology - ICISC 2011. *Lecture Notes in Computer Science*, **2012**,	0.9	
1496	Verified Indifferentiable Hashing into Elliptic Curves. *Lecture Notes in Computer Science*, **2012**, 209-228	0.9	9
1495	Information Theoretic Security. *Lecture Notes in Computer Science*, **2012**,	0.9	1
1494	. **2012**,		
1493	On the (im)possibility of obfuscating programs. **2012**, 59, 1-48		256
1492	Trust and Trustworthy Computing. *Lecture Notes in Computer Science*, **2012**,	0.9	2
1491	Cryptology and Network Security. *Lecture Notes in Computer Science*, **2012**,	0.9	3
1490	Fast Software Encryption. *Lecture Notes in Computer Science*, **2012**,	0.9	2
1489	Static Analysis. *Lecture Notes in Computer Science*, **2012**,	0.9	2
1488	Private Fingerprint Matching. *Lecture Notes in Computer Science*, **2012**, 426-433	0.9	16
1487	Trusted Systems. *Lecture Notes in Computer Science*, **2012**,	0.9	
1486	Generation of Cryptographic Keys from Personal Biometrics: An Illustration Based on Fingerprints. **2012**,		1

1485	Circular and KDM Security for Identity-Based Encryption. *Lecture Notes in Computer Science*, **2012**, 334-352	0.9	40
1484	A Thirty Year Old Conjecture about Promise Problems. *Lecture Notes in Computer Science*, **2012**, 473-484	0.9	3
1483	On Homomorphic Encryption and Chosen-Ciphertext Security. *Lecture Notes in Computer Science*, **2012**, 52-65	0.9	8
1482	An efficient key-management scheme for hierarchical access control in e-medicine system. **2012**, 36, 2325-37		47
1481	Turing und Kryptografie. **2012**, 35, 261-270		1
1480	On the Security of Key-Based Interval Splitting Arithmetic Coding With Respect to Message Indistinguishability. *IEEE Transactions on Information Forensics and Security*, **2012**, 7, 895-903	8	6
1479	Embedding edit distance to enable private keyword search. **2012**, 2,		8
1478	Smooth Projective Hashing and Two-Message Oblivious Transfer. *Journal of Cryptology*, **2012**, 25, 158-193	2.1	63
1477	Provably-Secure Time-Bound Hierarchical Key Assignment Schemes. *Journal of Cryptology*, **2012**, 25, 243-270	2.1	37
1476	Efficient Set Operations in the Presence of Malicious Adversaries. *Journal of Cryptology*, **2012**, 25, 383-433	2.1	35
1475	Computational Indistinguishability Between Quantum States and Its Cryptographic Application. *Journal of Cryptology*, **2012**, 25, 528-555	2.1	16
1474	Efficient chosen ciphertext secure public-key encryption under factoring assumption. *Security and Communication Networks*, **2013**, 6, 351-360	1.9	2
1473	On the Analysis of Cryptographic Assumptions in the Generic Ring Model. *Journal of Cryptology*, **2013**, 26, 225-245	2.1	6
1472	Public-Coin Parallel Zero-Knowledge for NP. *Journal of Cryptology*, **2013**, 26, 1-10	2.1	16
1471	Secure Integration of Asymmetric and Symmetric Encryption Schemes. *Journal of Cryptology*, **2013**, 26, 80-101	2.1	155
1470	Practical Chosen Ciphertext Secure Encryption from Factoring. *Journal of Cryptology*, **2013**, 26, 102-118	2.1	17
1469	Information Security and Privacy. *Lecture Notes in Computer Science*, **2013**,	0.9	
1468	Security and Privacy in Biometrics. **2013**,		51

1467	A Probabilistic Encryption Based MIN/MAX Computation in Wireless Sensor Networks. **2013**,		6
1466	Toward a taxonomy of communications security models. **2013**, 3, 181-195		1
1465	Quantum Attacks on Public-Key Cryptosystems. **2013**,		14
1464	Cloud computing in cryptography and steganography. **2013**, 49, 584-588		6
1463	A new model for privacy preserving multiparty collaborative data mining. **2013**,		
1462	Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing. **2013**, 66, 1687-1706		32
1461	IK-CPA security implies IE-CCA security in the random oracle model. **2013**, 56, 1-11		2
1460	Cryptography and Coding. *Lecture Notes in Computer Science*, **2013**,	0.9	
1459	Fully Homomorphic Encryption Using Hidden Ideal Lattice. *IEEE Transactions on Information Forensics and Security*, **2013**, 8, 2127-2137	8	29
1458	MrCrypt. **2013**,		31
1457	Decision and Game Theory for Security. *Lecture Notes in Computer Science*, **2013**,	0.9	1
1456	Introduction to Cryptography with Maple. **2013**,		3
1455	Security and Trust Management. *Lecture Notes in Computer Science*, **2013**,	0.9	0
1454	An efficient CCA-secure cryptosystem over ideal lattices from identity-based encryption. **2013**, 65, 1254-1263		4
1453	A privacy-aware reputation-based announcement scheme for VANETs. **2013**,		11
1452	Detect Zero by Using Symmetric Homomorphic Encryption. **2013**,		
1451	Bounds on inference. **2013**,		22
1450	Computational Semantics of a Verification Logic of Local Sessions. **2013**,		

1449	Towards secure mobile cloud computing: A survey. **2013**, 29, 1278-1299		222
1448	Privacy and verifiability in voting systems: Methods, developments and trends. **2013**, 10, 1-30		16
1447	. **2013**, 12, 248-260		38
1446	Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain. **2013**, 22, 2455-68		67
1445	Enhancements of Trapdoor Permutations. *Journal of Cryptology*, **2013**, 26, 484-512	2.1	22
1444	Fully Leakage-Resilient Signatures. *Journal of Cryptology*, **2013**, 26, 513-558	2.1	28
1443	Group homomorphic encryption: characterizations, impossibility results, and applications. **2013**, 67, 209-232		19
1442	. **2013**,		12
1441	Key privacy and anonymous protocols. **2013**,		
1440	Single-Database Private Information Retrieval from Fully Homomorphic Encryption. **2013**, 25, 1125-1134		46
1439	On the Circular Security of Bit-Encryption. *Lecture Notes in Computer Science*, **2013**, 579-598	0.9	30
1438	SplitX. **2013**,		13
1437	Fully automated analysis of padding-based encryption in the computational model. **2013**,		23
1436	Certified computer-aided cryptography. **2013**,		26
1435	Verified indifferentiable hashing into elliptic curves. **2013**, 21, 881-917		2
1434	Short blind signatures. **2013**, 21, 627-661		11
1433	Black-box construction of a more than non-malleable CCA1 encryption scheme from plaintext awareness1. **2013**, 21, 721-748		
1432	Private Database Queries Using Somewhat Homomorphic Encryption. *Lecture Notes in Computer Science*, **2013**, 102-118	0.9	73

1431	An efficient image homomorphic encryption scheme with small ciphertext expansion. **2013**,		20
1430	Amplification of Chosen-Ciphertext Security. *Lecture Notes in Computer Science*, **2013**, 503-519	0.9	16
1429	Security Engineering and Intelligence Informatics. *Lecture Notes in Computer Science*, **2013**,	0.9	0
1428	A fast additively symmetric homomorphic encryption scheme for vector data. **2013**,		
1427	ICDM: An Encryption That Supports Unlimited Times Homomorphic Arithmetic Operations on Encrypted Data. **2013**,		
1426	Witness encryption and its applications. **2013**,		147
1425	Private Information Retrieval. **2013**, 4, 1-114		5
1424	. **2013**, 30, 62-74		27
1423	Verifiable and Anonymous Encryption in Asymmetric Bilinear Maps. **2013**,		
1422	. **2013**,		15
1421	Strong Forward Security in Identity-Based Signcryption. **2013**, 16, 235-258		2
1420	SplitX. **2013**, 43, 315-326		6
1419	MrCrypt. **2013**, 48, 271-286		20
1418	Query-biased preview over outsourced and encrypted data. **2013**, 2013, 860621		2
1417	Homomorphic Encryption â Theory and Application. **2013**,		15
1416	A survey of noninteractive zero knowledge proof system and its applications. **2014**, 2014, 560484		6
1415	NTRU cryptosystem: Recent developments and emerging mathematical problems in finite polynomial rings. **2014**, 179-212		4
1414	Distributed Key Generation for Encrypted Deduplication. **2014**,		33

1413	Fast key generation for Gentry-style homomorphic encryption. **2014**, 21, 37-44		2
1412	On Minimal Assumptions for Sender-Deniable Public Key Encryption. *Lecture Notes in Computer Science*, **2014**, 574-591	0.9	6
1411	Explicit capacity-achieving coding scheme for the Gaussian wiretap channel. **2014**,		19
1410	. **2014**, 13, 6670-6683		11
1409	How to use indistinguishability obfuscation. **2014**,		324
1408	LUT based secure cloud computing â An implementation using FPGAs. **2014**,		
1407	Effectiveness of Fully Homomorphic Encryption to Preserve the Privacy of Biometric Data. **2014**,		5
1406	Authentication in Insecure Environments. **2014**,		3
1405	Network-level privacy for hosted cloud services. **2014**,		1
1404	On coinductive equivalences for higher-order probabilistic functional programs. **2014**,		22
1403	Cryptogenography. **2014**,		4
1402	Redactable Signature Schemes for Trees with Signer-Controlled Non-Leaf-Redactions. **2014**, 155-171		7
1401	Lattice based secure data transmission in MANETs. **2014**,		2
1400	The truth behind the myth of the folk theorem. **2014**,		4
1399	A New Additive Homomorphic Encryption based on the co-ACD Problem. **2014**,		7
1398	Blind Seer: A Scalable Private DBMS. **2014**,		130
1397	POLA: A privacy-preserving protocol for location-based real-time advertising. **2014**,		2
1396	A fully secure identity-based encryption scheme against chosen-ciphertext attack. **2014**,		

1395	Modeling Diffie-Hellman Derivability for Automated Analysis. **2014**,		1
1394	Financial Cryptography and Data Security. *Lecture Notes in Computer Science*, **2014**,	0.9	2
1393	Post-Quantum Cryptography. *Lecture Notes in Computer Science*, **2014**,	0.9	8
1392	Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks. **2014**, 75, 192-211		27
1391	A Survey on Zero-Knowledge Proofs. **2014**, 25-69		4
1390	Homomorphic Encryption and Applications. **2014**,		46
1389	Private-by-Design Advertising Meets the Real World. **2014**,		7
1388	Fully secure constructions of spatial encryption with vector privacy. **2014**, 27, 4307-4327		
1387	Code-Based Public-Key Encryption. **2014**, 47-55		2
1386	Secure Multimedia Big Data Sharing in Social Networks Using Fingerprinting and Encryption in the JPEG2000 Compressed Domain. **2014**,		8
1385	Security of Symmetric Encryption against Mass Surveillance. *Lecture Notes in Computer Science*, **2014**, 1-19	0.9	84
1384	A Secure Data Deduplication Scheme for Cloud Storage. *Lecture Notes in Computer Science*, **2014**, 99-118	0.9	58
1383	Large Universe Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability. *Lecture Notes in Computer Science*, **2014**, 55-72	0.9	41
1382	Bandwidth Efficient PIR from NTRU. *Lecture Notes in Computer Science*, **2014**, 195-207	0.9	13
1381	Leakage-Flexible CCA-secure Public-Key Encryption: Simple Construction and Free of Pairing. *Lecture Notes in Computer Science*, **2014**, 19-36	0.9	17
1380	Privacy-preserving restricted boltzmann machine. **2014**, 2014, 138498		
1379	. **2014**,		15
1378	Efficient Authentication for Mobile and Pervasive Computing. **2014**, 13, 469-481		19

1377	Key-Dependent Message Security: Generic Amplification and Completeness. *Journal of Cryptology*, **2014**, 27, 429-451	2.1	18
1376	Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting. *Journal of Cryptology*, **2014**, 27, 210-247	2.1	8
1375	Security Models and Proof Strategies for Plaintext-Aware Encryption. *Journal of Cryptology*, **2014**, 27, 139-180	2.1	3
1374	Formal verification of security protocol implementations: a survey. **2014**, 26, 99-123		27
1373	On private Hamming distance computation. **2014**, 69, 1123-1138		2
1372	Multi-party trust computation in decentralized environments in the presence of malicious adversaries. **2014**, 15, 53-66		29
1371	Paillier-based publicly verifiable (non-interactive) secret sharing. **2014**, 73, 529-546		5
1370	Categories and Types in Logic, Language, and Physics. *Lecture Notes in Computer Science*, **2014**,	0.9	
1369	Authenticated Encryption: Toward Next-Generation Algorithms. **2014**, 12, 70-72		13
1368	A New Payment System for Enhancing Location Privacy of Electric Vehicles. **2014**, 63, 3-18		55
1367	(Leveled) Fully Homomorphic Encryption without Bootstrapping. **2014**, 6, 1-36		319
1366	Cryptology and Network Security. *Lecture Notes in Computer Science*, **2014**,	0.9	0
1365	A new symmetric probabilistic encryption scheme based on random numbers. **2014**,		3
1364	An efficient and practical public key cryptosystem with CCA-security on standard model. **2014**, 19, 486-495		2
1363	. **2014**, 63, 204-217		2
1362	Separation of Reliability and Secrecy in Rate-Limited Secret-Key Generation. **2014**, 60, 4941-4957		26
1361	A Mathematical Approach to Research Problems of Science and Technology. **2014**,		0
1360	Homomorphic encryption in the cloud. **2014**,		18

1359	Semantically Secure Lattice Codes for the Gaussian Wiretap Channel. **2014**, 60, 6399-6416		86
1358	Data and Applications Security and Privacy XXVIII. *Lecture Notes in Computer Science*, **2014**,	0.9	2
1357	Confidentiality-Preserving Image Search: A Comparative Study Between Homomorphic Encryption and Distance-Preserving Randomization. *IEEE Access*, **2014**, 2, 125-141	3.5	51
1356	Construction of a key-dependent message secure symmetric encryption scheme in the ideal cipher model. **2014**, 8, 469-477		
1355	Theoretical Aspects of Computing â□CTAC 2014. *Lecture Notes in Computer Science*, **2014**,	0.9	
1354	The 2010 Benjamin Franklin medal in Computer and Cognitive Science presented to Shafrira Goldwasser, Ph.D.. **2014**, 351, 12-16		
1353	Timed encryption with application to deniable key exchange. **2014**, 560, 172-189		4
1352	Differential Privacy: A Cryptographic Approach to Private Data Analysis. 296-322		7
1351	Efficient and Secure File Deduplication in Cloud Storage. **2014**, E97.D, 184-197		5
1350	Anonymous broadcast encryption with an untrusted gateway. **2014**, 9, 20		
1349	Privacy Protection in the Internet of Things Based on Cryptography. **2015**, 713-715, 2462-2466		
1348	Quantifying information flow in cryptographic systems. **2015**, 25, 457-479		2
1347	A security framework for military application on infrastructure based wireless sensor network. **2015**,		14
1346	Security and privacy protocols for perceptual image hashing. **2015**, 17, 146		7
1345	New Circular Security Counterexamples from Decision Linear and Learning with Errors. *Lecture Notes in Computer Science*, **2015**, 776-800	0.9	14
1344	References. **2015**, 675-741		
1343	Privacy-preserving search for chemical compound databases. **2015**, 16 Suppl 18, S6		8
1342	New method of key-dependent message security for asymmetric encryption. *Security and Communication Networks*, **2015**, 8, 2157-2170	1.9	

1341	New methods for public key cryptosystems based on XTR. *Security and Communication Networks*, **2015**, 8, 3682-3689	1.9	3
1340	A novel CPA-secure hybrid encryption scheme based-on pNE cryptosystem. **2015**,		
1339	Secure Mobile Agent from Leakage-Resilient Proxy Signatures. **2015**, 2015, 1-12		0
1338	. **2015**, 21,		
1337	New Construction of PVPKE Scheme and Its Application in Information Systems and Mobile Communication. **2015**, 2015, 1-10		
1336	The challenges facing physical layer security. **2015**, 53, 16-20		150
1335	. **2015**, 61, 3901-3911		31
1334	Research on Uniformity Based on the Chebyshev Chaotic Map. **2015**,		1
1333	Research on Equivalence between Address Resolution and Duplicate Address Detection. **2015**,		1
1332	Wiretap channel with finite-rate feedback. **2015**,		
1331	Group anonymous D2D communication with end-to-end security in LTE-A. **2015**,		7
1330	A Scalable Multiparty Private Set Intersection. *Lecture Notes in Computer Science*, **2015**, 376-385	0.9	7
1329	Efficient and scalable aggregate signcryption scheme based on multi-trapdoor hash functions. **2015** ,		1
1328	A True Random Number Generator algorithm from digital camera image noise for varying lighting conditions. **2015**,		3
1327	Hierarchical and Shared Access Control. *IEEE Transactions on Information Forensics and Security*, **2015**, 1-1	8	9
1326	Indistinguishability Obfuscation from the Multilinear Subgroup Elimination Assumption. **2015**,		68
1325	Maximal correlation secrecy. **2015**,		3
1324	Metric reasoning about □terms: The affine case. **2015**,		6

1323	Using Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data. **2015**,		62
1322	Quantum Computational Number Theory. **2015**,		7
1321	Sound Proof of Proximity of Knowledge. *Lecture Notes in Computer Science*, **2015**, 105-126	0.9	10
1320	Privacy-preserving biometrics authentication systems using fully homomorphic encryption. **2015**, 11, 151-168		10
1319	THRIVE: threshold homomorphic encryption based secure and privacy preserving biometric verification system. **2015**, 2015,		13
1318	On Privacy for RFID. *Lecture Notes in Computer Science*, **2015**, 3-20	0.9	5
1317	Highly scalable verifiable encrypted search. **2015**,		1
1316	A Medical Healthcare System for Privacy Protection Based on IoT. **2015**,		35
1315	Provably secure public key cryptosystem with limited number of encryptions for authorised sharing of outsourced data. **2015**, 4, 317		1
1314	Information Security. *Lecture Notes in Computer Science*, **2015**,	0.9	
1313	CRT based somewhat homomorphic encryption over the integers. **2015**,		
1312	. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 152-167	8	61
1311	Low-Energy Security: Limits and Opportunities in the Internet of Things. **2015**, 13, 14-21		143
1310	On Security in Publish/Subscribe Services: A Survey. **2015**, 17, 966-997		39
1309	Arithmetic Cryptography. **2015**,		10
1308	Cryptanalysis of a new image alternate encryption algorithm based on chaotic map. **2015**, 80, 1483-1491		48
1307	On statistical distance based testing of pseudo random sequences and experiments with PHP and Debian OpenSSL. **2015**, 53, 44-64		10
1306	Two-Round Password-Only Authenticated Key Exchange in the Three-Party Setting. **2015**, 7, 105-124		6

1305	Improved Tampering Detection for Image Authentication Based on Image Partitioning. **2015**, 84, 69-85		2
1304	Secure watermarking scheme against watermark attacks in the encrypted domain. **2015**, 30, 125-135		61
1303	Anonymous protocols: Notions and equivalence. **2015**, 581, 9-25		1
1302	Spreading Alerts Quietly and the Subgroup Escape Problem. *Journal of Cryptology*, **2015**, 28, 796-819	2.1	2
1301	White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 1274-1288	8	124
1300	Function Secret Sharing. *Lecture Notes in Computer Science*, **2015**, 337-367	0.9	88
1299	Fully Homomorphic Encryption: Cryptography's holy grail. **2015**, 21, 24-29		8
1298	Topics in Cryptology â CT-RSA 2015. *Lecture Notes in Computer Science*, **2015**,	0.9	2
1297	A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 1052-1063	8	37
1296	Information Theoretic Security. *Lecture Notes in Computer Science*, **2015**,	0.9	
1295	Formal security proofs with minimal fuss: Implicit computational complexity at work. **2015**, 241, 96-113		2
1294	Introduction to Cryptography. **2015**,		18
1293	On Applicative Similarity, Sequentiality, and Full Abstraction. *Lecture Notes in Computer Science*, **2015**, 65-82	0.9	6
1292	Policy Privacy in Cryptographic Access Control. **2015**,		8
1291	Ambiguous Multi-Symmetric Cryptography. **2015**,		2
1290	Constant-Round Nonmalleable Commitments from Any One-Way Function. **2015**, 62, 1-30		9
1289	Another Look at Secure Big Data Processing: Formal Framework and a Potential Approach. **2015**,		1
1288	Concatenated codes using Reedâ Muller codes and bit-extension codes for a wiretap channel. **2015**, 9, 1437-1441		0

1287	Secure identity-based encryption in the quantum random oracle model. **2015**, 13, 1550014		15
1286	Modular Order-Preserving Encryption, Revisited. **2015**,		31
1285	An encrypted image editing scheme based on homomorphic encryption. **2015**,		3
1284	A Mechanized Proof of Security for Searchable Symmetric Encryption. **2015**,		5
1283	. **2015**, 103, 1781-1795		25
1282	Error-Control Coding for Physical-Layer Secrecy. **2015**, 103, 1725-1746		61
1281	Network and System Security. *Lecture Notes in Computer Science*, **2015**,	0.9	1
1280	Homomorphic Data Isolation for Hardware Trojan Protection. **2015**,		3
1279	Observing and Preventing Leakage in MapReduce. **2015**,		33
1278	Practical key-dependent message chosen-ciphertext security based on decisional composite residuosity and quadratic residuosity assumptions. *Security and Communication Networks*, **2015**, 8, 1525-1536	1.9	
1277	Implementing public-key cryptography on passive RFID tags is practical. **2015**, 14, 85-99		27
1276	A Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy. *Journal of Cryptology*, **2015**, 28, 671-717	2.1	11
1275	Subtleties in the Definition of IND-CCA: When and How Should Challenge Decryption Be Disallowed?. *Journal of Cryptology*, **2015**, 28, 29-48	2.1	25
1274	Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment. **2015**, 12, 428-442		276
1273	Secure support vector machines outsourcing with random linear transformation. **2015**, 44, 147-176		8
1272	Publicly evaluable pseudorandom functions and their applications. **2016**, 24, 289-320		1
1271	Formal Security-Proved Mobile Anonymous Authentication Protocols with Credit-Based Chargeability and Controllable Privacy. *Applied Sciences (Switzerland)*, **2016**, 6, 176	2.6	
1270	Efficient homomorphic encryption using ECC-elgamal scheme for cloud data. **2016**,		1

1269	. **2016**, 59,		2
1268	Information Extraction Under Privacy Constraints. **2016**, 7, 15		25
1267	Generic transformations for existentially unforgeable signature schemes in the bounded leakage model. *Security and Communication Networks*, **2016**, 9, 1829-1842	1.9	9
1266	Semantic Security and Key-Privacy with Random Split of St-Gen Codes. *Lecture Notes in Computer Science*, **2016**, 105-114	0.9	
1265	Content-Based Encryption. *Lecture Notes in Computer Science*, **2016**, 57-72	0.9	1
1264	Separations in circular security for arbitrary length key cycles, revisited. *Security and Communication Networks*, **2016**, 9, 5392-5400	1.9	1
1263	Privacy-Preserving Spectrum Query with Location Proofs in Database-Driven CRNs. **2016**,		2
1262	Semantic-security capacity for wiretap channels of type II. **2016**,		4
1261	Efficient private subset computation. *Security and Communication Networks*, **2016**, 9, 5965-5976	1.9	4
1260	Secure Shortest Path Search over Encrypted Graph Supporting Synonym Query in Cloud Computing. **2016**,		2
1259	Server-assisted fully homomorphic computation protocols. **2016**,		
1258	Arbitrarily Varying Wiretap Channels With Type Constrained States. **2016**, 62, 7216-7244		26
1257	Authenticated encryption: how reordering can impact performance. *Security and Communication Networks*, **2016**, 9, 6173-6188	1.9	
1256	Implementation of Fixed-Length Template Protection Based on Homomorphic Encryption with Application to Signature Biometrics. **2016**,		8
1255	Practice-Oriented Provable Security and the Social Construction of Cryptography. **2016**, 14, 10-17		2
1254	Relations between robustness and RKA security under public-key encryption. **2016**, 628, 78-91		2
1253	Secure ElGamal-Type Cryptosystems Without Message Encoding. *Lecture Notes in Computer Science* , **2016**, 470-478	0.9	
1252	Privacy-Enhancing Aggregation Techniques for Smart Grid Communications. **2016**,		20

1251	Homomorphic Public Key Encryption Techniques. **2016**, 13-40		1
1250	Einf□rung in die Kryptographie. **2016**,		17
1249	A semantically secure public key cryptoscheme using bit-pair shadows. **2016**, 654, 113-127		
1248	Private Over-Threshold Aggregation Protocols over Distributed Datasets. **2016**, 28, 2467-2479		2
1247	Cryptoleq: A Heterogeneous Abstract Machine for Encrypted and Unencrypted Computation. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 2123-2138	8	11
1246	The New Codebreakers. *Lecture Notes in Computer Science*, **2016**,	0.9	2
1245	Homomorphic Encryption for Security of Cloud Data. **2016**, 79, 175-181		41
1244	. **2016**,		41
1243	Tightly CCA-Secure Encryption Without Pairings. *Lecture Notes in Computer Science*, **2016**, 1-27	0.9	64
1242	Nonce-Based Cryptography: Retaining Security When Randomness Fails. *Lecture Notes in Computer Science*, **2016**, 729-757	0.9	9
1241	Concealed data aggregation in wireless sensor networks: A comprehensive survey. **2016**, 103, 207-227		17
1240	Hiding secrets in software. **2016**, 59, 113-120		5
1239	Efficient and Secure Storage for Outsourced Data: A Survey. **2016**, 1, 178-188		10
1238	Threeâ□ Compromised Too: Circular Insecurity for Any Cycle Length from (Ring-)LWE. *Lecture Notes in Computer Science*, **2016**, 659-680	0.9	12
1237	Secure Software Licensing: Models, Constructions, and Proofs. **2016**,		2
1236	Multiterminal Secrecy by Public Discussion. **2016**, 13, 129-275		13
1235	? Cryptographic Key Management for Data Protection. **2016**, 161-166		
1234	Security of Identity-Based Encryption Schemes from Quadratic Residues. *Lecture Notes in Computer Science*, **2016**, 63-77	0.9	2

1233	Private and Scalable Execution of SQL Aggregates on a Secure Decentralized Architecture. **2016**, 41, 1-43		10
1232	Semantic-Security Capacity for the Physical Layer via Information Theory. **2016**,		0
1231	Naor-Yung Paradigm with Shared Randomness and Applications. *Lecture Notes in Computer Science*, **2016**, 62-80	0.9	1
1230	Study of different cryptographic technique and challenges in future. **2016**,		8
1229	Challenges of Fully Homomorphic Encryptions for the Internet of Things. **2016**, E99.D, 1982-1990		7
1228	Secure and Scalable Statistical Computation of Questionnaire Data in R. *IEEE Access*, **2016**, 4, 4635-4645	3.5	5
1227	Secure multiparty computation of a comparison problem. **2016**, 5, 1489		6
1226	Network and System Security. *Lecture Notes in Computer Science*, **2016**,	0.9	5
1225	Privately Evaluating Decision Trees and Random Forests. **2016**, 2016, 335-355		64
1224	Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions. **2016**, 45, 1793-1834		5
1223	Non-Black-Box Simulation from One-Way Functions and Applications to Resettable Security. **2016**, 45, 415-458		11
1222	TaoStore: Overcoming Asynchronicity in Oblivious Data Storage. **2016**,		21
1221	References. **2016**, 273-305		
1220	Information Theoretic Security. *Lecture Notes in Computer Science*, **2016**,	0.9	1
1219	Homomorphic Encryption Based on Group Algebras and Goldwasser-Micali Scheme. *Lecture Notes in Computer Science*, **2016**, 149-166	0.9	1
1218	Privacy-aware MMSE estimation. **2016**,		22
1217	Evaluating applicability of perturbation techniques for privacy preserving data mining by descriptive statistics. **2016**,		3
1216	Public-key encryption indistinguishable under plaintext-checkable attacks. **2016**, 10, 288-303		8

1215	On the Black-box Use of Somewhat Homomorphic Encryption in NonInteractive Two-Party Protocols. **2016**, 30, 266-295		2
1214	Differential Privacy: From Theory to Practice. **2016**, 8, 1-138		41
1213	XPIR : Private Information Retrieval for Everyone. **2016**, 2016, 155-174		58
1212	Provably secure Rabin-p cryptosystem in hybrid setting. **2016**,		
1211	Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments. **2016**, 25, 607-666		6
1210	Toward a Game Theoretic View of Secure Computation. *Journal of Cryptology*, **2016**, 29, 879-926	2.1	5
1209	Semantic-Security Capacity for Wiretap Channels of Type II. **2016**, 62, 3863-3879		37
1208	$2DCrypt$: Image Scaling and Cropping in Encrypted Domains. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 2542-2555	8	15
1207	A Decade of Lattice Cryptography. **2016**, 10, 283-424		153
1206	Pursuit of the Universal. *Lecture Notes in Computer Science*, **2016**,	0.9	
1205	A thirty Year old conjecture about promise problems. **2016**, 25, 883-919		1
1204	Cryptographic Hierarchical Access Control for Dynamic Structures. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 2349-2364	8	61
1203	Selectively chosen ciphertext security in threshold public-key encryption. *Security and Communication Networks*, **2016**, 9, 189-200	1.9	1
1202	. **2016**, 13, 326-339		6
1201	Quantum cryptography beyond quantum key distribution. **2016**, 78, 351-382		86
1200	Secure Nonlocal Denoising in Outsourced Images. **2016**, 12, 1-23		9
1199	Efficient privacy-preserving string search and an application in genomics. **2016**, 32, 1652-61		30
1198	Public-Key Cryptography â PKC 2016. *Lecture Notes in Computer Science*, **2016**,	0.9	1

1197	Public-Key Cryptography â PKC 2016. *Lecture Notes in Computer Science*, **2016**,	0.9	
1196	Accountable mobile E-commerce scheme via identity-based plaintext-checkable encryption. **2016**, 345, 143-155		19
1195	Secretly Pruned Convolutional Codes: Security Analysis and Performance Results. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 1500-1514	8	1
1194	Private Cell Retrieval From Data Warehouses. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 1346-1361	8	5
1193	Cryptographic Assumptions: A Position Paper. *Lecture Notes in Computer Science*, **2016**, 505-522	0.9	20
1192	Analysis of One-Time Random Projections for Privacy Preserving Compressed Sensing. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 313-327	8	78
1191	A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks. **2016**, 18, 577-601		56
1190	Security Aspects of Compressed Sensing. **2016**, 145-162		1
1189	Tightly secure signatures and public-key encryption. **2016**, 80, 29-61		19
1188	Key Indistinguishability versus Strong Key Indistinguishability for Hierarchical Key Assignment Schemes. **2016**, 13, 451-460		23
1187	Secret-Sharing for NP. *Journal of Cryptology*, **2017**, 30, 444-469	2.1	16
1186	Write-only oblivious RAM-based privacy-preserved access of outsourced data. **2017**, 16, 23-42		12
1185	Security proof of the canonical form of self-synchronizing stream ciphers. **2017**, 82, 377-388		2
1184	ASICS: authenticated key exchange security incorporating certification systems. **2017**, 16, 151-171		2
1183	Reconciling Non-malleability with Homomorphic Encryption. *Journal of Cryptology*, **2017**, 30, 601-671	2.1	0
1182	Efficient Cryptosystems From (mathbf{2}^{{varvec{k}}})-th Power Residue Symbols. *Journal of Cryptology*, **2017**, 30, 519-549	2.1	14
1181	Indistinguishability of Compressed Encryption With Circulant Matrices for Wireless Security. **2017**, 24, 181-185		11
1180	Codes, Cryptology and Information Security. *Lecture Notes in Computer Science*, **2017**,	0.9	1

1179	Privacy-Enhanced Television Audience Measurements. **2017**, 17, 1-29	0
1178	Privacy-Preserving Integration of Medical Data : A Practical Multiparty Private Set Intersection. **2017**, 41, 37	16
1177	Chosen-Ciphertext Secure Fully Homomorphic Encryption. *Lecture Notes in Computer Science*, **2017**, 213-240	32
1176	Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism. **2017**, 45, 1-10	57
1175	Multi-biometric template protection based on Homomorphic Encryption. **2017**, 67, 149-163	82
1174	Homomorphic Encryption. **2017**, 219-276	13
1173	Arithmetic Cryptography. **2017**, 64, 1-74	3
1172	Dimension, pseudorandomness and extraction of pseudorandomness1. **2017**, 6, 277-305	
1171	Secure Centrality Computation Over Multiple Networks. **2017**,	4
1170	E-Technologies: Embracing the Internet of Things. **2017**,	2
1169	Securing the Internet of Things: A Worst-Case Analysis of Trade-Off between Query-Anonymity and Communication-Cost. **2017**,	0
1168	Information-theoretic physical layer security for satellite channels. **2017**,	5
1167	Physical-Layer Cryptography Through Massive MIMO. **2017**, 63, 5419-5436	16
1166	Information Security Education for a Global Digital Society. **2017**,	2
1165	Fully homomorphic encryption schemes: The state of the art. **2017**,	7
1164	Insight of the protection for data security under selective opening attacks. **2017**, 412-413, 223-241	129
1163	How to explain modern security concepts to your children. **2017**, 41, 422-447	1
1162	Principal Inertia Components and Applications. **2017**, 63, 5011-5038	18

1161	On the Multi-output Filtering Model and Its Applications. *Lecture Notes in Computer Science*, **2017**, 265-281	0.9	
1160	Multi-key privacy-preserving deep learning in cloud computing. **2017**, 74, 76-85		266
1159	Secure rank correlation computation for IoT applications. **2017**, 23, 40		
1158	Computing Platforms for Software-Defined Radio. **2017**,		
1157	Practical-oriented protocols for privacy-preserving outsourced big data analysis: Challenges and future research directions. **2017**, 69, 97-113		28
1156	One-Message Unilateral Entity Authentication Schemes. **2017**,		
1155	All-But-Many Lossy Trapdoor Functions and Selective Opening Chosen-Ciphertext Security from LWE. *Lecture Notes in Computer Science*, **2017**, 332-364	0.9	22
1154	On physical-layer concepts and metrics in secure signal transmission. **2017**, 25, 14-25		25
1153	Why Your Encrypted Database Is Not Secure. **2017**,		25
1152	Enhanced Operating System Protection to Support Digital Forensic Investigations. **2017**,		1
1151	Towards a Toolkit for Utility and Privacy-Preserving Transformation of Semi-structured Data Using Data Pseudonymization. *Lecture Notes in Computer Science*, **2017**, 163-179	0.9	2
1150	Encryption Switching Protocols Revisited: Switching Modulo p. *Lecture Notes in Computer Science*, **2017**, 255-287	0.9	11
1149	Efficient Commodity Matching for Privacy-Preserving Two-Party Bartering. **2017**,		1
1148	A Double Perturbation Method for Reducing Dynamical Degradation of the Digital Baker Map. **2017**, 27, 1750103		28
1147	Notice of Removal: New pseudorandom number generators from block ciphers. **2017**,		
1146	Naorâ€Yung paradigm with shared randomness and applications. **2017**, 692, 90-113		1
1145	Instantiability of RSA-OAEP Under Chosen-Plaintext Attack. *Journal of Cryptology*, **2017**, 30, 889-919	2.1	7
1144	On the Impossibility of Cryptography with Tamperable Randomness. **2017**, 79, 1052-1101		5

1143	Identity-Based Encryption from Codes with Rank Metric. *Lecture Notes in Computer Science*, **2017**, 194-224	0.9	18
1142	Multipurpose Public-Key Encryption. *Lecture Notes in Computer Science*, **2017**, 69-84	0.9	
1141	Automatic Encryption Schemes Based on the Neural Networks: Analysis and Discussions on the Various Adversarial Models (Short Paper). *Lecture Notes in Computer Science*, **2017**, 566-575	0.9	2
1140	Cryptography and Coding. *Lecture Notes in Computer Science*, **2017**,	0.9	
1139	Security, Privacy, and Applied Cryptography Engineering. *Lecture Notes in Computer Science*, **2017**,	0.9	3
1138	Short Integrated PKE+PEKS in Standard Model. *Lecture Notes in Computer Science*, **2017**, 226-246	0.9	2
1137	Practical Homomorphic Encryption Over the Integers for Secure Computation in the Cloud. *Lecture Notes in Computer Science*, **2017**, 44-76	0.9	4
1136	Resettably-Sound Resettable Zero Knowledge in Constant Rounds. *Lecture Notes in Computer Science*, **2017**, 111-138	0.9	2
1135	An Efficient Privacy-Preserving Palmprint Authentication Scheme Based on Homomorphic Encryption. *Lecture Notes in Computer Science*, **2017**, 503-512	0.9	1
1134	A New Method for Computational Private Information Retrieval. **2017**, 60, 1238-1250		1
1133	A Framework for the Cryptographic Enforcement of Information Flow Policies. **2017**,		2
1132	Redactable Blockchain â□br â□Rewriting History in Bitcoin and Friends. **2017**,		124
1131	An efficient solution to the socialist millionaires' problem. **2017**,		3
1130	Introduction to Security and Privacy on the Blockchain. **2017**,		66
1129	. **2017**, 19, 2820-2835		111
1128	Homomorphic Cryptosystems for Securing Data in Public Cloud Computing. **2017**, 59-75		1
1127	Multimedia Forensics and Security. **2017**,		0
1126	On the power of rewinding simulators in functional encryption. **2017**, 84, 373-399		4

1125 Statistical learning based fully homomorphic encryption on encrypted data. **2017**, 21, 7473-7483 7

1124 Audition for multimedia computing. **2017**, 31-50

1123 Hawkes processes for events in social media. **2017**, 191-218 15

1122 Cloud gaming. **2017**, 287-314 1

1121 Boolean Circuit Camouflage. **2017**, 3

1120 Enhanced message based random variable length key encryption algorithm (E-MRVLK). **2017**, 38, 1393-1407

1119 Channel-Aware Randomized Encryption and Channel Estimation Attack. *IEEE Access*, **2017**, 5, 25046-25054 3

1118 On the k-th order lfsr sequence with public key cryptosystems. **2017**, 67, 601-610 1

1117 No-Match Attacks and Robust Partnering Definitions. **2017**, 17

1116 DLSBD-MHT: Dual-level source-based deduplication with Merkle-Hash-Tree for big data. **2017**, 0

1115 One-time-commutative public key encryption. **2017**, 1

1114 Deep learning for video classification and captioning. **2017**, 3-29 23

1113 Group-Based Source-Destination Verifiable Encryption with Blacklist Checking. *Lecture Notes in Computer Science*, **2017**, 186-203 0.9

1112 Multimedia fog computing: minions in the cloud and crowd. **2017**, 255-286 2

1111 Secret key agreement using a virtual wiretap channel. **2017**, 4

1110 Encrypted domain multimedia content analysis. **2017**, 75-104

1109 On the indistinguishability of compressed encryption with partial unitary sensing matrices. **2017**,

1108 New Pseudorandom Number Generators from Block Ciphers. **2017**, 3

1107	. **2017**,		0
1106	Secrecy rate of channel-aware randomized secure transmission schemes in multicarrier systems. **2017**,		
1105	Bibliography. **2017**, 315-377		
1104	Introduction. **2017**, 3-34		
1103	Integer Factorization Based Cryptography. **2017**, 293-336		1
1102	Frontiers of Multimedia Research. **2017**,		1
1101	A new code-based encryption scheme and its applications. **2017**, 10, 515		4
1100	Literaturverzeichnis. **2017**,		
1099	Semantic Security with Practical Transmission Schemes over Fading Wiretap Channels. **2017**, 19, 491		1
1098	Semantically Secure Symmetric Encryption with Error Correction for Distributed Storage. *Security and Communication Networks*, **2017**, 2017, 1-10	1.9	
1097	Efficient KDM-CCA Secure Public-Key Encryption via Auxiliary-Input Authenticated Encryption. *Security and Communication Networks*, **2017**, 2017, 1-27	1.9	1
1096	Research on a New Signature Scheme on Blockchain. *Security and Communication Networks*, **2017**, 2017, 1-10	1.9	8
1095	An Efficient Secret Key Homomorphic Encryption Used in Image Processing Service. *Security and Communication Networks*, **2017**, 2017, 1-11	1.9	6
1094	Social-sensed multimedia computing. **2017**, 137-157		
1093	On the security of compressed encryption with partial unitary sensing matrices embedding a secret keystream. **2017**, 2017,		3
1092	Preface. **2017**, xi-xv		
1091	A Novel Perfect Privacy Preserving Single Database Private Information Retrieval With Non-trivial Communication. **2017**,		
1090	Multimodal analysis of free-standing conversational groups. **2017**, 51-74		

1089	Efficient similarity search. **2017**, 105-134		
1088	Utilizing implicit user cues for multimedia analytics. **2017**, 219-251		
1087	Homomorphic Encryption as a Service for Outsourced Images in Mobile Cloud Computing Environment. **2017**, 7, 27-40		53
1086	Situation recognition using multimodal data. **2017**, 159-189		
1085	A game-theoretical and cryptographical approach to crypto-cloud computing and its economical and financial aspects. **2018**, 260, 217-231		6
1084	Minimizing Ciphertext in Homomorphic Encryption Scheme for Cloud Data. **2018**, 583-591		
1083	Efficient pairing-free PRE schemes for multimedia data sharing in IoT. **2018**, 77, 18327-18354		1
1082	Tightly SIM-SO-CCA Secure Public Key Encryption from Standard Assumptions. *Lecture Notes in Computer Science*, **2018**, 62-92	0.9	5
1081	Non-Binary Pseudorandom Number Generators For Information Security Purposes. **2018**, 123, 203-211		1
1080	Fiat-Shamir and Correlation Intractability from Strong KDM-Secure Encryption. *Lecture Notes in Computer Science*, **2018**, 91-122	0.9	53
1079	Formal verification of the W3C web authentication protocol. **2018**,		5
1078	Achieving Secrecy Capacity of the Gaussian Wiretap Channel With Polar Lattices. **2018**, 64, 1647-1665		14
1077	GRAAD: Group Anonymous and Accountable D2D Communication in Mobile Networks. *IEEE Transactions on Information Forensics and Security*, **2018**, 13, 449-464	8	35
1076	Efficient Encryption From Random Quasi-Cyclic Codes. **2018**, 64, 3927-3943		31
1075	Security Formalizations and Their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography. **2018**, 64, 654-685		11
1074	Public-Key Encryption with Tight Simulation-Based Selective-Opening Security. **2018**, 61, 288-318		2
1073	Deterministic Public-Key Encryption for Adaptively-Chosen Plaintext Distributions. *Journal of Cryptology*, **2018**, 31, 1012-1063	2.1	1
1072	On the (Im-)Possibility of Extending Coin Toss. *Journal of Cryptology*, **2018**, 31, 1120-1163	2.1	

1071	Maximal Correlation Secrecy. **2018**, 64, 3916-3926		3
1070	Modelling and Verification of Secure Exams. **2018**,		2
1069	PDA: Semantically Secure Time-Series Data Analytics with Dynamic User Groups. **2018**, 15, 260-274		5
1068	White-Box Traceable CP-ABE for Cloud Storage Service: How to Catch People Leaking Their Access Credentials Effectively. **2018**, 15, 883-897		61
1067	. **2018**, 15, 694-707		19
1066	Privacy-preserving outsourced classification in cloud computing. **2018**, 21, 277-286		112
1065	Incremental Deterministic Public-Key Encryption. *Journal of Cryptology*, **2018**, 31, 134-161	2.1	10
1064	Robust Encryption. *Journal of Cryptology*, **2018**, 31, 307-350	2.1	8
1063	A Black-Box Construction of Non-malleable Encryption from Semantically Secure Encryption. *Journal of Cryptology*, **2018**, 31, 172-201	2.1	4
1062	UFace: Your universal password that no one can see. **2018**, 77, 627-641		6
1061	The Applied Pi Calculus. **2018**, 65, 1-41		43
1060	Efficient machine learning over encrypted data with non-interactive communication. **2018**, 58, 87-108		13
1059	Privacy Preserving Fisherâ Exact Test on Genomic Data. **2018**,		1
1058	Fast Secret Key Generation in Static Environments Using Induced Randomness. **2018**,		5
1057	Security and robustness of a modified ElGamal encryption scheme. **2018**, 13, 375		1
1056	Privacy Preserving in Blockchain Based on Partial Homomorphic Encryption System for Ai Applications. **2018**,		14
1055	Privacy Amplification: Recent Developments and Applications. **2018**,		1
1054	Usage of DHS and De-duplicating Encrypted Data using ABE & ECC for Secured Cloud Environment. **2018**,		

1053	SoK. **2018**,		12
1052	A Pragmatic Introduction to Secure Multi-Party Computation. **2018**, 2, 70-246		49
1051	. **2018**,		10
1050	Data Service Outsourcing and Privacy Protection in Mobile Internet. **2018**,		
1049	Encrypted Domain Image Scaling and Cropping in Cloud. **2018**,		
1048	Analysis on Homomorphic Properties of Attribute involved Probabilistic Public Key Cryptosystem based on Sylow P-subgroups. **2018**,		
1047	Implementation of Public Key Crypto Processor with Probabilistic Encryption on FPGA for Nodes in Wireless Sensor Networks. **2018**,		2
1046	Communication Lower Bounds via Critical Block Sensitivity. **2018**, 47, 1778-1806		10
1045	Two-Round Adaptively Secure Multiparty Computation from Standard Assumptions. *Lecture Notes in Computer Science*, **2018**, 175-205	0.9	11
1044	Encyclopedia of Database Systems. **2018**, 2888-2893		
1043	On Intersection Types and Probabilistic Lambda Calculi. **2018**,		6
1042	Privacy-Preserving Certification of Sustainability Metrics. **2018**,		
1041	An Efficient Hash Based Parallel Block Cipher Mode of Operation. **2018**,		4
1040	Encoding of Rational Numbers and Their Homomorphic Computations for FHE-Based Applications. **2018**, 29, 1023-1044		3
1039	A Privacy-Preserving Classifier in Statistic Pattern Recognition. *Lecture Notes in Computer Science*, **2018**, 496-507	0.9	1
1038	. *IEEE Access*, **2018**, 6, 47521-47534	3.5	10
1037	An applications of signed quadratic residues in public key cryptography. **2018**, 10, 1850081		
1036	Traceable ciphertext-policy attribute-based encryption scheme with attribute level user revocation for cloud storage. **2018**, 13, e0203225		11

1035	An Application of Partial Homomorphic Encryption in Computer System with Limited Resources. **2018**, 25,		
1034	Zero knowledge proof for secure two-party computation with malicious adversaries in distributed networks. **2018**, 16, 441		3
1033	A Robust Algorithm of Encrypted Face Recognition Based on DWT-DCT and Tent Map. *Lecture Notes in Computer Science*, **2018**, 508-518	0.9	1
1032	Hierarchical Group Signatures with Verifier-Local Revocation. *Lecture Notes in Computer Science*, **2018**, 271-286	0.9	2
1031	Hybrid cryptosystem implementation using fast data encipherment algorithm (FEAL) and goldwasser-micali algorithm for file security. **2018**, 1013, 012159		
1030	A chaos-based probabilistic block cipher for image encryption. **2018**, 34, 1533-1533		10
1029	A New Symmetric Key Encryption Algorithm Based on Jumbling Binary Sequence of Message. **2018**,		
1028	Comparative Analysis of Double Gate TFET and Hetero Dielectric Double Gate TFET. **2018**,		2
1027	Chaotic grey wolf optimization-based active disturbance rejection control applied to quadrotor trajectory tracking. **2018**,		
1026	Power Flow Control and Seamless transfer of Single-Phase Grid Interactive Inverter Between Off-grid and Utility-Connected Systems. **2018**,		0
1025	Distributed Formation Control of Multirotors with Switching Topologies. **2018**,		
1024	Receiver- and sender-deniable functional encryption. **2018**, 12, 207-216		1
1023	Evaluating AND gates over encrypted data in cloud computing. **2018**,		2
1022	On the Bit Security of Cryptographic Primitives. *Lecture Notes in Computer Science*, **2018**, 3-28	0.9	18
1021	Practical witness encryption for algebraic languages or how to encrypt under Grothâ Sahai proofs. **2018**, 86, 2525-2547		3
1020	Private information retrieval in vehicular location-based services. **2018**,		3
1019	A novel hybrid private information retrieval with non-trivial communication cost. **2018**,		
1018	Introduction to Security Reduction. **2018**,		7

1017	From Sample to Big Data: Competing or Complementary Paradigms?. **2018**, 77-104		1
1016	Security in Cyber-Enabled Design and Manufacturing: A Survey. **2018**, 18,		11
1015	Cloud-Assisted Privacy-Preserving Classification for IoT Applications. **2018**,		1
1014	A Novel Text Encryption Algorithm Based on the Two-Square Cipher and Caesar Cipher. **2018**, 78-88		10
1013	Is privacy ?. **2018**, 376,		15
1012	Practical and Tightly-Secure Digital Signatures and Authenticated Key Exchange. *Lecture Notes in Computer Science*, **2018**, 95-125	0.9	34
1011	Privacy-Preserving Plaintext-Equality of Low-Entropy Inputs. *Lecture Notes in Computer Science*, **2018**, 262-279	0.9	3
1010	Security Analysis of Smartphone and Cloud Computing Authentication Frameworks and Protocols. *IEEE Access*, **2018**, 6, 34527-34542	3.5	10
1009	Homomorphic Encryption-Based Reversible Data Hiding for 3D Mesh Models. **2018**, 43, 8145-8157		17
1008	Verifiable Chebyshev maps-based chaotic encryption schemes with outsourcing computations in the cloud/fog scenarios. **2019**, 31, e4523		8
1007	A New Blind ECDSA Scheme for Bitcoin Transaction Anonymity. **2019**,		8
1006	Implementation of Homomorphic Encryption for Wireless Sensor Networks Integrated with Cloud Infrastructure. **2019**, 15, 235-248		3
1005	Additively Homomorphic IBE from Higher Residuosity. *Lecture Notes in Computer Science*, **2019**, 496-515	0.9	3
1004	A privacy-preserving multifactor authentication system. **2019**, 2, e88		5
1003	Freestyle, a randomized version of ChaCha for resisting offline brute-force and dictionary attacks. **2019**, 49, 102396		4
1002	How to (not) Share a Password. **2019**,		1
1001	Cloud-based Outsourcing for Enabling Privacy-Preserving Large-scale Non-Negative Matrix Factorization. *IEEE Transactions on Services Computing*, **2019**, 1-1	4.8	16
1000	On the Termination Problem for Probabilistic Higher-Order Recursive Programs. **2019**,		4

999	Symbolic Methods in Computational Cryptography Proofs. **2019**,		0
998	Learning Radio Maps for Physical-Layer Security in the Radio Access. **2019**,		4
997	Prediction error expansion-based reversible data hiding in encrypted images with public key cryptosystem. **2019**, 13, 1705-1713		3
996	Paillier Cryptosystem based Mean Value Computation for Encrypted Domain Image Processing Operations. **2019**, 15, 1-21		2
995	Homomorphic Encryption Technology for Cloud Computing. **2019**, 154, 73-83		14
994	Simulation-based receiver selective opening CCA secure PKE from standard computational assumptions. **2019**, 795, 570-597		2
993	. **2019**, 1-1		3
992	Privacy-Preserving MAX/MIN Query Processing for WSN -as-a -Service. **2019**,		1
991	Two dimensional ElGamal public key cryptosystem. **2019**, 28, 120-126		0
990	Secure and Efficient Adjacency Search Supporting Synonym Query on Encrypted Graph in the Cloud. *IEEE Access*, **2019**, 7, 133716-133724	3.5	2
989	. *IEEE Access*, **2019**, 7, 6765-6773	3.5	0
988	Innovations in Computer Science and Engineering. **2019**,		2
987	Search in My Way: Practical Outsourced Image Retrieval Framework Supporting Unshared Key. **2019**,		18
986	Privacy Techniques for Edge Computing Systems. **2019**, 107, 1632-1654		13
985	A Survey of Various Cryptographic Techniques: From Traditional Cryptography to Fully Homomorphic Encryption. **2019**, 295-305		4
984	. **2019**,		2
983	Updatable Ciphertext-Policy Attribute-Based Encryption Scheme With Traceability and Revocability. *IEEE Access*, **2019**, 7, 66832-66844	3.5	10
982	Non-interactive Zero Knowledge Proofs in the Random Oracle Model. *Lecture Notes in Computer Science*, **2019**, 118-141	0.9	

981	Efficient Proactive Secret Sharing for Large Data via Concise Vector Commitments. *Lecture Notes in Computer Science*, **2019**, 171-194	0.9	1
980	Limitless HTTP in an HTTPS World. **2019**,		2
979	Privacy-Preserving Reversible Information Hiding Based on Arithmetic of Quadratic Residues. *IEEE Access*, **2019**, 7, 54117-54132	3.5	27
978	Foundations and Practice of Security. *Lecture Notes in Computer Science*, **2019**,	0.9	1
977	The truth behind the myth of the Folk theorem. **2019**, 117, 479-498		1
976	Hidden Protocol Strengthening with Random Sentences as Cryptographic Nonces. **2019**,		
975	Two-Server Delegation of Computation on Label-Encrypted Data. **2019**, 1-1		3
974	. *IEEE Transactions on Information Forensics and Security*, **2019**, 14, 2689-2704	8	5
973	Public-Key Encryption with Integrated Keyword Search. **2019**, 3, 12-25		2
972	An efficient scheme for secure domain medical image fusion over cloud. **2019**, 78, 20609-20636		3
971	Wiretap Channels: Nonasymptotic Fundamental Limits. **2019**, 65, 4069-4093		37
970	Towards Non-Interactive Zero-Knowledge for NP from LWE. *Lecture Notes in Computer Science*, **2019**, 472-503	0.9	6
969	Break-glass Encryption. *Lecture Notes in Computer Science*, **2019**, 34-62	0.9	5
968	Monoidal Encryption over ((mathbb {F}_2,cdot)). *Lecture Notes in Computer Science*, **2019**, 504-517	0.9	
967	Innovative Security Solutions for Information Technology and Communications. *Lecture Notes in Computer Science*, **2019**,	0.9	1
966	Practical homomorphic encryption over the integers for secure computation in the cloud. **2019**, 18, 549-579		9
965	A Graph-Based Modular Coding Scheme Which Achieves Semantic Security. **2019**,		1
964	[Copyright notice]. **2019**,		

963	SecReS: A Secure and Reliable Storage Scheme for Cloud with Client-Side Data Deduplication. **2019**,	0
962	The Experiences and Practices on Market with Large-Scale Renewable Energy Grid Integration. **2019**,	1
961	Proportionate Minimum-Symbol-Error-Rate Based Sparse Equalization for Underwater Acoustic Channels. **2019**,	0
960	Attrition of women students in the first year of informatics studies at UTFSM. **2019**,	1
959	Absorptive Surface Based on Graphene Composite for Advanced EMI Suppression. **2019**,	4
958	Comparative Models of Induced Thermomechanical Stress in Silicon Solar Cells Interconnected with Conventional Tabbing and Wire-Based Interconnection Methods. **2019**,	1
957	On the Achievable Resolution in Inverse Source beyond the Fresnel Approximation: Numerical Results. **2019**,	
956	A Practical Image Encryption Algorithm for Privacy Protection. **2019**,	
955	Development of a Power System Restoration Plan with Renewable-based Microgrids. **2019**,	1
954	IEEE Industrial Electronics Society. **2019**, 15, C2-C2	
953	. **2019**,	2
952	The Case of Adversarial Inputs for Secure Similarity Approximation Protocols. **2019**,	
951	Classification of Social Content Management Strategy using Delphi Study. **2019**,	
950	Covariance Evolution for Spatially â Mt. Fujiâ Coupled LDPC Codes. **2019**,	2
949	Recurrent U-Net for Resource-Constrained Segmentation. **2019**,	31
948	CSAT: A User-interactive Cyber Security Architecture Tool based on NIST-compliance Security Controls for Risk Management. **2019**,	2
947	Multi-dimensional Risk Assessment Method for Electric Transmission Line. **2019**,	0
946	On Fully Homomorphic Encryption for Privacy-Preserving Deep Learning. **2019**,	0

945 Recognition of Branch Series Resonance Based on Port Equivalent Method. **2019**, 4, 197-203 0

944 Four-Junction Wafer Bonded Solar Cells for Space Applications. **2019**, 0

943 Secrecy Analysis under Dual Correlated Rician Fading Employing Opportunistic Relays. **2019**,

942 Survey on renewable energy forecasting using different techniques. **2019**, 5

941 [Copyright notice]. **2019**,

940 Event Driven Motif Exploration of Dynamic Banking Transaction Network. **2019**, 0

939 EAARG(Energy Aware Allocation of Resources using Game Theory) Approach for Multi-hop Cognitive Radio Network. **2019**,

938 Aspect-based Opinion Mining for Code-Mixed Restaurant Reviews in Indonesia. **2019**, 1

937 Determination of the Sensitivity of Linear Periodically-Time-Variable Circuits by the Frequency Symbolic Method. **2019**,

936 EDUNINE 2019 Awards. **2019**,

935 IEEE Transactions on Games. **2019**, 11, C2-C2

934 . **2019**, 3

933 On the Okamoto-Uchiyama cryptosystem: (A brief essay on basic mathematics applied in cryptography). **2019**, 1341, 042013

932 Three hub lncRNAs associated with prognosis of endometrial cancer identified by co-expression analysis. **2019**,

931 Introduction to PDSEC-19. **2019**,

930 A Modular Semantically Secure Wiretap Code with Shared Key for Weakly Symmetric Channels. **2019**, 1

929 A New Approach for EEG-Based Biometric Authentication Using Auditory Stimulation. **2019**, 1

928 Progress in Si IGBT Technology â□s an ongoing Competition with WBG Power Devices. **2019**, 3

927	A Real-Time Compliant State-Space Model of Induction Machines Including Winding Distribution Harmonics and Winding Interconnections. **2019**,	0
926	Multispectral Imaging for Fine-Grained Recognition of Powders on Complex Backgrounds. **2019**,	3
925	Linear Distribution-based SHADE with Variable Population Size. **2019**,	
924	The virtual simulation system of nuclear radiation dose field based on virtual reality technology. **2019**,	1
923	Design of Secure Reconfigurable Power Converters. **2019**,	0
922	An Integrated Power Differential Scheme for Tertiary Power Transformer Protection. **2019**,	
921	A caching strategy for industrial edge networks. **2019**,	1
920	Hollow-Core Photonic Crystal Fibers Filled with Noble Gases: He, Ne, Ar, Kr, Xe. **2019**,	
919	Electrical Characterization Methodology for Raw Cable up to 30 GHz. **2019**,	
918	Unit commitment using time-ahead priority list and heterogeneous comprehensive learning PSO. **2019**,	1
917	. **2019**,	
916	Analysis and Optimal Design of a New Single-Photon Memristor. **2019**,	
915	Tracking Control of a Skid Steered Mobile Robot with Adaptive Robust Second Order Sliding-Mode Controller. **2019**,	1
914	Design of High-power Fully Automatic Charging Device. **2019**,	2
913	Verifiable Arithmetic Computations Using Additively Homomorphic Tags. **2019**,	1
912	A Range Search Scheme Based on Encrypted Index Hiding Order and Access Patterns. **2019**,	
911	Outsourcing Computations Through Smith Normal Form with Access Control. **2019**,	
910	The Strength of Weak Randomization: Easily Deployable, Efficiently Searchable Encryption with Minimal Leakage. **2019**,	1

909	On Privacy Notions in Anonymous Communication. **2019**, 2019, 105-125		6
908	Compressed Sensing for Privacy-Preserving Data Processing. **2019**,		2
907	Security analysis and new models on the intelligent symmetric key encryption. **2019**, 80, 14-24		16
906	Physical Layer Security for RF Satellite Channels in the Finite-Length Regime. *IEEE Transactions on Information Forensics and Security*, **2019**, 14, 981-993	8	15
905	Security and Fault Tolerance in Internet of Things. **2019**,		4
904	Quantum encryption and generalized Shannon impossibility. **2019**, 87, 1961-1972		5
903	Real-time reversible data hiding with shifting block histogram of pixel differences in encrypted image. **2019**, 16, 709-724		12
902	A secure channel code-based scheme for privacy preserving data aggregation in wireless sensor networks. **2019**, 32, e3832		4
901	Searchable encryption approaches: attacks and challenges. **2019**, 61, 1179-1207		3
900	Traceable-then-revocable ciphertext-policy attribute-based encryption scheme. **2019**, 93, 903-913		25
899	An optimal approach for watermarking using MRC4 encryption scheme. **2019**, 22, 11183-11191		3
898	A Novel Group Ownership Delegate Protocol for RFID Systems. **2019**, 21, 1153-1166		11
897	Secure Wavelet Matrix: Alphabet-Friendly Privacy-Preserving String Search for Bioinformatics. **2019** , 16, 1675-1684		7
896	Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud. **2019**, 5, 330-342		35
895	. **2019**, 7, 827-837		3
894	How to Extract Image Features Based on Co-Occurrence Matrix Securely and Efficiently in Cloud Computing. **2020**, 8, 207-219		8
893	Comprehensive survey on privacy-preserving protocols for sealed-bid auctions. **2020**, 88, 101502		9
892	Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. **2020**, 167, 107286		34

891	Unbalanced private set intersection cardinality protocol with low communication cost. **2020**, 102, 1054-1061		14
890	ReHand: Secure Region-Based Fast Handover With User Anonymity for Small Cell Networks in Mobile Communications. *IEEE Transactions on Information Forensics and Security*, **2020**, 15, 927-942	8	12
889	Polynomial AND homomorphic cryptosystem and applications. **2020**, 63, 1		0
888	A public key cryptosystem and signature scheme based on numerical series. **2020**, 2, 1		1
887	On probabilistic term rewriting. *Science of Computer Programming*, **2020**, 185, 102338	1.1	7
886	Authorized Keyword Searches on Public Key Encrypted Data With Time Controlled Keyword Privacy. *IEEE Transactions on Information Forensics and Security*, **2020**, 15, 2096-2109	8	6
885	SoK: Differential Privacy as a Causal Property. **2020**,		2
884	Linking Sensitive Data. **2020**,		6
883	Zero-knowledge identity authentication for internet of vehicles: Improvement and application. **2020**, 15, e0239043		1
882	. *IEEE Access*, **2020**, 8, 107601-107613	3.5	7
881	Protecting Privacy of Location-Based Services in Road Networks. **2020**, 1-14		5
880	Cryptanalysis and Improvement of a Group Authentication Scheme with Multiple Trials and Multiple Authentications. *Security and Communication Networks*, **2020**, 2020, 1-8	1.9	1
879	Plaintext aware encryption in the standard model under the linear Diffie-Hellman knowledge assumption. **2020**, 22, 270		1
878	Public key and levelled attributes access policy oriented fully homomorphic encryption scheme. **2020**, 12, 51		0
877	Security analysis for fixed-time traffic control systems. **2020**, 139, 473-495		3
876	Quality-of-Service Prediction for Physical-layer Security via Secrecy Maps. **2020**,		
875	On Using The First Variant of Dependent RSA Encryption Scheme to Secure Text: A Tutorial. **2020**, 1542, 012024		
874	Advances in Cryptography and Secure Hardware for Data Outsourcing. **2020**,		2

873	Improved lattice-based CCA2-secure PKE in the standard model. **2020**, 63, 1		4
872	. **2020**,		1
871	Multi-use Deterministic Public Key Proxy Re-Encryption from Lattices in the Auxiliary-Input Setting. **2020**, 31, 551-567		4
870	Effective Activation Functions for Homomorphic Evaluation of Deep Neural Networks. *IEEE Access*, **2020**, 8, 153098-153112	3.5	9
869	Non-malleable Encryption: Simpler, Shorter, Stronger. *Journal of Cryptology*, **2020**, 33, 1984-2033	2.1	
868	A Survey on Secure Computation Based on Homomorphic Encryption in Vehicular Ad Hoc Networks. **2020**, 20,		5
867	Privacy-Protection Path Finding Supporting the Ranked Order on Encrypted Graph in Big Data Environment. *IEEE Access*, **2020**, 8, 214596-214604	3.5	0
866	Information encryption communication system based on the adversarial networks Foundation. **2020**, 415, 347-357		4
865	Privacy-Preserving Distributed Analytics in Fog-Enabled IoT Systems. **2020**, 20,		1
864	Physical Layer Secret Key Generation in Static Environments. *IEEE Transactions on Information Forensics and Security*, **2020**, 15, 2692-2705	8	31
863	Privacy-Preserving Krawtchouk Moment feature extraction over encrypted image data. **2020**, 536, 244-262		4
862	A novel trusted third party based signcryption scheme. **2020**, 79, 22749-22769		1
861	An Efficient Two-Server Ranked Dynamic Searchable Encryption Scheme. *IEEE Access*, **2020**, 8, 86328-86344	3.5	1
860	Homomorphic Comparison for Point Numbers with User-Controllable Precision and Its Applications. **2020**, 12, 788		2
859	CryptHOL: Game-Based Proofs in Higher-Order Logic. *Journal of Cryptology*, **2020**, 33, 494-566	2.1	5
858	A Traceable and Revocable Ciphertext-policy Attribute-based Encryption Scheme Based on Privacy Protection. **2020**, 1-1		34
857	Negative/Positive Electrocaloric Effect in Single-Layer Pb(ZrxTi1â)Oâ Thin Films for Solid-State Cooling Device. **2020**, 67, 1769-1775		3
856	Threshold-Based Edge Selection MPA for SCMA. **2020**, 69, 2957-2966		4

855	Privacy-Aware Distributed Hypothesis Testing. **2020**, 22,		4
854	ARTDL: Adaptive Random Testing for Deep Learning Systems. *IEEE Access*, **2020**, 8, 3055-3064	3.5	8
853	Innovative Security Solutions for Information Technology and Communications. *Lecture Notes in Computer Science*, **2020**,	0.9	
852	Information Security and Cryptology â□ICISC 2019. *Lecture Notes in Computer Science*, **2020**,	0.9	
851	Certain sequence of arithmetic progressions and a new key sharing method. **2020**, 12, 597-612		0
850	On privacy preserving data release of linear dynamic networks. **2020**, 115, 108839		3
849	Practical Data-in-Use Protection Using Binary Decision Diagrams. *IEEE Access*, **2020**, 8, 23847-23862	3.5	
848	An Operational Approach to Information Leakage. **2020**, 66, 1625-1657		30
847	Cryptography Arithmetic. **2020**,		2
846	Multi-client Sub-Linear Boolean Keyword Searching for Encrypted Cloud Storage with Owner-enforced Authorization. **2020**, 1-1		6
845	Practical Privacy-Preserving Face Authentication for Smartphones Secure Against Malicious Clients. *IEEE Transactions on Information Forensics and Security*, **2020**, 15, 2386-2401	8	13
844	WGAN-E: A Generative Adversarial Networks for Facial Feature Security. **2020**, 9, 486		3
843	Fair Data Transactions Across Private Databases. *IEEE Access*, **2020**, 8, 53720-53732	3.5	1
842	6.5 A 6.4-to-32Gb/s 0.96pJ/b Referenceless CDR Employing ML-Inspired Stochastic Phase-Frequency Detection Technique in 40nm CMOS. **2020**,		9
841	Security Infrastructure Technology for Integrated Utilization of Big Data. **2020**,		0
840	Obscure: Information-Theoretically Secure, Oblivious, and Verifiable Aggregation Queries on Secret-Shared Outsourced Data. **2020**, 1-1		
839	Lossless Data Hiding Based on Homomorphic Cryptosystem. **2021**, 18, 692-705		15
838	An alternative practical public-key cryptosystems based on the Dependent RSA Discrete Logarithm Problems. **2021**, 164, 114047		2

837	On designing an unaided authentication service with threat detection and leakage control for defeating opportunistic adversaries. **2021**, 15, 1		
836	Blockchain technology: Theory and practice. **2021**, 44, 75-103		
835	RSA and redactable blockchains. **2021**, 6, 1-6		4
834	Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. **2021**, 166, 91-109		31
833	Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. **2021**, 116, 406-425		8
832	Multiple-replica integrity auditing schemes for cloud data storage. **2021**, 33, 1-1		4
831	Privacy of outsourced two-party k-means clustering. **2021**, 33, e5473		1
830	OUP accepted manuscript.		
829	EHRChain: A Blockchain-based EHR System Using Attribute-Based and Homomorphic Cryptosystem. *IEEE Transactions on Services Computing*, **2021**, 1-1	4.8	3
828	A New Generalisation of the Goldwasser-Micali Cryptosystem Based on the Gap (2^k)-Residuosity Assumption. *Lecture Notes in Computer Science*, **2021**, 24-40	0.9	0
827	A Systematic Review of Challenges and Techniques of Privacy-Preserving Machine Learning. **2021**, 19-41		1
826	PDLHR: Privacy-Preserving Deep Learning Model With Homomorphic Re-Encryption in Robot System. **2021**, 1-12		2
825	Rate-1 Key-Dependent Message Security via Reusable Homomorphic Extractor Against Correlated-Source Attacks. *Lecture Notes in Computer Science*, **2021**, 421-450	0.9	
824	On the CCA Compatibility of Public-Key Infrastructure. *Lecture Notes in Computer Science*, **2021**, 235-260	0.9	1
823	Security issues for the Semantic Web. **2021**, 253-267		
822	Equivalence between Non-Malleability against Replayable CCA and Other RCCA-Security Notions. **2021**, E104.A, 89-103		
821	MoSS: Modular Security Specifications Framework. *Lecture Notes in Computer Science*, **2021**, 33-63	0.9	
820	On the Possibility of Basing Cryptography on (mathsf{EXP}ne mathsf{BPP}). *Lecture Notes in Computer Science*, **2021**, 11-40	0.9	0

819	Universal Proxy Re-Encryption. *Lecture Notes in Computer Science*, **2021**, 512-542	0.9	3
818	Toward Non-interactive Zero-Knowledge Proofs for NP from LWE. *Journal of Cryptology*, **2021**, 34, 1	2.1	3
817	CrypSH: A Novel IoT Data Protection Scheme Based on BGN Cryptosystem. **2021**, 1-1		1
816	Golden Grain: Building a Secure and Decentralized Model Marketplace for MLaaS. **2021**, 1-1		2
815	Fast Reaching Finite Time synchronization Approach for Chaotic Systems With Application in Medical Image Encryption. *IEEE Access*, **2021**, 9, 25911-25925	3.5	34
814	Threats and Security Issues in Smart City Devices. **2021**, 1230-1251		
813	Security in Distributed Ledger Technology: An Analysis of Vulnerabilities and Attack Vectors. **2021**, 722-742		3
812	On the Security of Homomorphic Encryption on Approximate Numbers. *Lecture Notes in Computer Science*, **2021**, 648-677	0.9	8
811	SO-CCA secure PKE from pairing based all-but-many lossy trapdoor functions. **2021**, 89, 895-923		1
810	Multiuser wireless speech encryption using synchronized chaotic systems. **2021**, 24, 651-663		2
809	Covid notions: Towards formal definitions - and documented understanding - of privacy goals and claimed protection in proximity-tracing services. **2021**, 22, 100125		6
808	A survey on multi-authority and decentralized attribute-based encryption. *Journal of Ambient Intelligence and Humanized Computing*, 1	3.7	6
807	Analog Lagrange Coded Computing. **2021**, 2, 283-295		6
806	Privacy-Guarding Optimal Route Finding with Support for Semantic Search on Encrypted Graph in Cloud Computing Scenario. **2021**, 2021, 1-12		2
805	Guest Column. **2021**, 52, 47-69		
804	A Family of Probabilistic Triple-bit Encryptions for Secure Cloud Applications. **2021**,		
803	Round-Optimal Secure Multi-party Computation. *Journal of Cryptology*, **2021**, 34, 1	2.1	2
802	Blockchain-based Fair and Decentralized Data Trading Model.		1

801	Cryptography from sublinear-time average-case hardness of time-bounded Kolmogorov complexity. **2021**,		0
800	DRBFT: Delegated randomization Byzantine fault tolerance consensus protocol for blockchains. **2021**, 559, 8-21		9
799	Privacy-Enhancing -Nearest Neighbors Search over Mobile Social Networks. **2021**, 21,		
798	The Design and Evolution of OCB. *Journal of Cryptology*, **2021**, 34, 1	2.1	0
797	Analog Privacy-Preserving Coded Computing. **2021**,		
796	On continuation-passing transformations and expected cost analysis. **2021**, 5, 1-30		2
795	Receiver Selective Opening CCA Secure Public Key Encryption from Various Assumptions. **2021**, E104.A, 1206-1218		
794	Cryptographic Hardness Based on the Decoding of Reed-Solomon Codes. *Lecture Notes in Computer Science*, **2002**, 232-243	0.9	20
793	Private Selective Payment Protocols. *Lecture Notes in Computer Science*, **2001**, 72-89	0.9	23
792	Sharing Decryption in the Context of Voting or Lotteries. *Lecture Notes in Computer Science*, **2001**, 90-104	0.9	122
791	Formal Eavesdropping and Its Computational Interpretation. *Lecture Notes in Computer Science*, **2001**, 82-94	0.9	60
790	Fair Encryption of RSA Keys. *Lecture Notes in Computer Science*, **2000**, 172-189	0.9	20
789	Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements. *Lecture Notes in Computer Science*, **2000**, 259-274	0.9	234
788	Optimal Chosen-Ciphertext Secure Encryption of Arbitrary-Length Messages. *Lecture Notes in Computer Science*, **2002**, 17-33	0.9	11
787	Formal Proofs for the Security of Signcryption. *Lecture Notes in Computer Science*, **2002**, 80-98	0.9	80
786	Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks. *Lecture Notes in Computer Science*, **2001**, 351-368	0.9	61
785	Mutually Independent Commitments. *Lecture Notes in Computer Science*, **2001**, 385-401	0.9	8
784	Practical Construction and Analysis of Pseudo-Randomness Primitives. *Lecture Notes in Computer Science*, **2001**, 442-459	0.9	6

783	Key-Privacy in Public-Key Encryption. *Lecture Notes in Computer Science*, **2001**, 566-582	0.9	216
782	Analysis and Improvements of NTRU Encryption Paddings. *Lecture Notes in Computer Science*, **2002**, 210-225	0.9	21
781	On the Security of RSA Encryption in TLS. *Lecture Notes in Computer Science*, **2002**, 127-142	0.9	20
780	Randomness-Optimal Characterization of Two NP Proof Systems. *Lecture Notes in Computer Science* , **2002**, 179-193	0.9	10
779	GEM: A Generic Chosen-Ciphertext Secure Encryption Method. *Lecture Notes in Computer Science*, **2002**, 263-276	0.9	26
778	Observability Analysis - Detecting When Improved Cryptosystems Fail -. *Lecture Notes in Computer Science*, **2002**, 17-29	0.9	16
777	Nonuniform Polynomial Time Algorithm to Solve Decisional Diffie-Hellman Problem in Finite Fields under Conjecture. *Lecture Notes in Computer Science*, **2002**, 290-299	0.9	2
776	On the Impossibility of Constructing Non-interactive Statistically-Secret Protocols from Any Trapdoor One-Way Function. *Lecture Notes in Computer Science*, **2002**, 79-95	0.9	11
775	Practical Security in Public-Key Cryptography. *Lecture Notes in Computer Science*, **2002**, 1-17	0.9	1
774	Content Extraction Signatures. *Lecture Notes in Computer Science*, **2002**, 285-304	0.9	101
773	Design and Analysis of Fast Provably Secure Public-Key Cryptosystems Based on a Modular Squaring. *Lecture Notes in Computer Science*, **2002**, 81-102	0.9	8
772	Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation. *Lecture Notes in Computer Science*, **2002**, 103-113	0.9	5
771	Subliminal-free Authentication and Signature. *Lecture Notes in Computer Science*, **1988**, 23-33	0.9	20
770	A New Probabilistic Encryption Scheme. **1988**, 415-418		2
769	Cryptanalysis of a Pseudorandom Generator Based on Braid Groups. *Lecture Notes in Computer Science*, **2002**, 1-13	0.9	5
768	On the Security of Joint Signature and Encryption. *Lecture Notes in Computer Science*, **2002**, 83-107	0.9	239
767	How to Fool an Unbounded Adversary with a Short Key. *Lecture Notes in Computer Science*, **2002**, 133-148	0.9	30
766	Non-interactive Private Auctions. *Lecture Notes in Computer Science*, **2002**, 364-377	0.9	18

765	Direct Zero Knowledge Proofs of Computational Power in Five Rounds. **1991**, 96-105		2
764	Spectral Bounds on General Hard Core Predicates. *Lecture Notes in Computer Science*, **2000**, 614-625	0.9	5
763	The Use of Interaction in Public Cryptosystems.. **1991**, 242-251		20
762	Secure Computation. **1991**, 392-404		135
761	A Cryptographic Scheme for Computerized General Elections. **1991**, 405-419		18
760	All Languages in NP Have Divertible Zero-Knowledge Proofs and Arguments Under Cryptographic Assumptions. *Lecture Notes in Computer Science*, **1991**, 1-10	0.9	7
759	Practical Zero-Knowledge Proofs: Giving Hints and Using Deficiencies. **1989**, 155-172		8
758	Sorting out zero-knowledge. **1989**, 181-191		4
757	Cryptographic Protocols Provably Secure Against Dynamic Adversaries. **1992**, 307-323		52
756	Private Information Retrieval Based on the Subgroup Membership Problem. *Lecture Notes in Computer Science*, **2001**, 206-220	0.9	10
755	Cryptographic Capsules: A Disjunctive Primitive for Interactive Protocols. **1986**, 213-222		9
754	Zero-Knowledge Simulation of Boolean Circuits. **1986**, 223-233		12
753	All-or-Nothing Disclosure of Secrets. **1986**, 234-238		60
752	A zero-knowledge Poker protocol that achieves confidentiality of the playersâ strategy or How to achieve an electronic Poker face. **1986**, 239-247		19
751	Practical Approaches to Attaining Security against Adaptively Chosen Ciphertext Attacks. **1992**, 292-304		13
750	Entity Authentication and Key Distribution. **1993**, 232-249		670
749	Another Method for Attaining Security Against Adaptively Chosen Ciphertext Attacks. **1993**, 420-434		12
748	Anonymous Authentication of Membership in Dynamic Groups. *Lecture Notes in Computer Science*, **1999**, 184-195	0.9	32

747	Blinding of Credit Card Numbers in the SET Protocol. *Lecture Notes in Computer Science*, **1999**, 17-28	0.9	5
746	Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions. *Lecture Notes in Computer Science*, **1999**, 252-269	0.9	43
745	Separability and Efficiency for Generic Group Signature Schemes. *Lecture Notes in Computer Science* , **1999**, 413-430	0.9	87
744	Can Statistical Zero Knowledge Be Made Non-interactive? or On the Relationship of SZK and NISZK. *Lecture Notes in Computer Science*, **1999**, 467-484	0.9	32
743	On the Construction of Variable-Input-Length Ciphers. *Lecture Notes in Computer Science*, **1999**, 231-244	0.9	32
742	Non-interactive Zero-Knowledge: A Low-Randomness Characterization of NP (Extended Abstract). *Lecture Notes in Computer Science*, **1999**, 271-280	0.9	8
741	Designated Confirmer Signatures and Public-Key Encryption are Equivalent. **1994**, 61-74		37
740	Coin-Based Anonymous Fingerprinting. *Lecture Notes in Computer Science*, **1999**, 150-164	0.9	27
739	New Public Key Cryptosystems Based on the Dependent-RSA Problems. *Lecture Notes in Computer Science*, **1999**, 239-254	0.9	25
738	Computationally Private Information Retrieval with Polylogarithmic Communication. *Lecture Notes in Computer Science*, **1999**, 402-414	0.9	249
737	Pseudorandom Function Tribe Ensembles Based on One-Way Permutations: Improvements and Applications. *Lecture Notes in Computer Science*, **1999**, 432-445	0.9	16
736	Conditional Oblivious Transfer and Timed-Release Encryption. *Lecture Notes in Computer Science*, **1999**, 74-89	0.9	50
735	Practice-Oriented Provable-Security. *Lecture Notes in Computer Science*, **1999**, 1-15	0.9	16
734	Universal Distributions and Time-Bounded Kolmogorov Complexity. *Lecture Notes in Computer Science*, **1999**, 434-443	0.9	2
733	Decision Oracles are Equivalent to Matching Oracles. *Lecture Notes in Computer Science*, **1999**, 276-289	0.9	6
732	On Quorum Controlled Asymmetric Proxy Re-encryption. *Lecture Notes in Computer Science*, **1999**, 112-121	0.9	45
731	Fair Off-Line e-Cash Made Easy. *Lecture Notes in Computer Science*, **1998**, 257-270	0.9	19
730	Adaptively Secure Oblivious Transfer. *Lecture Notes in Computer Science*, **1998**, 300-314	0.9	9

729	A New and Efficient All-Or-Nothing Disclosure of Secrets Protocol. *Lecture Notes in Computer Science*, **1998**, 357-371	0.9	55
728	Duality between two cryptographic primitives. *Lecture Notes in Computer Science*, **1991**, 379-390	0.9	5
727	Open problems in number theoretic complexity, II. *Lecture Notes in Computer Science*, **1994**, 291-322	0.9	27
726	Efficient Dynamic-Resharing â Verifiable Secret Sharingâ against mobile adversary. *Lecture Notes in Computer Science*, **1995**, 523-537	0.9	9
725	A progress report on subliminal-free channels. *Lecture Notes in Computer Science*, **1996**, 157-168	0.9	13
724	On characterizations of escrow encryption schemes. *Lecture Notes in Computer Science*, **1997**, 705-715	0.9	2
723	Equivocable Oblivious Transfer. *Lecture Notes in Computer Science*, **1996**, 119-130	0.9	6
722	Round-Optimal Zero-Knowledge Arguments Based on Any One-Way Function. *Lecture Notes in Computer Science*, **1997**, 280-305	0.9	28
721	Distributed â Magic Inkâ Signatures. *Lecture Notes in Computer Science*, **1997**, 450-464	0.9	23
720	Kleptography: Using Cryptography Against Cryptography. *Lecture Notes in Computer Science*, **1997**, 62-74	0.9	99
719	A Taxonomy of Proof Systems. **1997**, 109-134		2
718	Computational Information Theory. **1998**, 1-15		1
717	Perfect Zero-Knowledge Sharing Schemes over any Finite Abelian Group. **1993**, 369-378		5
716	The Varieties of Secure Distributed Computation. **1993**, 392-417		8
715	Cloud-Specific Services for Data Management. **2013**, 137-160		1
714	A Data Hiding Scheme with High Quality for H.264/AVC Video Streams. *Lecture Notes in Computer Science*, **2018**, 99-110	0.9	3
713	Homomorphic Secret Sharing for Low Degree Polynomials. *Lecture Notes in Computer Science*, **2018**, 279-309	0.9	9
712	Certifying Trapdoor Permutations, Revisited. *Lecture Notes in Computer Science*, **2018**, 476-506	0.9	11

711	Efficient Noninteractive Certification of RSA Moduli and Beyond. *Lecture Notes in Computer Science*, **2019**, 700-727	0.9	6
710	A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement. *Lecture Notes in Computer Science*, **2019**, 111-130	0.9	7
709	Provably Secure Group Authentication in the Asynchronous Communication Model. *Lecture Notes in Computer Science*, **2020**, 324-340	0.9	1
708	New Assumptions and Efficient Cryptosystems from the e-th Power Residue Symbol. *Lecture Notes in Computer Science*, **2020**, 408-424	0.9	2
707	Handling Adaptive Compromise for Practical Encryption Schemes. *Lecture Notes in Computer Science*, **2020**, 3-32	0.9	5
706	Fully Deniable Interactive Encryption. *Lecture Notes in Computer Science*, **2020**, 807-835	0.9	7
705	Chosen Ciphertext Security from Injective Trapdoor Functions. *Lecture Notes in Computer Science*, **2020**, 836-866	0.9	5
704	Can a Public Blockchain Keep a Secret?. *Lecture Notes in Computer Science*, **2020**, 260-290	0.9	25
703	Constructive t-secure Homomorphic Secret Sharing for Low Degree Polynomials. *Lecture Notes in Computer Science*, **2020**, 763-785	0.9	3
702	A Survey of Hard Core Functions. **2001**, 227-255		9
701	Probabilistic Proof Systems. **1995**, 1395-1406		5
700	Transparent Proofs and Limits to Approximation. **1994**, 31-91		10
699	Equilibrium Concepts for Rational Multiparty Computation. *Lecture Notes in Computer Science*, **2013**, 226-245	0.9	7
698	Semantically-Secure Functional Encryption: Possibility Results, Impossibility Results and the Quest for a General Definition. *Lecture Notes in Computer Science*, **2013**, 218-234	0.9	41
697	Universal Hash-Function Families: From Hashing to Authentication. *Lecture Notes in Computer Science*, **2014**, 459-474	0.9	1
696	On Updatable Redactable Signatures. *Lecture Notes in Computer Science*, **2014**, 457-475	0.9	23
695	EyeDecrypt â Private Interactions in Plain Sight. *Lecture Notes in Computer Science*, **2014**, 255-276	0.9	12
694	Publicly Evaluable Pseudorandom Functions and Their Applications. *Lecture Notes in Computer Science*, **2014**, 115-134	0.9	5

693	A Note on Quantum Security for Post-Quantum Cryptography. *Lecture Notes in Computer Science*, **2014**, 246-265	0.9	34
692	A New Public Key Encryption with Equality Test. *Lecture Notes in Computer Science*, **2014**, 550-557	0.9	8
691	Practical Receipt-Free Sealed-Bid Auction in the Coercive Environment. *Lecture Notes in Computer Science*, **2014**, 418-434	0.9	3
690	Homomorphic Encryption. **2014**, 27-46		19
689	On the Lossiness of 2k-th Power and the Instantiability of Rabin-OAEP. *Lecture Notes in Computer Science*, **2014**, 34-49	0.9	1
688	The Probabilistic Encryption Algorithm Using Linear Transformation. **2015**, 389-395		1
687	Secure and Efficient Private Set Intersection Cardinality Using Bloom Filter. *Lecture Notes in Computer Science*, **2015**, 209-226	0.9	33
686	TrustedMR: A Trusted MapReduce System Based on Tamper Resistance Hardware. *Lecture Notes in Computer Science*, **2015**, 38-56	0.9	3
685	Round-Efficient Private Stable Matching from Additive Homomorphic Encryption. *Lecture Notes in Computer Science*, **2015**, 69-86	0.9	1
684	Mitigating Server Breaches in Password-Based Authentication: Secure and Efficient Solutions. *Lecture Notes in Computer Science*, **2016**, 3-18	0.9	6
683	Deterministic Public-Key Encryption Under Continual Leakage. *Lecture Notes in Computer Science*, **2016**, 304-323	0.9	6
682	A Robust Zero-Watermarking Algorithm for Encrypted Medical Images in the DWT-DFT Encrypted Domain. **2016**, 197-208		2
681	Bounded Size-Hiding Private Set Intersection. *Lecture Notes in Computer Science*, **2016**, 449-467	0.9	5
680	Breaking into the KeyStore: A Practical Forgery Attack Against Android KeyStore. *Lecture Notes in Computer Science*, **2016**, 531-548	0.9	6
679	Searchable Symmetric Encryption Supporting Queries with Multiple-Character Wildcards. *Lecture Notes in Computer Science*, **2016**, 266-282	0.9	4
678	Computational Security of Quantum Encryption. *Lecture Notes in Computer Science*, **2016**, 47-71	0.9	14
677	Encoding-Free ElGamal-Type Encryption Schemes on Elliptic Curves. *Lecture Notes in Computer Science*, **2017**, 19-35	0.9	2
676	A Note on Perfect Correctness by Derandomization. *Lecture Notes in Computer Science*, **2017**, 592-606	0.9	13

675	Another Look at Tightness II: Practical Issues in Cryptography. *Lecture Notes in Computer Science*, **2017**, 21-55	0.9	8
674	A Formal Treatment of Multi-key Channels. *Lecture Notes in Computer Science*, **2017**, 587-618	0.9	9
673	Preliminaries. **2017**, 3-30		1
672	Factoring Based Cryptography. **2019**, 217-286		4
671	Public-Key Encryption Resistant to Parameter Subversion and Its Realization from Efficiently-Embeddable Groups. *Lecture Notes in Computer Science*, **2018**, 348-377	0.9	16
670	Semantically Secure Anonymity: Foundations of Re-encryption. *Lecture Notes in Computer Science*, **2018**, 255-273	0.9	1
669	A Password-Based Authenticator: Security Proof and Applications. *Lecture Notes in Computer Science*, **2003**, 388-401	0.9	8
668	On the Security of Multiple Encryption or CCA-security+CCA-security=CCA-security?. *Lecture Notes in Computer Science*, **2004**, 360-374	0.9	23
667	Undeniable Signatures Based on Characters: How to Sign with One Bit. *Lecture Notes in Computer Science*, **2004**, 69-85	0.9	18
666	Alternatives to Non-malleability: Definitions, Constructions, and Applications. *Lecture Notes in Computer Science*, **2004**, 171-190	0.9	52
665	A Universally Composable Mix-Net. *Lecture Notes in Computer Science*, **2004**, 317-335	0.9	46
664	A General Composition Theorem for Secure Reactive Systems. *Lecture Notes in Computer Science*, **2004**, 336-354	0.9	46
663	Simpler Session-Key Generation from Short Random Passwords. *Lecture Notes in Computer Science*, **2004**, 428-445	0.9	16
662	Five Practical Attacks for â□Optimistic Mixing for Exit-Pollsâ□ *Lecture Notes in Computer Science*, **2004**, 160-174	0.9	15
661	Immunizing Encryption Schemes from Decryption Errors. *Lecture Notes in Computer Science*, **2004**, 342-360	0.9	45
660	Probabilistic Bisimulation and Equivalence for Security Analysis of Network Protocols. *Lecture Notes in Computer Science*, **2004**, 468-483	0.9	19
659	Private Fingerprint Verification without Local Storage. *Lecture Notes in Computer Science*, **2004**, 387-394	0.9	12
658	Protocols with Security Proofs for Mobile Applications. *Lecture Notes in Computer Science*, **2004**, 358-369	0.9	10

657	Selecting Correlated Random Actions. *Lecture Notes in Computer Science*, **2004**, 181-195	0.9	5
656	Deciding Knowledge in Security Protocols Under Equational Theories. *Lecture Notes in Computer Science*, **2004**, 46-58	0.9	26
655	Constant-Round Resettable Zero Knowledge with Concurrent Soundness in the Bare Public-Key Model. *Lecture Notes in Computer Science*, **2004**, 237-253	0.9	34
654	Certified E-Mail with Temporal Authentication: An Improved Optimistic Protocol. *Lecture Notes in Computer Science*, **2004**, 181-190	0.9	2
653	A Public-Key Encryption Scheme with Pseudo-random Ciphertexts. *Lecture Notes in Computer Science*, **2004**, 335-351	0.9	23
652	Practical Two-Party Computation Based on the Conditional Gate. *Lecture Notes in Computer Science*, **2004**, 119-136	0.9	55
651	Generic Homomorphic Undeniable Signatures. *Lecture Notes in Computer Science*, **2004**, 354-371	0.9	21
650	OAEP 3-Round:A Generic and Secure Asymmetric Encryption Padding. *Lecture Notes in Computer Science*, **2004**, 63-77	0.9	24
649	Fair-Zero Knowledge. *Lecture Notes in Computer Science*, **2005**, 245-263	0.9	13
648	Sufficient Conditions for Collision-Resistant Hashing. *Lecture Notes in Computer Science*, **2005**, 445-456	0.9	24
647	Cryptography in Subgroups of (mathbb{Z}_{n}^{*}). *Lecture Notes in Computer Science*, **2005**, 50-65	0.9	31
646	Adaptively-Secure, Non-interactive Public-Key Encryption. *Lecture Notes in Computer Science*, **2005**, 150-168	0.9	41
645	On the Security Notions for Public-Key Encryption Schemes. *Lecture Notes in Computer Science*, **2005**, 33-46	0.9	6
644	Completing the Picture: Soundness of Formal Encryption in the Presence of Active Adversaries. *Lecture Notes in Computer Science*, **2005**, 172-185	0.9	23
643	A Formal System for Analysis of Cryptographic Encryption and Their Security Properties. *Lecture Notes in Computer Science*, **2004**, 87-112	0.9	3
642	Initiator-Resilient Universally Composable Key Exchange. *Lecture Notes in Computer Science*, **2003**, 61-84	0.9	15
641	Practical Symmetric On-Line Encryption. *Lecture Notes in Computer Science*, **2003**, 362-375	0.9	13
640	Chosen-Ciphertext Security without Redundancy. *Lecture Notes in Computer Science*, **2003**, 1-18	0.9	20

639	A General Construction of IND-CCA2 Secure Public Key Encryption. *Lecture Notes in Computer Science*, **2003**, 152-166	0.9	12
638	Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. *Lecture Notes in Computer Science*, **2003**, 103-121	0.9	133
637	Weak Key Authenticity and the Computational Completeness of Formal Encryption. *Lecture Notes in Computer Science*, **2003**, 530-547	0.9	11
636	Plaintext Awareness via Key Registration. *Lecture Notes in Computer Science*, **2003**, 548-564	0.9	42
635	Computational Analogues of Entropy. *Lecture Notes in Computer Science*, **2003**, 200-215	0.9	49
634	Chosen-Ciphertext Security for Any One-Way Cryptosystem. *Lecture Notes in Computer Science*, **2000**, 129-146	0.9	55
633	Multi-factor Authenticated Key Exchange. *Lecture Notes in Computer Science*, **2008**, 277-295	0.9	42
632	Homomorphic Encryption with CCA Security. *Lecture Notes in Computer Science*, **2008**, 667-678	0.9	25
631	How to Encrypt with the LPN Problem. *Lecture Notes in Computer Science*, **2008**, 679-690	0.9	39
630	An Indistinguishability-Based Characterization of Anonymous Channels. *Lecture Notes in Computer Science*, **2008**, 24-43	0.9	24
629	Securely Obfuscating Re-encryption. **2007**, 233-252		81
628	Towards a Separation of Semantic and CCA Security for Public Key Encryption. **2007**, 434-455		41
627	How to Encrypt with a Malicious Random Number Generator. *Lecture Notes in Computer Science*, **2008**, 303-315	0.9	9
626	A Survey of Single-Database Private Information Retrieval: Techniques and Applications. *Lecture Notes in Computer Science*, **2007**, 393-411	0.9	121
625	A Closer Look at PKI: Security and Efficiency. **2007**, 458-475		27
624	Optimistic Fair Exchange in a Multi-user Setting. **2007**, 118-133		43
623	Conditional Computational Entropy, or Toward Separating Pseudoentropy from Compressibility. *Lecture Notes in Computer Science*, **2007**, 169-186	0.9	45
622	Privacy-Preserving Set Union. *Lecture Notes in Computer Science*, **2007**, 237-252	0.9	31

621	Unlinkable Secret Handshakes and Key-Private Group Key Management Schemes. *Lecture Notes in Computer Science*, **2007**, 270-287	0.9	30
620	Tweaking TBE/IBE to PKE Transforms with Chameleon Hash Functions. *Lecture Notes in Computer Science*, **2007**, 323-339	0.9	22
619	A âÞroof-readingâÐof Some Issues in Cryptography. *Lecture Notes in Computer Science*, **2007**, 2-11	0.9	7
618	Offline/Online Mixing. *Lecture Notes in Computer Science*, **2007**, 484-495	0.9	11
617	Construction of Threshold (Hybrid) Encryption in the Random Oracle Model: How to Construct Secure Threshold Tag-KEM from Weakly Secure Threshold KEM. **2007**, 259-273		2
616	Efficient Chosen-Ciphertext Secure Identity-Based Encryption with Wildcards. **2007**, 274-292		11
615	Provably-Secure Schemes for Basic Query Support in Outsourced Databases. *Lecture Notes in Computer Science*, **2007**, 14-30	0.9	23
614	Invertible Universal Hashing and the TET Encryption Mode. **2007**, 412-429		31
613	Efficient Provably-Secure Hierarchical Key Assignment Schemes. *Lecture Notes in Computer Science*, **2007**, 371-382	0.9	14
612	Dial C for Cipher. *Lecture Notes in Computer Science*, **2007**, 76-95	0.9	7
611	On the Privacy of Concealed Data Aggregation. *Lecture Notes in Computer Science*, **2007**, 390-405	0.9	5
610	Game-Based Criterion Partition Applied to Computational Soundness of Adaptive Security. *Lecture Notes in Computer Science*, **2007**, 47-64	0.9	1
609	Trapdoor Permutation Polynomials of Z/nZ and Public Key Cryptosystems. *Lecture Notes in Computer Science*, **2007**, 333-350	0.9	1
608	A Generalization and a Variant of Two Threshold Cryptosystems Based on Factoring. *Lecture Notes in Computer Science*, **2007**, 351-361	0.9	1
607	Towards a DL-Based Additively Homomorphic Encryption Scheme. *Lecture Notes in Computer Science*, **2007**, 362-375	0.9	2
606	Two-Party Computing with Encrypted Data. **2007**, 298-314		15
605	Bounded CCA2-Secure Encryption. *Lecture Notes in Computer Science*, **2007**, 502-518	0.9	57
604	Relations Among Notions of Non-malleability for Encryption. **2007**, 519-535		21

603	On Privacy Models for RFID. *Lecture Notes in Computer Science*, **2007**, 68-87	0.9	216
602	Generic Combination of Public Key Encryption with Keyword Search and Public Key Encryption. **2007**, 159-174		23
601	A Framework for Game-Based Security Proofs. *Lecture Notes in Computer Science*, **2007**, 319-333	0.9	19
600	An Ad Omnia Approach to Defining and Achieving Private Data Analysis. **2007**, 1-13		15
599	Cryptography and Data Hiding for Media Security. **2008**, 227-255		1
598	Black-Box Construction of a Non-malleable Encryption Scheme from Any Semantically Secure One. **2008**, 427-444		33
597	Obfuscating Point Functions with Multibit Output. **2008**, 489-508		68
596	Towards Key-Dependent Message Security in the Standard Model. **2008**, 108-126		33
595	Computational Soundness of Non-Malleable Commitments. *Lecture Notes in Computer Science*, **2008**, 361-376	0.9	4
594	Dynamic Threshold Public-Key Encryption. *Lecture Notes in Computer Science*, **2008**, 317-334	0.9	49
593	Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles. *Lecture Notes in Computer Science*, **2008**, 360-378	0.9	94
592	Communication Complexity in Algebraic Two-Party Protocols. *Lecture Notes in Computer Science*, **2008**, 379-396	0.9	6
591	Circular-Secure Encryption from Decision Diffie-Hellman. *Lecture Notes in Computer Science*, **2008**, 108-125	0.9	160
590	Public-Key Locally-Decodable Codes. *Lecture Notes in Computer Science*, **2008**, 126-143	0.9	21
589	PBS: Private Bartering Systems. *Lecture Notes in Computer Science*, **2008**, 113-127	0.9	6
588	Linear Bandwidth Naccache-Stern Encryption. *Lecture Notes in Computer Science*, **2008**, 327-339	0.9	8
587	New Anonymity Notions for Identity-Based Encryption. *Lecture Notes in Computer Science*, **2008**, 375-391	0.9	6
586	Peer-to-Peer Private Information Retrieval. *Lecture Notes in Computer Science*, **2008**, 315-323	0.9	8

585	Towards a Concrete Security Proof of Courtois, Finiasz and Sendrier Signature Scheme. *Lecture Notes in Computer Science*, **2008**, 65-77	0.9	21
584	A CCA Secure Hybrid Damgâ ElGamal Encryption. *Lecture Notes in Computer Science*, **2008**, 68-82	0.9	5
583	Practical Insecurity for Effective Steganalysis. *Lecture Notes in Computer Science*, **2008**, 195-208	0.9	2
582	Efficient Chosen Ciphertext Secure Public Key Encryption under the Computational Diffie-Hellman Assumption. *Lecture Notes in Computer Science*, **2008**, 308-325	0.9	57
581	Chosen Ciphertext Security with Optimal Ciphertext Overhead. *Lecture Notes in Computer Science*, **2008**, 355-371	0.9	15
580	OAEP Is Secure under Key-Dependent Messages. *Lecture Notes in Computer Science*, **2008**, 506-523	0.9	25
579	Quantum Cryptography. **2012**, 1521-1543		1
578	Simultaneous Hardcore Bits and Cryptography against Memory Attacks. *Lecture Notes in Computer Science*, **2009**, 474-495	0.9	264
577	Compact CCA-Secure Encryption for Messages of Arbitrary Length. *Lecture Notes in Computer Science*, **2009**, 377-392	0.9	10
576	On Formal Verification of Arithmetic-Based Cryptographic Primitives. *Lecture Notes in Computer Science*, **2009**, 368-382	0.9	3
575	A CCA2 Secure Public Key Encryption Scheme Based on the McEliece Assumptions in the Standard Model. *Lecture Notes in Computer Science*, **2009**, 240-251	0.9	22
574	Possibility and Impossibility Results for Encryption and Commitment Secure under Selective Opening. *Lecture Notes in Computer Science*, **2009**, 1-35	0.9	152
573	Practical Chosen Ciphertext Secure Encryption from Factoring. *Lecture Notes in Computer Science*, **2009**, 313-332	0.9	76
572	The Power of Anonymous Veto in Public Discussion. *Lecture Notes in Computer Science*, **2009**, 41-52	0.9	5
571	Formal Certification of ElGamal Encryption. *Lecture Notes in Computer Science*, **2009**, 1-19	0.9	4
570	New Anonymity Notions for Identity-Based Encryption. *Lecture Notes in Computer Science*, **2009**, 138-157	0.9	3
569	Cryptographic Functions from Worst-Case Complexity Assumptions. **2009**, 427-452		1
568	Models and Proofs of Protocol Security: A Progress Report. *Lecture Notes in Computer Science*, **2009**, 35-49	0.9	52

567	Public-Key Cryptosystems Resilient to Key Leakage. *Lecture Notes in Computer Science*, **2009**, 18-35	0.9	233
566	The Group of Signed Quadratic Residues and Applications. *Lecture Notes in Computer Science*, **2009**, 637-653	0.9	57
565	Smooth Projective Hashing for Conditionally Extractable Commitments. *Lecture Notes in Computer Science*, **2009**, 671-689	0.9	53
564	Coercion Resistant End-to-end Voting. *Lecture Notes in Computer Science*, **2009**, 344-361	0.9	11
563	Relations Among Privacy Notions. *Lecture Notes in Computer Science*, **2009**, 362-380	0.9	6
562	Security and Tradeoffs of the Akl-Taylor Scheme and Its Variants. *Lecture Notes in Computer Science* , **2009**, 247-257	0.9	7
561	Towards Security Notions for White-Box Cryptography. *Lecture Notes in Computer Science*, **2009**, 49-58	0.9	15
560	Chosen-Ciphertext Secure RSA-Type Cryptosystems. *Lecture Notes in Computer Science*, **2009**, 32-46	0.9	5
559	A 2-Round Anonymous Veto Protocol. *Lecture Notes in Computer Science*, **2009**, 202-211	0.9	23
558	Hedged Public-Key Encryption: How to Protect against Bad Randomness. *Lecture Notes in Computer Science*, **2009**, 232-249	0.9	89
557	Improved Non-committing Encryption with Applications to Adaptively Secure Protocols. *Lecture Notes in Computer Science*, **2009**, 287-302	0.9	52
556	Anonymizer-Enabled Security and Privacy for RFID. *Lecture Notes in Computer Science*, **2009**, 134-153	0.9	15
555	A Twist on the Naor-Yung Paradigm and Its Application to Efficient CCA-Secure Encryption from Hard Search Problems. *Lecture Notes in Computer Science*, **2010**, 146-164	0.9	14
554	Robust Encryption. *Lecture Notes in Computer Science*, **2010**, 480-497	0.9	63
553	Plaintext-Awareness of Hybrid Encryption. *Lecture Notes in Computer Science*, **2010**, 57-72	0.9	5
552	Encryption Schemes Secure against Chosen-Ciphertext Selective Opening Attacks. *Lecture Notes in Computer Science*, **2010**, 381-402	0.9	56
551	Cryptographic Agility and Its Relation to Circular Encryption. *Lecture Notes in Computer Science*, **2010**, 403-422	0.9	44
550	Adaptive Trapdoor Functions and Chosen-Ciphertext Security. *Lecture Notes in Computer Science*, **2010**, 673-692	0.9	60

549	Efficient Implementation of the Orlandi Protocol. *Lecture Notes in Computer Science*, **2010**, 255-272	0.9	10
548	Relations among Notions of Complete Non-malleability: Indistinguishability Characterisation and Efficient Construction without Random Oracles. *Lecture Notes in Computer Science*, **2010**, 145-163	0.9	6
547	Proof-of-Knowledge of Representation of Committed Value and Its Applications. *Lecture Notes in Computer Science*, **2010**, 352-369	0.9	6
546	Towards Reliable Remote Healthcare Applications Using Combined Fuzzy Extraction. **2010**, 387-407		3
545	Collaborative, Privacy-Preserving Data Aggregation at Scale. *Lecture Notes in Computer Science*, **2010**, 56-74	0.9	19
544	Circular and Leakage Resilient Public-Key Encryption under Subgroup Indistinguishability. *Lecture Notes in Computer Science*, **2010**, 1-20	0.9	97
543	Efficient Chosen-Ciphertext Security via Extractable Hash Proofs. *Lecture Notes in Computer Science* , **2010**, 314-332	0.9	58
542	Securing Computation against Continuous Leakage. *Lecture Notes in Computer Science*, **2010**, 59-79	0.9	46
541	Additively Homomorphic Encryption with d-Operand Multiplications. *Lecture Notes in Computer Science*, **2010**, 138-154	0.9	23
540	i-Hop Homomorphic Encryption and Rerandomizable Yao Circuits. *Lecture Notes in Computer Science*, **2010**, 155-172	0.9	62
539	Mediated Traceable Anonymous Encryption. *Lecture Notes in Computer Science*, **2010**, 40-60	0.9	9
538	How to Evaluate the Security of Real-Life Cryptographic Protocols?. *Lecture Notes in Computer Science*, **2010**, 182-194	0.9	12
537	Generic Constructions of Parallel Key-Insulated Encryption. *Lecture Notes in Computer Science*, **2010** , 36-53	0.9	6
536	Computationally Efficient Searchable Symmetric Encryption. *Lecture Notes in Computer Science*, **2010**, 87-100	0.9	93
535	A Calculus for Game-Based Security Proofs. *Lecture Notes in Computer Science*, **2010**, 35-52	0.9	8
534	Computationally Private Randomizing Polynomials and Their Applications. **2014**, 79-106		1
533	A Closer Look at Anonymity and Robustness in Encryption Schemes. *Lecture Notes in Computer Science*, **2010**, 501-518	0.9	22
532	Structured Encryption and Controlled Disclosure. *Lecture Notes in Computer Science*, **2010**, 577-594	0.9	196

531	Parallel Decryption Queries in Bounded Chosen Ciphertext Attacks. *Lecture Notes in Computer Science*, **2011**, 246-264	0.9	4
530	Homomorphic Encryption: From Private-Key to Public-Key. *Lecture Notes in Computer Science*, **2011**, 219-234	0.9	30
529	Identity-Based Encryption Secure against Selective Opening Attack. *Lecture Notes in Computer Science*, **2011**, 235-252	0.9	54
528	On the Black-Box Complexity of Optimally-Fair Coin Tossing. *Lecture Notes in Computer Science*, **2011**, 450-467	0.9	26
527	Towards Non-Black-Box Lower Bounds in Cryptography. *Lecture Notes in Computer Science*, **2011**, 579-596	0.9	12
526	Key-Dependent Message Security: Generic Amplification and Completeness. *Lecture Notes in Computer Science*, **2011**, 527-546	0.9	52
525	Deniable Encryption with Negligible Detection Probability: An Interactive Construction. *Lecture Notes in Computer Science*, **2011**, 610-626	0.9	19
524	Fully Leakage-Resilient Signatures. *Lecture Notes in Computer Science*, **2011**, 89-108	0.9	54
523	A Practical (Non-interactive) Publicly Verifiable Secret Sharing Scheme. *Lecture Notes in Computer Science*, **2011**, 273-287	0.9	7
522	Public-Key Encrypted Bloom Filters with Applications to Supply Chain Integrity. *Lecture Notes in Computer Science*, **2011**, 60-75	0.9	5
521	Generic Construction of Strongly Secure Timed-Release Public-Key Encryption. *Lecture Notes in Computer Science*, **2011**, 319-336	0.9	6
520	Three XOR-Lemmas â An Exposition. *Lecture Notes in Computer Science*, **2011**, 248-272	0.9	12
519	Randomness and Computation. *Lecture Notes in Computer Science*, **2011**, 507-539	0.9	1
518	Authenticated and Misuse-Resistant Encryption of Key-Dependent Data. *Lecture Notes in Computer Science*, **2011**, 610-629	0.9	11
517	Robust Watermarking of Compressed JPEG Images in Encrypted Domain. *Lecture Notes in Computer Science*, **2011**, 37-57	0.9	1
516	Research on Secure Multi-party Computational Geometry. *Lecture Notes in Computer Science*, **2011**, 322-329	0.9	2
515	Publicly Verifiable Secret Sharing for Cloud-Based Key Management. *Lecture Notes in Computer Science*, **2011**, 290-309	0.9	5
514	A Computational Indistinguishability Logic for the Bounded Storage Model. *Lecture Notes in Computer Science*, **2012**, 102-117	0.9	4

513	Security Protocol Verification: Symbolic and Computational Models. *Lecture Notes in Computer Science*, **2012**, 3-29	0.9	35
512	Confidentiality and Integrity: A Constructive Perspective. *Lecture Notes in Computer Science*, **2012**, 209-229	0.9	16
511	Subspace LWE. *Lecture Notes in Computer Science*, **2012**, 548-563	0.9	18
510	Bounded-Collusion IBE from Key Homomorphism. *Lecture Notes in Computer Science*, **2012**, 564-581	0.9	15
509	A Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy. *Lecture Notes in Computer Science*, **2012**, 582-599	0.9	43
508	All-But-Many Lossy Trapdoor Functions. *Lecture Notes in Computer Science*, **2012**, 209-227	0.9	48
507	Incremental Deterministic Public-Key Encryption. *Lecture Notes in Computer Science*, **2012**, 628-644	0.9	35
506	Standard Security Does Not Imply Security against Selective-Opening. *Lecture Notes in Computer Science*, **2012**, 645-662	0.9	49
505	Detecting Dangerous Queries: A New Approach for Chosen Ciphertext Security. *Lecture Notes in Computer Science*, **2012**, 663-681	0.9	31
504	On Definitions of Selective Opening Security. *Lecture Notes in Computer Science*, **2012**, 522-539	0.9	35
503	New Definitions and Separations for Circular Security. *Lecture Notes in Computer Science*, **2012**, 540-557	0.9	28
502	SmartTokens: Delegable Access Control with NFC-Enabled Smartphones. *Lecture Notes in Computer Science*, **2012**, 219-238	0.9	19
501	PRISM â Privacy-Preserving Search in MapReduce. *Lecture Notes in Computer Science*, **2012**, 180-200	0.9	31
500	Reaction Attack on Outsourced Computing with Fully Homomorphic Encryption Schemes. *Lecture Notes in Computer Science*, **2012**, 419-436	0.9	6
499	Strong Security Notions for Timed-Release Public-Key Encryption Revisited. *Lecture Notes in Computer Science*, **2012**, 88-108	0.9	6
498	On the Amortized Complexity of Zero Knowledge Protocols for Multiplicative Relations. *Lecture Notes in Computer Science*, **2012**, 62-79	0.9	13
497	Shannon Impossibility, Revisited. *Lecture Notes in Computer Science*, **2012**, 100-110	0.9	11
496	Selective Document Retrieval from Encrypted Database. *Lecture Notes in Computer Science*, **2012**, 224-241	0.9	16

495	McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes. *Lecture Notes in Computer Science*, **2012**, 196-215	0.9	62
494	Strong Privacy for RFID Systems from Plaintext-Aware Encryption. *Lecture Notes in Computer Science*, **2012**, 247-262	0.9	9
493	On the Semantic Security of Functional Encryption Schemes. *Lecture Notes in Computer Science*, **2013**, 143-161	0.9	18
492	Functional Encryption: Origins and Recent Developments. *Lecture Notes in Computer Science*, **2013**, 51-54	0.9	9
491	Computational Soundness of Coinductive Symbolic Security under Active Attacks. *Lecture Notes in Computer Science*, **2013**, 539-558	0.9	3
490	Private Over-Threshold Aggregation Protocols. *Lecture Notes in Computer Science*, **2013**, 472-486	0.9	3
489	Message-Locked Encryption and Secure Deduplication. *Lecture Notes in Computer Science*, **2013**, 296-312	0.9	197
488	Regularity of Lossy RSA on Subdomains and Its Applications. *Lecture Notes in Computer Science*, **2013**, 55-75	0.9	8
487	Efficient Cryptosystems from 2k-th Power Residue Symbols. *Lecture Notes in Computer Science*, **2013**, 76-92	0.9	37
486	Deterministic Public-Key Encryption for Adaptively Chosen Plaintext Distributions. *Lecture Notes in Computer Science*, **2013**, 93-110	0.9	35
485	Efficient and Private Three-Party Publish/Subscribe. *Lecture Notes in Computer Science*, **2013**, 278-292	0.9	5
484	Key-Dependent Message Chosen-Ciphertext Security of the Cramer-Shoup Cryptosystem. *Lecture Notes in Computer Science*, **2013**, 136-151	0.9	1
483	Plug-and-Play IP Security. *Lecture Notes in Computer Science*, **2013**, 255-272	0.9	7
482	Constructing Confidential Channels from Authenticated Channelsâ Public-Key Encryption Revisited. *Lecture Notes in Computer Science*, **2013**, 134-153	0.9	13
481	Secure Two-Party Computation with Reusable Bit-Commitments, via a Cut-and-Choose with Forge-and-Lose Technique. *Lecture Notes in Computer Science*, **2013**, 441-463	0.9	17
480	An Encrypted In-Memory Column-Store: The Onion Selection Problem. *Lecture Notes in Computer Science*, **2013**, 14-26	0.9	3
479	A Leakage-Resilient Pairing-Based Variant of the Schnorr Signature Scheme. *Lecture Notes in Computer Science*, **2013**, 173-192	0.9	3
478	Can Optimally-Fair Coin Tossing Be Based on One-Way Functions?. *Lecture Notes in Computer Science*, **2014**, 217-239	0.9	14

477	Standard versus Selective Opening Security: Separation and Equivalence Results. *Lecture Notes in Computer Science*, **2014**, 591-615	0.9	24
476	4-Round Resettably-Sound Zero Knowledge. *Lecture Notes in Computer Science*, **2014**, 192-216	0.9	16
475	Bounded-Collusion Identity-Based Encryption from Semantically-Secure Public-Key Encryption: Generic Constructions with Short Ciphertexts. *Lecture Notes in Computer Science*, **2014**, 257-274	0.9	11
474	Enhanced Chosen-Ciphertext Security and Applications. *Lecture Notes in Computer Science*, **2014**, 329-344	0.9	7
473	Encryption Schemes Secure under Related-Key and Key-Dependent Message Attacks. *Lecture Notes in Computer Science*, **2014**, 483-500	0.9	10
472	A Black-Box Construction of a CCA2 Encryption Scheme from a Plaintext Aware (sPA1) Encryption Scheme. *Lecture Notes in Computer Science*, **2014**, 37-55	0.9	7
471	General Impossibility of Group Homomorphic Encryption in the Quantum World. *Lecture Notes in Computer Science*, **2014**, 556-573	0.9	10
470	On Probabilistic Applicative Bisimulation and Call-by-Value □Calculi. *Lecture Notes in Computer Science*, **2014**, 209-228	0.9	22
469	Reconsidering Generic Composition. *Lecture Notes in Computer Science*, **2014**, 257-274	0.9	65
468	Honey Encryption: Security Beyond the Brute-Force Bound. *Lecture Notes in Computer Science*, **2014**, 293-310	0.9	38
467	The Foundations of Modern Cryptography. **1999**, 1-37		5
466	On Minimizing the Size of Encrypted Databases. *Lecture Notes in Computer Science*, **2014**, 364-372	0.9	2
465	Maliciously Circuit-Private FHE. *Lecture Notes in Computer Science*, **2014**, 536-553	0.9	26
464	Authenticating Computation on Groups: New Homomorphic Primitives and Applications. *Lecture Notes in Computer Science*, **2014**, 193-212	0.9	20
463	Secret-Sharing for NP. *Lecture Notes in Computer Science*, **2014**, 254-273	0.9	15
462	Adaptive Security of Constrained PRFs. *Lecture Notes in Computer Science*, **2014**, 82-101	0.9	32
461	Poly-Many Hardcore Bits for Any One-Way Function and a Framework for Differing-Inputs Obfuscation. *Lecture Notes in Computer Science*, **2014**, 102-121	0.9	28
460	Adaptive Witness Encryption and Asymmetric Password-Based Cryptography. *Lecture Notes in Computer Science*, **2015**, 308-331	0.9	12

459	Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks. *Lecture Notes in Computer Science*, **2015**, 332-352	0.9	31
458	How Secure is Deterministic Encryption?. *Lecture Notes in Computer Science*, **2015**, 52-73	0.9	6
457	From Single-Bit to Multi-bit Public-Key Encryption via Non-malleable Codes. *Lecture Notes in Computer Science*, **2015**, 532-560	0.9	39
456	Separations in Circular Security for Arbitrary Length Key Cycles. *Lecture Notes in Computer Science*, **2015**, 378-400	0.9	18
455	Obfuscation of Probabilistic Circuits and Applications. *Lecture Notes in Computer Science*, **2015**, 468-497	0.9	69
454	Multi-Client Verifiable Computation with Stronger Security Guarantees. *Lecture Notes in Computer Science*, **2015**, 144-168	0.9	30
453	Universal Signature Aggregators. *Lecture Notes in Computer Science*, **2015**, 3-34	0.9	24
452	Resisting Randomness Subversion: Fast Deterministic and Hedged Public-Key Encryption in the Standard Model. *Lecture Notes in Computer Science*, **2015**, 627-656	0.9	38
451	Privacy Preserving Collaborative Filtering from Asymmetric Randomized Encoding. *Lecture Notes in Computer Science*, **2015**, 459-477	0.9	8
450	Zeroizing Without Low-Level Zeroes: New MMAP Attacks and their Limitations. *Lecture Notes in Computer Science*, **2015**, 247-266	0.9	81
449	Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. *Lecture Notes in Computer Science*, **2015**, 609-629	0.9	37
448	Oblivious Transfer from Weakly Random Self-Reducible Public-Key Cryptosystem. *Lecture Notes in Computer Science*, **2015**, 261-273	0.9	1
447	Selective Opening Security for Receivers. *Lecture Notes in Computer Science*, **2015**, 443-469	0.9	22
446	Non-Malleable Encryption: Simpler, Shorter, Stronger. *Lecture Notes in Computer Science*, **2016**, 306-335	0.9	29
445	Chosen-Ciphertext Security from Subset Sum. *Lecture Notes in Computer Science*, **2016**, 35-46	0.9	4
444	Deniable Functional Encryption. *Lecture Notes in Computer Science*, **2016**, 196-222	0.9	7
443	Identity-Based Cryptosystems and Quadratic Residuosity. *Lecture Notes in Computer Science*, **2016**, 225-254	0.9	3
442	Easing Coppersmith Methods Using Analytic Combinatorics: Applications to Public-Key Cryptography with Weak Pseudorandomness. *Lecture Notes in Computer Science*, **2016**, 36-66	0.9	5

441	On Generic Constructions of Circularly-Secure, Leakage-Resilient Public-Key Encryption Schemes. *Lecture Notes in Computer Science*, **2016**, 129-158	0.9	4
440	KDM-Security via Homomorphic Smooth Projective Hashing. *Lecture Notes in Computer Science*, **2016**, 159-179	0.9	17
439	On the Power of Hierarchical Identity-Based Encryption. *Lecture Notes in Computer Science*, **2016**, 243-272	2.9	6
438	Practical Order-Revealing Encryption with Limited Leakage. *Lecture Notes in Computer Science*, **2016**, 474-493	0.9	79
437	Quantum Homomorphic Encryption for Polynomial-Sized Circuits. *Lecture Notes in Computer Science* , **2016**, 3-32	0.9	21
436	Semantic Security and Indistinguishability in the Quantum World. *Lecture Notes in Computer Science* , **2016**, 60-89	0.9	24
435	Optimal Fair Computation. *Lecture Notes in Computer Science*, **2016**, 143-157	0.9	2
434	Efficient KDM-CCA Secure Public-Key Encryption for Polynomial Functions. *Lecture Notes in Computer Science*, **2016**, 307-338	0.9	12
433	Separating IND-CPA and Circular Security for Unbounded Length Key Cycles. *Lecture Notes in Computer Science*, **2017**, 232-246	0.9	4
432	Metric Reasoning About (lambda)-Terms: The General Case. *Lecture Notes in Computer Science*, **2017**, 341-367	0.9	4
431	Beyond the Turing Machine. **1995**, 387-402		1
430	A Survey of Number Theory and Cryptography. **2000**, 217-239		2
429	Low-Size Cipher Text Homomorphic Encryption Scheme for Cloud Data. **2018**, 93-102		1
428	A New Encryption Approach Based on Four-Square and Zigzag Encryption (C4CZ). **2020**, 589-597		3
427	The Hunting of the SNARK. *Journal of Cryptology*, **2017**, 30, 989-1066	2.1	30
426	Hopes, fears, and software obfuscation. **2016**, 59, 88-96		17
425	Computational Extensive-Form Games. **2016**,		5
424	A lambda-calculus foundation for universal probabilistic programming. **2016**,		33

423	A lambda-calculus foundation for universal probabilistic programming. **2016**, 51, 33-46	5
422	Processing Over Encrypted Data. **2016**, 45, 5-16	5
421	Homomorphic Encryption for Machine Learning in Medicine and Bioinformatics. **2020**, 53, 1-35	20
420	PANDA. **2020**, 11, 1-41	2
419	Universally Composable Security. **2020**, 67, 1-94	20
418	Privacy-preserving auditable token payments in a permissioned blockchain system. **2020**,	14
417	Anonymous Fingerprinting with Robust QIM Watermarking Techniques. **2007**, 2007, 031340	6
416	Oblivious Neural Network Computing via Homomorphic Encryption. **2007**, 2007, 037343	26
415	Protection and Retrieval of Encrypted Multimedia Content: When Cryptography Meets Signal Processing. **2007**, 2007, 078943	27
414	Embedding edit distance to enable private keyword search. **2012**, 2, 2	16
413	Efficient and anonymous two-factor user authentication in wireless sensor networks: achieving user anonymity with lightweight sensor computation. **2015**, 10, e0116709	49
412	Obscure. **2019**, 12, 1030-1043	2
411	Formal Security Treatments for IBE-to-Signature Transformation: Relations among Security Notions. **2009**, E92-A, 53-66	9
410	Methods for Restricting Message Space in Public-Key Encryption. **2013**, E96.A, 1156-1168	6
409	Website Fingerprinting with Website Oracles. **2020**, 2020, 235-255	9
408	SoK: Differential privacies. **2020**, 2020, 288-313	10
407	Belief Multiset Formalism for Cryptographic Protocol Analysis. **2009**, 20, 3060-3076	4
406	Computer Simulation: A Hybrid Model for Traffic Signal Optimisation. **2011**, 7, 1-16	9

405	Generic Constructions for Strong Designated Verifier Signature. **2011**, 7, 159-172		6
404	Threats and Security Issues in Smart City Devices. **2019**, 220-250		7
403	Homomorphic Encryption as a Service for Outsourced Images in Mobile Cloud Computing Environment. **2020**, 316-330		5
402	Improved Methodology to Detect Advanced Persistent Threat Attacks. **2020**, 184-202		2
401	COMPRESS MULTIPLE CIPHERTEXTS USING ELGAMAL ENCRYPTION SCHEMES. **2013**, 50, 361-377		3
400	A Homomorphic Crypto System for Electronic Election Schemes. **2016**, 07, 3193-3203		3
399	Novel Scheme for Compressed Image Authentication Using LSB Watermarking and EMRC6 Encryption. **2016**, 07, 1722-1733		10
398	Neural-Based Adversarial Encryption of Images in ECB Mode with 16-Bit Blocks. **2021**, 425-435		
397	A Fragile Watermarking in Ciphertext Domain Based on Multi-Permutation Superposition Coding for Remote Sensing Image. **2021**,		1
396	Pseudorandomness. *Lecture Notes in Computer Science*, **2000**, 687-704	0.9	1
395	Information Security, Mathematics, and Public-Key Cryptography. **2000**, 7-29		
394	Steganography Using Modern Arts. *Lecture Notes in Computer Science*, **2000**, 140-151	0.9	
393	Taming the Adversary. *Lecture Notes in Computer Science*, **2000**, 353-358	0.9	1
392	Equitability in Retroactive Data Confiscation versus Proactive Key Escrow. *Lecture Notes in Computer Science*, **2001**, 277-286	0.9	1
391	A New Aspect for Security Notions: Secure Randomness in Public-Key Encryption Schemes. *Lecture Notes in Computer Science*, **2001**, 87-103	0.9	2
390	Strong Adaptive Chosen-Ciphertext Attacks with Memory Dump (or: The Importance of the Order of Decryption and Validation). *Lecture Notes in Computer Science*, **2001**, 114-127	0.9	3
389	New Chosen-Plaintext Attacks on the One-Wayness of the Modified McEliece PKC Proposed at Asiacrypt 2000. *Lecture Notes in Computer Science*, **2002**, 237-251	0.9	
388	On Sufficient Randomness for Secure Public-Key Cryptosystems. *Lecture Notes in Computer Science*, **2002**, 34-47	0.9	3

387	New Semantically Secure Public-Key Cryptosystems from the RSA-Primitive. *Lecture Notes in Computer Science*, **2002**, 1-16	0.9	5
386	Anonymous Group Communication in Mobile Networks. *Lecture Notes in Computer Science*, **2003**, 316-328	0.9	
385	A CCA2 Secure Key Encapsulation Scheme Based on 3rd Order Shift Registers. *Lecture Notes in Computer Science*, **2003**, 428-442	0.9	
384	Cryptography and the Methodology of Provable Security. *Lecture Notes in Computer Science*, **2003**, 1-5	0.9	
383	Efficient Zero-Knowledge Proofs for Some Practical Graph Problems. *Lecture Notes in Computer Science*, **2003**, 290-302	0.9	2
382	Modeling Complexity in Secure Distributed Computing. *Lecture Notes in Computer Science*, **2003**, 57-61	0.9	1
381	Private Keyword-Based Push and Pull with Applications to Anonymous Communication. *Lecture Notes in Computer Science*, **2004**, 16-30	0.9	3
380	Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes. *Lecture Notes in Computer Science*, **2004**, 212-226	0.9	8
379	List-Decoding of Linear Functions and Analysis of a Two-Round Zero-Knowledge Argument. *Lecture Notes in Computer Science*, **2004**, 101-120	0.9	1
378	Number-Theoretic Cryptography. **2004**, 193-222		
377	Foundations of Modern Cryptography. **2005**, 89-131		
376	Security Analysis of Three Cryptographic Schemes from Other Cryptographic Schemes. *Lecture Notes in Computer Science*, **2005**, 290-301	0.9	
375	Chaumâ Designated Confirmer Signature Revisited. *Lecture Notes in Computer Science*, **2005**, 164-178	0.9	2
374	The Physically Observable Security of Signature Schemes. *Lecture Notes in Computer Science*, **2005**, 220-232	0.9	1
373	Justifying a Dolev-Yao Model Under Active Attacks. *Lecture Notes in Computer Science*, **2005**, 1-41	0.9	
372	Unconditionally Secure Chaffing-and-Winnowing: A Relationship Between Encryption and Authentication. *Lecture Notes in Computer Science*, **2006**, 154-162	0.9	4
371	Language Modeling and Encryption on Packet Switched Networks. *Lecture Notes in Computer Science*, **2006**, 359-372	0.9	1
370	On the Definition of Anonymity for Ring Signatures. *Lecture Notes in Computer Science*, **2006**, 157-174	0.9	

369	An Efficient Public Key Cryptosystem Secure Against Chosen Ciphertext Attack. *Lecture Notes in Computer Science*, **2006**, 303-314	0.9	
368	Conditionally Verifiable Signature. *Lecture Notes in Computer Science*, **2006**, 206-220	0.9	
367	Secure Quantization Index Modulation Watermark Detection. *Lecture Notes in Computer Science*, **2006**, 16-18	0.9	
366	A Separation Between Selective and Full-Identity Security Notions for Identity-Based Encryption. *Lecture Notes in Computer Science*, **2006**, 318-326	0.9	3
365	ACM SIGACT news distributed computing column 24. **2006**, 37, 58-84		
364	Hiding Information Hiding. *Lecture Notes in Computer Science*, **2007**, 161-171	0.9	
363	Computational Soundness of Formal Indistinguishability and Static Equivalence. *Lecture Notes in Computer Science*, **2007**, 182-196	0.9	4
362	Security of Invertible Media Authentication Schemes Revisited. *Lecture Notes in Computer Science*, **2007**, 189-203	0.9	
361	Client-Server Trade-Offs in Secure Computation. **2007**, 197-211		1
360	Privacy and Anonymity in Mobile Ad Hoc Networks. **2007**, 159-181		
359	Quadratic Residue Integrity Standard. **2007**, 1, 81-84		
358	Privacy-Preserving Cryptographic Protocols. **2007**, 47-69		
357	Note bibliografiche. **2008**, 533-601		
356	Characterization of Security Notions for Probabilistic Private-Key Encryption.		
355	Two Generic Constructions of Probabilistic Cryptosystems and Their Applications. *Lecture Notes in Computer Science*, **2008**, 92-108	0.9	
354	Residual Information of Redacted Images Hidden in the Compression Artifacts. *Lecture Notes in Computer Science*, **2008**, 87-101	0.9	1
353	[redacted]**2008**, 20, 147-159		3
352	Unconditionally Secure Chaffing-and-Winnowing for Multiple Use. *Lecture Notes in Computer Science*, **2009**, 133-145	0.9	

351	A Practical Approach to a Reliable Electronic Election. *Lecture Notes in Computer Science*, **2009**, 191-203	0.9	
350	Formal Indistinguishability Extended to the Random Oracle Model. *Lecture Notes in Computer Science*, **2009**, 555-570	0.9	
349	Efficient Constructions of Deterministic Encryption from Hybrid Encryption and Code-Based PKE. *Lecture Notes in Computer Science*, **2009**, 159-168	0.9	1
348	Group-Based Proxy Re-encryption Scheme. *Lecture Notes in Computer Science*, **2009**, 1025-1034	0.9	3
347	On the Impossibility of Strong Encryption Over (aleph_0). *Lecture Notes in Computer Science*, **2009**, 202-218	0.9	1
346	Simple CCA-Secure Public Key Encryption from Any Non-Malleable Identity-Based Encryption. *Lecture Notes in Computer Science*, **2009**, 1-19	0.9	
345	Computational Semantics for First-Order Logical Analysis of Cryptographic Protocols. *Lecture Notes in Computer Science*, **2009**, 33-56	0.9	2
344	On the Correctness of an Approach against Side-Channel Attacks. *Lecture Notes in Computer Science* , **2009**, 336-344	0.9	
343	Primitive Power Roots of Unity and Its Application to Encryption. **2009**, E92-A, 1836-1844		
342	Secure Data Aggregation in Wireless Sensor Networks. **2009**, 533-559		1
341	Non-malleable Schemes Resisting Adaptive Adversaries. *Lecture Notes in Computer Science*, **2009**, 240-253	0.9	
340	Discrete-Log-Based Additively Homomorphic Encryption and Secure WSN Data Aggregation. *Lecture Notes in Computer Science*, **2009**, 493-502	0.9	
339	Generic Construction of Stateful Identity Based Encryption. *Lecture Notes in Computer Science*, **2009**, 338-346	0.9	
338	Public Key in RFIDs. **2009**,		
337	Enhancing Sensor Network Security with RSL Codes. **2010**, 443-447		
336	Signcryption Schemes Based on the DiffieâHellman Problem. **2010**, 57-69		
335	Constructing Better KEMs with Partial Message Recovery. *Lecture Notes in Computer Science*, **2010**, 303-312	0.9	1
334	Schemes for Privately Computing Trust and Reputation. **2010**, 1-16		1

333	Efficient Completely Non-malleable Public Key Encryption. *Lecture Notes in Computer Science*, **2010**, 127-139	0.9	4
332	Public-Key Cryptography. **2010**, 21-34		2
331	Mechanism Design and Communication Networks.		1
330	Security of Sequential Multiple Encryption. *Lecture Notes in Computer Science*, **2010**, 20-39	0.9	6
329	Pseudorandomness In Computer Science and In Additive Combinatorics. **2010**, 619-650		2
328	Computational Soundness, Co-induction, and Encryption Cycles. *Lecture Notes in Computer Science*, **2010**, 362-380	0.9	4
327	Chosen Ciphertext Security with Optimal Ciphertext Overhead. **2010**, E93-A, 22-33		1
326	Resiliency Aspects of Security Protocols. *Lecture Notes in Computer Science*, **2010**, 37-57	0.9	
325	Delayed-Key Message Authentication for Streams. *Lecture Notes in Computer Science*, **2010**, 290-307	0.9	2
324	Encyclopedia of Cryptography and Security. **2011**, 516-516		
323	Encyclopedia of Cryptography and Security. **2011**, 849-852		
322	Encyclopedia of Cryptography and Security. **2011**, 560-562		
321	Encyclopedia of Cryptography and Security. **2011**, 1167-1168		
320	Encyclopedia of Cryptography and Security. **2011**, 161-162		
319	(mathcal{E})-MACs: Towards More Secure and More Efficient Constructions of Secure Channels. *Lecture Notes in Computer Science*, **2011**, 292-310	0.9	1
318	Acquiring Key Privacy from Data Privacy. *Lecture Notes in Computer Science*, **2011**, 359-372	0.9	
317	Public-Key Encryptions with Invariant Security Reductions in the Multi-User Setting. **2011**, E94-A, 735-760		
316	Implementing Cryptographic Primitives in the Symbolic Model. *Lecture Notes in Computer Science*, **2011**, 267-281	0.9	

315	Deniable Encryption in Replacement of Untappable Channel to Prevent Coercion. **2011**, 491-501		
314	Probabilistic Public-Key Encryption. **2011**, 980-980		
313	Encyclopedia of Cryptography and Security. **2011**, 358-359		
312	Embedding Edit Distance to Allow Private Keyword Search in Cloud Computing. **2011**, 105-113		2
311	Towards Restricting Plaintext Space in Public Key Encryption. *Lecture Notes in Computer Science*, **2011**, 193-209	0.9	1
310	An Encrypted Data-Transportation Method for Distributed System. *Lecture Notes in Computer Science*, **2011**, 390-396	0.9	
309	The Efficient CCA Secure Public-Key Encryption Scheme. **2011**, 34, 236-241		1
308	A Survey on Analysis of Selected Cryptographic Primitives and Security Protocols in Symbolic Model and Computational Model. **2011**, 10, 1068-1091		6
307	Rational Secret Sharing Scheme Based on Probability Encryption without Trusted Center. **2011**, 6,		
306	Two Cryptographic Properties of Strong Security Tweakable Enciphering Scheme. **2011**, 33, 1761-1764		
305	Security of Sequential Multiple Encryption. **2012**, E95-A, 57-69		
304	Secure Implementation of Asynchronous Method Calls and Futures. *Lecture Notes in Computer Science*, **2012**, 25-47	0.9	1
303	Guarantee of Cryptographic Protocol Security. **2012**, 215-247		
302	Informal Analysis Schemes of Cryptographic Protocols. **2012**, 83-152		
301	Cryptanalysis of a Lattice-Knapsack Mixed Public Key Cryptosystem. *Lecture Notes in Computer Science*, **2012**, 32-42	0.9	
300	A Generic Construction of Accountable Decryption and Its Applications. *Lecture Notes in Computer Science*, **2012**, 322-335	0.9	
299	Adaptive and Composable Non-interactive String-Commitment Protocols. **2012**, 233-242		
298	Design of Cryptographic Protocols Based on Trusted Freshness. **2012**, 299-340		

297	Towards Symbolic Encryption Schemes. *Lecture Notes in Computer Science*, **2012**, 557-572	0.9	1
296	Cifrari simmetrici. **2012**, 101-143		
295	Relaxing IND-CCA: Indistinguishability against Chosen Ciphertext Verification Attack. *Lecture Notes in Computer Science*, **2012**, 63-76	0.9	2
294	Computer-Aided Cryptographic Proofs. *Lecture Notes in Computer Science*, **2012**, 1-2	0.9	
293	Designing the API for a Cryptographic Library. *Lecture Notes in Computer Science*, **2012**, 75-88	0.9	0
292	Modeling Adversaries in a Logic for Security Protocol Analysis. **2012**, 8,		0
291	Privacy Background. **2013**, 19-45		
290	Code-Based Public-Key Encryption Resistant to Key Leakage. *Lecture Notes in Computer Science*, **2013**, 44-54	0.9	1
289	Symbolic Probabilistic Analysis of Off-Line Guessing. *Lecture Notes in Computer Science*, **2013**, 363-380	0.9	1
288	Privacy-Aware Processing of Biometric Templates by Means of Secure Two-Party Computation. **2013**, 149-185		
287	New Attacks against Transformation-Based Privacy-Preserving Linear Programming. *Lecture Notes in Computer Science*, **2013**, 17-32	0.9	0
286	Primeless Factoring-Based Cryptography. *Lecture Notes in Computer Science*, **2013**, 552-569	0.9	
285	Secure End-to-End Communication with Optimal Throughput and Resilience against Malicious Adversary. *Lecture Notes in Computer Science*, **2013**, 403-417	0.9	
284	Quantum Attacks on IFP-Based Cryptosystems. **2013**, 31-91		1
283	Generic Construction of Strongly Secure Timed-Release Public-Key Encryption. **2013**, E96.A, 76-91		
282	Coinductive techniques for higher-order languages. 131, 1-4		
281	On coinductive equivalences for higher-order probabilistic functional programs. **2014**, 49, 297-308		2
280	Enabling Short Fragments for Uncoordinated Spread Spectrum Communication. *Lecture Notes in Computer Science*, **2014**, 488-507	0.9	

279	Higher-Order Languages: Bisimulation and Coinductive Equivalences (Extended Abstract). *Lecture Notes in Computer Science*, **2014**, 3-9	0.9	
278	Cryptography in NC0. **2014**, 33-78		2
277	Weakened Anonymity of Group Signature and Its Application to Subscription Services. **2014**, E97.A, 1240-1258		2
276	Probabilistic Recursion Theory and Implicit Computational Complexity. *Lecture Notes in Computer Science*, **2014**, 97-114	0.9	
275	Complete Robustness in Identity-Based Encryption. *Lecture Notes in Computer Science*, **2014**, 342-349	0.9	
274	Chasing Diagrams in Cryptography. *Lecture Notes in Computer Science*, **2014**, 353-367	0.9	5
273	Privacy Preserving T□onnement. *Lecture Notes in Computer Science*, **2014**, 399-416	0.9	2
272	Sicherheit kryptographischer Systeme. **2014**, 63-105		
271	Chosen Ciphertext Security on Hard Membership Decision Groups: The Case of Semi-smooth Subgroups of Quadratic Residues. *Lecture Notes in Computer Science*, **2014**, 558-577	0.9	1
270	Knowledge and Efficient Computation. **1986**, 353-362		
269	Unbedingte Unbeobachtbarkeit mit kryptographischer Robustheit. **1987**, 302-320		
268	Cryptography and Reliable Interaction. **1987**, 359-379		
267	C. **1988**, 1-508		
266	A Basic Theory of Public and Private Cryptosystems. *Lecture Notes in Computer Science*, **1990**, 249-255	0.9	1
265	Removing Interaction from Zero-Knowledge Proofs. **1990**, 377-393		1
264	Public-Randomness in Public-Key Cryptography. *Lecture Notes in Computer Science*, **1991**, 46-62	0.9	6
263	One-message statistical Zero-Knowledge Proofs and space-bounded verifier. *Lecture Notes in Computer Science*, **1992**, 28-40	0.9	7
262	How to construct a family of strong one way permutations. *Lecture Notes in Computer Science*, **1993**, 97-110	0.9	

261	Transparent Proofs and Limits to Approximation. **1994**, 31-91		
260	C. **1995**, 1-78		
259	Randomness, Interactive Proofs, and Zero-Knowledge â A Survey. **1995**, 349-375		
258	A formal framework for evaluating heuristic programs. *Lecture Notes in Computer Science*, **1996**, 634-645	0.9	
257	Efficient and provably secure key agreement. **1996**, 227-236		
256	Wie man Beweise führen kann: interaktiv und ohne den Beweis zu Verraten. **1996**, 287-304		
255	Computer Security and Cryptography. **1997**,		
254	Checking Programs Discreetly: Demonstrating Result-Correctness Efficiently While Concealing It. *Lecture Notes in Computer Science*, **1998**, 60-71	0.9	
253	Over the Air Service Provisioning. *Lecture Notes in Computer Science*, **1999**, 174-189	0.9	
252	On the Security of an RSA Based Encryption Scheme. *Lecture Notes in Computer Science*, **1999**, 135-148	0.9	
251	Cryptography. **2014**, 1-18		
250	How to Leak a Secret and Reap the Rewards Too. *Lecture Notes in Computer Science*, **2015**, 348-367	0.9	1
249	Encrypted Secret Sharing and Analysis by Plaintext Randomization. *Lecture Notes in Computer Science*, **2015**, 49-65	0.9	
248	mOT+: An Efficient and Secure Identity-Based Diffie-Hellman Protocol over RSA Group. *Lecture Notes in Computer Science*, **2015**, 407-421	0.9	
247	Collaborative Multiparty Association Rules Mining with Threshold Homomorphic Encryption. *Lecture Notes in Computer Science*, **2015**, 251-263	0.9	
246	Non-malleability Under Selective Opening Attacks: Implication and Separation. *Lecture Notes in Computer Science*, **2015**, 87-104	0.9	0
245	Simpler CCA-Secure Public Key Encryption from Lossy Trapdoor Functions. *Lecture Notes in Computer Science*, **2015**, 193-206	0.9	
244	Constructing and Understanding Chosen Ciphertext Security via Puncturable Key Encapsulation Mechanisms. *Lecture Notes in Computer Science*, **2015**, 561-590	0.9	8

243	Gambling, Computational Information and Encryption Security. *Lecture Notes in Computer Science*, **2015**, 141-158	0.9	
242	Non-Interactive Zero-Knowledge Proofs of Non-Membership. *Lecture Notes in Computer Science*, **2015**, 145-164	0.9	6
241	Introduction. **2015**, 1-31		
240	Quantum Algorithms for Integer Factorization. **2015**, 59-119		
239	A Public Key Cryptoscheme Using Bit-Pairs with Provable Semantical Security. *Lecture Notes in Computer Science*, **2015**, 674-686	0.9	
238	Almost Perfect Privacy for Additive Gaussian Privacy Filters. *Lecture Notes in Computer Science*, **2016**, 259-278	0.9	1
237	A Posteriori Openable Public Key Encryption. **2016**, 17-31		2
236	Secure Key Establishment in Wireless Sensor Networks. **2016**, 342-367		
235	Security Analysis of the Modular Enhanced Symmetric Role Authentication (mERA) Protocol. *Lecture Notes in Computer Science*, **2016**, 518-542	0.9	
234	Simultaneous Secrecy and Reliability Amplification for a General Channel Model. *Lecture Notes in Computer Science*, **2016**, 235-261	0.9	
233	Privacy Protection of Digital Speech Based on Homomorphic Encryption. *Lecture Notes in Computer Science*, **2016**, 365-376	0.9	
232	Approximate-Deterministic Public Key Encryption from Hard Learning Problems. *Lecture Notes in Computer Science*, **2016**, 25-42	0.9	1
231	A Novel Smart-Card Based Authentication Scheme Using Proactive Secret Sharing. **2016**, 5, 196-205		
230	A Formal Treatment of Privacy in Video Data. *Lecture Notes in Computer Science*, **2016**, 406-424	0.9	1
229	Provable Security for Public Key Cryptosystems. **2016**, 317-341		
228	? Computation Over Encrypted Data. **2016**, 331-346		
227	Secure Wavelet Matrix: Alphabet-Friendly Privacy-Preserving String Search.		
226	Towards Adaptive Cryptography and Security with Software Defined Platforms. **2017**, 209-236		

225	KDM-Secure Public-Key Encryption from Constant-Noise LPN. *Lecture Notes in Computer Science*, **2017**, 44-64	0.9	
224	Privacy Preserving Discovery of Nearby-Friends. **2017**, 41-55		2
223	Studying Formal Security Proofs for Cryptographic Protocols. **2017**, 63-73		0
222	Encyclopedia of Database Systems. **2017**, 1-6		
221	Exploiting Autocorrect to Attack Privacy. *Lecture Notes in Computer Science*, **2017**, 103-109	0.9	
220	Ambiguous Multi-Symmetric Scheme and Applications. **2017**, 08, 383-401		
219	Hash-then-Encode: A Modular Semantically Secure Wiretap Code. **2018**, 49-63		2
218	Malleable Cryptosystems and Their Applications in Wireless Sensor Networks. **2018**, 97-111		
217	Encyclopedia of Database Systems. **2018**, 2825-2830		
216	Cryptographic Uncertainness: Some Experiments on Finite Semifield Based Substitution Boxes. **2018**, 485-492		
215	No-signaling Linear PCPs. *Lecture Notes in Computer Science*, **2018**, 67-97	0.9	1
214	Leakage-Resilient Cryptography from Puncturable Primitives and Obfuscation. *Lecture Notes in Computer Science*, **2018**, 575-606	0.9	3
213	Simulation-Based Receiver Selective Opening CCA Secure PKE from Standard Computational Assumptions. *Lecture Notes in Computer Science*, **2018**, 140-159	0.9	7
212	Securing Public Key Encryption Against Adaptive Chosen Ciphertext Attacks. **2018**, 134-144		
211	The Roll of Dices in Cryptology. **2018**, 493-504		
210	Secure Key Establishment in Wireless Sensor Networks. **2018**, 883-908		
209	SLIDE: An Efficient Secure Linguistic Steganography Detection Protocol. *Lecture Notes in Computer Science*, **2018**, 298-309	0.9	1
208	A Variant of BLS Signature Scheme with Tight Security Reduction. **2018**, 150-163		2

207	Design of fully homomorphic encryption by prime modular operation. **2018**, 10, 118-122		0
206	Security of Identity-Based Encryption Algorithms. **2018**, 4975-4984		
205	New Attacks and Secure Design for Anonymous Distance-Bounding. *Lecture Notes in Computer Science*, **2018**, 598-616	0.9	1
204	A Novel Private Information Retrieval Technique for Private DNS Resolution. **2019**, 163-171		
203	Compressed Sensing as a Cryptosystem. **2019**, 25-71		1
202	Lightweight Fault Tolerance for Secure Aggregation of Homomorphic Data. **2019**, 87-110		
201	PINFER: Privacy-Preserving Inference. *Lecture Notes in Computer Science*, **2019**, 3-21	0.9	0
200	Security of Identity-Based Encryption Algorithms. **2019**, 312-325		
199	Improving Signature Schemes with Tight Security Reductions. *Lecture Notes in Computer Science*, **2019**, 273-292	0.9	1
198	Cryptographic Formula Obfuscation. *Lecture Notes in Computer Science*, **2019**, 208-224	0.9	1
197	Universally Composable Secure Computation with Corrupted Tokens. *Lecture Notes in Computer Science*, **2019**, 432-461	0.9	1
196	Cocksâ□Identity-Based Encryption in the Standard Model, via Obfuscation Techniques (Short Paper). *Lecture Notes in Computer Science*, **2019**, 273-283	0.9	
195	Equivalence Between Non-malleability Against Replayable CCA and Other RCCA-Security Notions. *Lecture Notes in Computer Science*, **2019**, 253-272	0.9	1
194	The PRF Security of Compression-Function-Based MAC Functions in the Multi-User Setting. **2019**, E102.A, 270-277		
193	Secure Computation of Private Set Intersection Cardinality With Linear Complexity. **2019**, 142-180		1
192	Cryptographic Sensing. *Lecture Notes in Computer Science*, **2019**, 583-604	0.9	1
191	Lossy Trapdoor Permutations with Improved Lossiness. *Lecture Notes in Computer Science*, **2019**, 230-250	0.9	2
190	Symbolic Encryption with Pseudorandom Keys. *Lecture Notes in Computer Science*, **2019**, 64-93	0.9	

189	How much data may be safely processed on one key in different modes?. **2019**, 10, 125-134		
188	The Local Forking Lemma and Its Application to Deterministic Encryption. *Lecture Notes in Computer Science*, **2019**, 607-636	0.9	3
187	An Obsession with Definitions. *Lecture Notes in Computer Science*, **2019**, 3-20	0.9	
186	An improved Fully Homomorphic Encryption model based on N-Primes. **2019**, 4,		0
185	An Efficient Privacy-Preserving Protocol for Computing kth Minimum Value in P2P Networks. **2020**, 29, 2050138		1
184	Anonymous IBE from Quadratic Residuosity with Fast Encryption. *Lecture Notes in Computer Science* , **2020**, 3-19	0.9	
183	Logic Locking of Boolean Circuits: Provable Hardware-Based Obfuscation from a Tamper-Proof Memory. *Lecture Notes in Computer Science*, **2020**, 172-192	0.9	3
182	MaTRU-KE revisited: CCA2-secure key establishment protocol based on MaTRU. **2020**, 33, e4326		
181	IoT Expunge. **2020**,		0
180	Indistinguishability and Non-deterministic Encryption of the Quantum Safe Multivariate Polynomial Public Key Cryptographic System. **2021**,		0
179	Secure Scalar Product Protocols. **2021**, 30, 1059-1068		
178	Method for hiding information in lattice. **1998**, 34, 2226		1
177	Public-key Encryption. **2020**, 23-49		
176	A Review of Machine Learning and Cryptography Applications. **2020**,		0
175	A non-Symmetric Key Dependent for Reverse Encryption Algorithm (REA). **2020**,		
174	Efficient message transmission via twisted Edwards curves. **2020**, 70, 1511-1520		
173	Computing Blindfolded on Data Homomorphically Encrypted under Multiple Keys: A Survey. **2022**, 54, 1-37		0
172	Random Algebraic Lattices and Codes for Wireless Communications. **2020**, 143-177		

171	Verifiable Registration-Based Encryption. *Lecture Notes in Computer Science*, **2020**, 621-651	0.9	6
170	A Data Trading Scheme with Efficient Data Usage Control for Industrial IoT. **2021**, 1-1		1
169	Authenticated Encryption Based on Lesamnta-LW Hashing Mode. *Lecture Notes in Computer Science* , **2020**, 52-69	0.9	1
168	Semantic Definition of Anonymity in Identity-Based Encryption and Its Relation to Indistinguishability-Based Definition. *Lecture Notes in Computer Science*, **2020**, 65-85	0.9	0
167	A Chaos-Based Multi-level Dynamic Framework for Image Encryption. **2020**, 189-217		1
166	Modular-Arithmetic Cryptosystems. **2020**, 89-104		
165	A Calculus of Chaos in Stochastic Compilation. *Lecture Notes in Computer Science*, **2020**, 167-184	0.9	
164	Two-Server Verifiable Homomorphic Secret Sharing for High-Degree Polynomials. *Lecture Notes in Computer Science*, **2020**, 75-91	0.9	
163	Impossibility of Strong KDM Security with Auxiliary Input. *Lecture Notes in Computer Science*, **2020**, 512-524	0.9	
162	Towards Blockchain-Enabled Searchable Encryption. *Lecture Notes in Computer Science*, **2020**, 482-500	0.9	4
161	Receiver Selective Opening CCA Secure Public Key Encryption from Various Assumptions. *Lecture Notes in Computer Science*, **2020**, 213-233	0.9	1
160	Succinct Non-interactive Secure Computation. *Lecture Notes in Computer Science*, **2020**, 216-245	0.9	5
159	Secure Key Encapsulation Mechanism with Compact Ciphertext and Public Key from Generalized Srivastava Code. *Lecture Notes in Computer Science*, **2020**, 175-193	0.9	
158	Secure Primitive for Big Data Utilization. **2020**, 35-63		
157	Privacy preserving anomaly detection based on local density estimation. **2020**, 17, 3478-3497		
156	Secure Deterministic Automata Evaluation: Completeness and Efficient 2-party Protocols. *Lecture Notes in Computer Science*, **2020**, 50-64	0.9	
155	THE DIVIDE AND CONQUER METHOD IN THE DENIABLE ENCRYPTION ALGORITHMS. **2020**, 2, 29-44		
154	Introduction. **2020**, 1-6		

153	Provable Security for Public Key Cryptosystems. **2020**, 214-238		
152	Crypto Primer. **2021**, 241-268		
151	Recent Advances in Information-Theoretically Secure Data Outsourcing. **2020**,		
150	Cryptocurrencies with Security Policies and Two-Factor Authentication. **2021**,		
149	Hardware Attacks. 33-44		
148	A Remedy of Zhu-Lee-Dengâ Public Key Cryptosystem. **2004**, 187-194		
147	Quantum Computational Cryptography. **2006**, 167-184		
146	Kryptografie und zuverlässige Interaktion. **2006**, 383-406		
145	Interactive Proofs with Provable Security against Honest Verifiers. **1990**, 378-392		
144	Establishing secure links in low-rate wireless personal area networks. **2008**, 109-123		
143	On Performance Cost of On-demand Anonymous Routing Protocols in Mobile Ad Hoc Networks. **2007**, 119-142		2
142	One-More Extension of Paillier Inversion Problem and Concurrent Secure Identification. *Lecture Notes in Computer Science*, **2007**, 65-77	0.9	
141	A Cryptographic Method for Secure Watermark Detection. *Lecture Notes in Computer Science*, **2006**, 26-41	0.9	3
140	Security Protocols: Principles and Calculi. *Lecture Notes in Computer Science*, **2007**, 1-23	0.9	6
139	A New Scheme for Deniable/Repudiable Authentication. *Lecture Notes in Computer Science*, **2007**, 424-432	0.9	1
138	A Note on the (Im)possibility of Using Obfuscators to Transform Private-Key Encryption into Public-Key Encryption. **2007**, 1-12		3
137	An Approach for Symmetric Encryption Against Side Channel Attacks in Provable Security. **2007**, 178-187		1
136	Homomorphic Encryptions of Sums of Groups. **2007**, 357-366		1

135	Design of Secure Watermarking Scheme for Watermarking Protocol. **2007**, 357-366		1
134	Computational Soundness of Equational Theories (Tutorial). **2007**, 363-382		1
133	Orthogonality between Key Privacy and Data Privacy, Revisited. *Lecture Notes in Computer Science*, **2008**, 313-327	0.9	3
132	Some Information Theoretic Arguments for Encryption: Non-malleability and Chosen-Ciphertext Security (Invited Talk). *Lecture Notes in Computer Science*, **2008**, 223-231	0.9	5
131	Computation Over Encrypted Data. **2020**, 329-346		
130	Review of Techniques for Privacy-Preserving Blockchain Systems. **2020**,		3
129	Modeling advanced security aspects of key exchange and secure channel protocols. **2020**, 62, 287-293		
128	The Eleventh Power Residue Symbol. **2020**, 15, 111-122		1
127	Application of non-associative structures for construction of homomorphic cryptosystems. **2020**, 11, 31-39		
126	Greedy adversarial equilibrium: an efficient alternative to nonconvex-nonconcave min-max optimization. **2021**,		
125	Introduction. **2021**, 47-53		
124	C3PO: C loud-based C onfidentiality-preserving C ontinuous Query P r o cessing. **2022**, 25, 1-36		
123	Bibliographie. **2021**, 195-198		
122	Practical Provably Secure Encryption Scheme Based on Hashed Bilinear Pairing. **2022**, 705-711		
121	Beyond Software Watermarking: Traitor-Tracing for Pseudorandom Functions. *Lecture Notes in Computer Science*, **2021**, 250-280	0.9	1
120	Popular Homomorphic Encryption Schemes. **2021**, 77-84		
119	Faster Private Rating Update via Integer-Based Homomorphic Encryption. *Lecture Notes in Computer Science*, **2021**, 218-236	0.9	0
118	Report and Trace Ring Signatures. *Lecture Notes in Computer Science*, **2021**, 179-199	0.9	2

117	Adaptive Security via Deletion in Attribute-Based Encryption: Solutions from Search Assumptions in Bilinear Groups. *Lecture Notes in Computer Science*, **2021**, 311-341	0.9	1
116	Is it Easier to Prove Theorems that are Guaranteed to be True?. **2020**,		2
115	On One-way Functions and Kolmogorov Complexity. **2020**,		3
114	Small Quantum-safe Design Approach for Long-term Safety in Cloud Environments. **2021**,		
113	Weak Zero-Knowledge beyond the Black-Box Barrier. STOC19-156-STOC19-199		
112	Efficient Recovery of a Shared Secret via Cooperation: Applications to SDMM and PIR. **2022**, 1-1		1
111	Lightweight Secure Integer Comparison. *Mathematics*, **2022**, 10, 305	2.3	1
110	Cryptographic Techniques for Data Processing. **2022**,		1
109	CCA Secure A Posteriori Openable Encryption in the Standard Model. *Lecture Notes in Computer Science*, **2022**, 370-394	0.9	
108	A Comprehensive Survey of Fully Homomorphic Encryption from Its Theory to Applications. **2022**, 73-90		
107	Differential Privacy. **2022**, 5-11		
106	Overview of Block Chain Privacy Protection Methods. **2022**,		
105	Lifting Standard Model Reductions to Common Setup Assumptions. *Lecture Notes in Computer Science*, **2022**, 130-160	0.9	
104	Cryptography and Digital Transformation. **2022**, 159-171		
103	The Boneh-Katz Transformation, Revisited: Pseudorandom/Obliviously-Samplable PKE from Lattices and Codes and Its Application. *Lecture Notes in Computer Science*, **2022**, 47-67	0.9	
102	ABE-AC4DDS: An Access Control Scheme Based on Attribute-Based Encryption for Data Distribution Service. *Lecture Notes in Computer Science*, **2022**, 67-80	0.9	
101	Categorical composable cryptography. *Lecture Notes in Computer Science*, **2022**, 161-183	0.9	0
100	A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels. *Lecture Notes in Computer Science*, **2022**, 316-344	0.9	

99	Scope and Related Work. **2022**, 79-87		
98	Efficient Generation of Roots of Power Residues Modulo Powers of Two. *Mathematics*, **2022**, 10, 908	2.3	
97	A Survey on Applications of H-Technique: Revisiting Security Analysis of PRP and PRF.. **2022**, 24,		1
96	A Survey of Practical Formal Methods for Security.		3
95	A multipermutation superposition coding-based fragile watermarking for probabilistic encryption. 1		1
94	A K-nearest neighbor classifier based on homomorphic encryption scheme. **2021**,		
93	Efficient Lattice-Based Cryptosystems with Key Dependent Message Security. *Applied Sciences (Switzerland)*, **2021**, 11, 12161	2.6	1
92	Optimized Paillierâ Cryptosystem with Fast Encryption and Decryption. **2021**,		
91	Module Research of Blockchain-based Power Equipment Inspection and Data Asset Sharing. **2021**,		
90	Perfect Secrecy in the Bounded Storage Model. **2021**,		
89	Halkla Ili kiler Ajanslar n n Bulut Taban l Güvenli k Taraf Hesaplama ve Birli Servisi - SMPCCaaS. *European Journal of Science and Technology*,	0.4	
88	Privacy-preserving Hamming distance Protocol and Its Applications. **2021**,		
87	An Efficient and Privacy-Preserving Route Matching Scheme for Carpooling Services. *IEEE Internet of Things Journal*, **2022**, 1-1	10.7	0
86	Quest: Privacy-Preserving Monitoring of Network Data: A System for Organizational Response to Pandemics. *IEEE Transactions on Services Computing*, **2022**, 1-1	4.8	
85	Quantum Computational Cryptography. **2006**, 167-184		
84	Analog Secret Sharing with Applications to Private Distributed Learning. *IEEE Transactions on Information Forensics and Security*, **2022**, 1-1	8	0
83	Generalized Goldwasser and Micaliâ Type Cryptosystem. *Journal of Computer Science and Technology*, **2022**, 37, 459-467	1.7	
82	Privacy-Preserving KNN Classification Algorithm for Smart Grid. *Security and Communication Networks*, **2022**, 2022, 1-11	1.9	1

81	A tunable quantum random number generator based on a fiber-optical Sagnac interferometer. *Journal of Optics (United Kingdom)*, **2022**, 24, 064010	1.7	0
80	The Case of Small Prime Numbers Versus the Joyeâ□ibert Cryptosystem. *Mathematics*, **2022**, 10, 1577	2.3	
79	Succinct Non-Interactive Arguments via Linear Interactive Proofs. *Journal of Cryptology*, **2022**, 35, 1	2.1	1
78	Creation of two distant entangled qutrits via interference of polarized photons: With and without rotating wave approximation. *Optik*, **2022**, 169253	2.5	0
77	A Note on Perfect Correctness by Derandomization. *Journal of Cryptology*, **2022**, 35,	2.1	
76	HLSBD2: a quantum secure hybrid level source based data deduplication for the cloud. *Journal of Ambient Intelligence and Humanized Computing*,	3.7	
75	Chosen-Ciphertext Attack Secure Public-Key Encryption with Keyword Search. *Computers, Materials and Continua*, **2022**, 73, 69-85	3.9	0
74	Slicing of probabilistic programs based on specifications. *Science of Computer Programming*, **2022**, 220, 102822	1.1	
73	Anamorphic Encryption: Private Communication Against a Dictator. *Lecture Notes in Computer Science*, **2022**, 34-63	0.9	
72	Secure Multiparty Computation with Sublinear Preprocessing. *Lecture Notes in Computer Science*, **2022**, 427-457	0.9	1
71	Single-Server Private Information Retrieval with Sublinear Amortized Time. *Lecture Notes in Computer Science*, **2022**, 3-33	0.9	4
70	A Performance Evaluation of Pairing-Based Broadcast Encryption Systems. *Lecture Notes in Computer Science*, **2022**, 24-44	0.9	0
69	An Overview of RSA and OAEP Padding. 1, 82-86		
68	Rethinking block storage encryption with virtual disks. **2022**,		
67	Performance Analysis of Probabilistic Encryption on FPGA for Wireless Sensor Nodes. *Journal of the Institution of Engineers (India): Series B*,	0.9	
66	Little extension of Eulerâ criterion for quadratic residue. *Sao Paulo Journal of Mathematical Sciences*,	0.4	
65	Modular Framework for Constructing IoT-Server AKE in Post-Quantum Setting. *IEEE Access*, **2022**, 10, 71598-71611	3.5	
64	Privacy-Preserving Feature Selection with Fully Homomorphic Encryption. *Algorithms*, **2022**, 15, 229	1.8	

63	A novel distortion-tolerant speech encryption scheme for secure voice communication. *Speech Communication*, **2022**,	2.8	0
62	Privacy-Preserving Deep Learning With Homomorphic Encryption: An Introduction. *IEEE Computational Intelligence Magazine*, **2022**, 17, 14-25	5.6	2
61	Mind the Gap: Studying the Insecurity of Provably Secure Embedded Trusted Execution Architectures. **2022**,		0
60	BB-CSP: An Efficient Blockchain-Based Collective Salary Payment Framework Using Weighted Functional Encryption. **2022**, 3,		0
59	Privacy-preserving â€Check-in Awardâ€Service in Location-based Social Networks. **2022**, 15, 2364-2375		
58	A Gift that Keeps on Giving: The Impact of Public-Key Cryptography on Theoretical Computer Science. **2022**, 157-184		
57	An authenticated and secure accounting system for international emissions trading. 1-10		
56	Toward Round-Efficient Verifiable Re-Encryption Mix-Net. **2022**, 10, 91397-91413		0
55	On Extension of ´Evaluation Algorithms in ´Keyed-Homomorphic Encryption. **2022**, 189-207		0
54	Collision-Resistant and ´Pseudorandom Function Based on ´Merkle-Damgrd Hash Function. **2022**, 325-338		1
53	High Speed Encrypted Computing: Stochastic Confusion and Lies in a Secret Computer. **2022**,		0
52	Privacy-preserving time series prediction with temporal convolutional neural networks. **2022**,		0
51	??SM2?????RCCA????. **2022**,		0
50	Novel Authentication Protocols Based on Quadratic Diophantine Equations. **2022**, 10, 3136		0
49	You Are Revoked and Out: Towards Directly Revocable Ciphertext-Policy Attribute-Based Encryption. **2022**, 2022, 1-17		0
48	No free lunch theorem for security and utility in federated learning.		0
47	Anonymous Identity Based Broadcast Encryption against Continual Side Channel Attacks in the State Partition Model. **2022**, 12, 9395		1
46	A probabilistic public key encryption switching scheme for secure cloud storage.		0

45	Beyond the ´Csiszár-Korner Bound: Best-Possible ´Wiretap ´Coding ´via ´Obfuscation. **2022**, 573-602	0
44	Securing Approximate Homomorphic Encryption Using Differential Privacy. **2022**, 560-589	0
43	Differential Privacy Mechanisms: A State-of-the-Art Survey. **2022**, 1049-1060	0
42	Privacy-Preserving Computing via Homomorphic Encryption. **2022**, 288-313	0
41	Taming the Round Efficiency of Cryptographic Protocols for Private Web Search Schemes. **2022**,	0
40	PSI from Ring-OLE. **2022**,	1
39	Poster EveGAN. **2022**,	0
38	Ibex. **2022**,	0
37	Foundations of Coin Mixing Services. **2022**,	0
36	Differential privacy performance evaluation under the condition of non-uniform noise distribution. **2022**, 71, 103366	0
35	Accountable Attribute-Based Data Sharing Scheme Based on Blockchain for Vehicular Ad Hoc Network. **2022**, 1-1	0
34	Understanding Failures in Security Proofs of Multi-Factor Authentication for Mobile Devices. **2023**, 18, 597-612	2
33	A Key Recovery Protocol for Multiparty Threshold ECDSA Schemes. **2022**, 1-1	0
32	Semantic Security with Infinite Dimensional Quantum Eavesdropping Channel. **2022**,	0
31	Differential privacy: Review of improving utility through cryptography-based technologies.	0
30	Multi-party Secure Comparison of ´Strings Based on ´Outsourced Computation. **2023**, 15-30	0
29	A tradeoff paradigm shift in cryptographically-secure pseudorandom number generation based on discrete logarithm. **2023**, 73, 103430	0
28	File Security using Image-based Encryption (FSUIE). **2022**,	0

27	Threshold Linearly Homomorphic Encryption on ´$$textbf{Z}/2^ktextbf{Z}$$. **2022**, 99-129	1
26	Instantiability of ´Classical Random-Oracle-Model Encryption Transforms. **2022**, 323-352	0
25	Frontmatter. **2022**, 1-4	0
24	6. Schluss. **2022**, 227-230	0
23	Implementing Data Exfiltration Defense in Situ: A Survey of Countermeasures and Human Involvement.	0
22	2. Kryptographische Sicherheitsbestimmungen. **2022**, 23-88	0
21	Literatur und weitere Quellen. **2022**, 231-252	0
20	Design and Analysis of Two Efficient Socialist Millionairesâ Protocols for Privacy Protection. **2023**, 142-151	0
19	Structured encryption for triangle counting on graph data. **2023**, 145, 200-210	0
18	A Gradual Probabilistic Lambda Calculus. **2023**, 7, 256-285	0
17	Scalable Cryptography. **2022**, 169-178	0
16	5. F einen queeren Sicherheitsbegriff. **2022**, 187-226	0
15	1. Einleitung. **2022**, 7-22	0
14	Die unsicheren Kan e. **2022**,	0
13	Danksagungen. **2022**, 253-258	0
12	3. IT-Sicherheit: Digitale Grenzaushandlungen. **2022**, 89-144	0
11	Inhalt. **2022**, 5-6	0
10	4. Backdoors. **2022**, 145-186	0

9	An enhanced traceable CP-ABE scheme against various types of privilege leakage in cloud storage. **2023**, 136, 102833	0
8	A Survey on Homomorphic Encryption for Biometrics Template Security Based on Machine Learning Models. **2023**,	0
7	Efficient Two-Party Privacy-Preserving Protocols for Activation Functions. **2022**,	0
6	No-Signaling Linear PCPs. **2023**, 36,	0
5	End-to-End Database Software Security. **2023**, 2, 163-176	0
4	On-Line/Off-Line DCR-Based Homomorphic Encryption and´Applications. **2023**, 115-131	0
3	Toward Basing Cryptography on the Hardness of EXP. **2023**, 66, 91-99	0
2	A Duality between One-Way Functions and Average-Case Symmetry of Information. **2023**,	0
1	NP-Hardness of Approximating Meta-Complexity: A Cryptographic Approach. **2023**,	0