Universal classes of hash functions

DOI: 10.1016/0022-0000(79)90044-8

Journal of Computer and System Sciences, 1979, 18, 143-154.

#	Paper	IF	Citations
1591	An adaptive constant time hashing scheme for dynamic key set.		
1590	PRAM programming: theory vs. practice.		2
1589	Probabilistic computations: Toward a unified measure of complexity. **1977**,		359
1588	A note on universal classes of hash functions. **1980**, 10, 41-45		17
1587	. **1980**, 24, 95-100		
1586	Tuning the coalesced hashing method to obtain optimum performance. **1980**,		2
1585	New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, **1981**, 22, 265-279	1	798
1584	On Logic Comparison. **1981**,		5
1583	Implementations for coalesced hashing. **1982**, 25, 911-926		13
1582	The theory of signature testing for VLSI. **1982**,		18
1581	On the program size of perfect and universal hash functions. **1982**,		34
1580	The program complexity of searching a table. **1983**,		2
1579	Analysis of the Search Performance of Coalesced Hashing. **1983**, 30, 231-258		19
1578	Bounded index exponential hashing. **1983**, 8, 136-165		28
1577	Compact Hash Tables Using Bidirectional Linear Probing. **1984**, C-33, 828-834		28
1576	How To Construct Randolli Functions.		25
1575	Hash table reorganization. **1985**, 6, 322-335		5

1574	Efficient Netlist Comparison Using Hierarchy and Randomization. **1985**,		5
1573	A Simple Parallel Algorithm for the Maximal Independent Set Problem. *SIAM Journal on Computing*, **1986**, 15, 1036-1053	1.1	647
1572	NP is as easy as detecting unique solutions. **1986**, 47, 85-93		327
1571	How to Reduce your Enemy�s Information (extended abstract). **1985**, 468-476		19
1570	Graph isomorphism is in the low hierarchy. **1987**, 114-124		17
1569	Optimal signature extraction and information loss. **1987**, 12, 395-428		20
1568	Approximating the number of unique values of an attribute without sorting. **1987**, 12, 11-15		23
1567	A probabilistic distributed algorithm for set intersection and its analysis. **1987**, 49, 267-282		6
1566	Graph isomorphism is in the low hierarchy. *Journal of Computer and System Sciences*, **1988**, 37, 312-323	1	108
1565	Arthur-Merlin games: A randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, **1988**, 36, 254-276	1	310
1564	The generation of random permutations on the fly. **1988**, 28, 207-212		5
1563	Dynamic hash tables. **1988**, 31, 446-457		57
1562	. **1988**,		42
1561	Privacy Amplification by Public Discussion. *SIAM Journal on Computing*, **1988**, 17, 210-229	1.1	557
1560	. **1988**,		27
1559	Hashing practice: analysis of hashing and universal hashing. **1988**, 17, 191-199		3
1558	Parallel hashing. **1988**, 35, 876-892		35
1557	Randomized algorithms and pseudorandom numbers. **1988**,		16

1556	.		
1555	. **1989**,		142
1554	Universal one-way hash functions and their cryptographic applications. **1989**,		414
1553	File organization using composite perfect hashing. **1989**, 14, 231-263		17
1552	Proving properties of interactive proofs by a generalized counting technique. **1989**, 82, 185-197		3
1551	On the power of two-point based sampling. **1989**, 5, 96-106		116
1550	On hiding information from an oracle. *Journal of Computer and System Sciences*, **1989**, 39, 21-50	1	114
1549	. **1989**,		168
1548	. **1989**,		41
1547	Practical performance of Bloom filters and parallel free-text searching. **1989**, 32, 1237-1239		65
1546	The parallel simplicity of compaction and chaining. **1990**, 744-751		19
1545	Evaluating computer-generated domain-oriented vocabularies. **1990**, 26, 791-801		14
1544	Kolmogorov Complexity and its Applications. **1990**, 187-254		31
1543	General Purpose Parallel Architectures. **1990**, 943-971		84
1542	.		37
1541	.		16
1540	.		45
1539	.		2

1538	Randomness in interactive proofs.		9
1537	Faster algorithms for the shortest path problem. **1990**, 37, 213-223		292
1536	A bridging model for parallel computation. **1990**, 33, 103-111		2044
1535	Applications of Kolmogorov Complexity in the Theory of Computation. **1990**, 147-203		14
1534	Efficient computation on oblivious RAMs. **1990**,		115
1533	A Time-Randomness Trade-Off for Oblivious Routing. *SIAM Journal on Computing*, **1990**, 19, 256-266	1.1	11
1532	No better ways to generate hard NP instances than picking uniformly at random. **1990**,		46
1531	.		9
1530	.		3
1529	.		21
1528	On the complexity of counting in the polynomial hierarchy. **1991**, 81, 77-95		
1527	On parallel hashing and integer sorting. **1991**, 12, 573-606		27
1526	The greedy coloring is a bad probabilistic algorithm. **1991**, 12, 674-684		29
1525	How to emulate shared memory. *Journal of Computer and System Sciences*, **1991**, 42, 307-326	1	114
1524	Statistical zero-knowledge languages can be recognized in two rounds. *Journal of Computer and System Sciences*, **1991**, 42, 327-345	1	77
1523	A caution on universal classes of hash functions. **1991**, 37, 247-256		3
1522	Broadcast with partial knowledge (preliminary version). **1991**,		2
1521	A dynamic hash method with signature. **1991**, 16, 309-337		5

1520	.		5
1519	Advances in Cryptology EUROCRYPT 90. **1991**,		4
1518	Nonoblivious hashing. **1992**, 39, 764-782		18
1517	Efficient PRAM simulation on a distributed memory machine. **1992**,		49
1516	A theory for memory-based learning. **1992**,		
1515	Practical minimal perfect hash functions for large databases. **1992**, 35, 105-121		55
1514	.		15
1513	Chapter 7 Fundamental algorithms and data structures. **1992**, 3, 323-373		
1512	. **1992**, 12, 23-30		174
1511	.		2
1510	Bounded Round Interactive Proofs in Finite Groups. **1992**, 5, 88-111		25
1509	On the theory of average case complexity. *Journal of Computer and System Sciences*, **1992**, 44, 193-219	1	89
1508	Linear-density hashing with dynamic overflow sharing. **1992**, 17, 359-380		1
1507	Pseudorandom generators for space-bounded computation. **1992**, 12, 449-461		210
1506	The computational complexity of universal hashing. **1993**, 107, 121-133		72
1505	Estimating the size of a relational join. **1993**, 18, 189-196		16
1504	Clocked adversaries for hashing. **1993**, 9, 239-252		11
1503	Mathematical problems in cryptology. **1993**, 67, 3373-3406		

1502	Bonsai: A compact representation of trees. **1993**, 23, 277-291		25
1501	Randomness in interactive proofs. **1993**, 3, 319-354		28
1500	Improved behaviour of tries by adaptive branching. **1993**, 46, 295-300		48
1499	Finding extremal sets in less than quadratic time. **1993**, 48, 29-34		18
1498	Rounds in Communication Complexity Revisited. *SIAM Journal on Computing*, **1993**, 22, 211-219	1.1	101
1497	On the Existence of Pseudorandom Generators. *SIAM Journal on Computing*, **1993**, 22, 1163-1175	1.1	71
1496	Local Randomness in Polynomial Random Number and Random Function Generators. *SIAM Journal on Computing*, **1993**, 22, 684-694	1.1	9
1495	A Monte-Carlo Algorithm for Estimating the Permanent. *SIAM Journal on Computing*, **1993**, 22, 284-293	1.1	64
1494	. **1993**, 11, 715-724		38
1493	Hashing strategies for simulating shared memory on distributed memory machines. **1993**, 20-29		9
1492	Randomized algorithms and pseudorandom numbers. **1993**, 40, 454-476		21
1491	Universal Hashing and Unconditional Authentication Codes.		1
1490	.		1
1489	Advances in Cryptology CRYPTO92. **1993**,		7
1488	. **1994**, 6, 79-85		2
1487	Simple fast parallel hashing. **1994**, 239-250		
1486	Advances in Cryptology EUROCRYPT 93. **1994**,		14
1485	Broadcast Encryption. **1993**, 480-491		569

1484	A BDD Package For A Massively Parallel SIMD Architecture.		0
1483	Provably good pattern generators for a random pattern test. **1994**, 11, 429-442		4
1482	Universal hashing and authentication codes. **1994**, 4, 369-380		145
1481	Algorithms for parallel memory, I: Two-level memories. **1994**, 12, 110-147		217
1480	Locality-preserving hash functions for general purpose parallel computation. **1994**, 12, 170-181		5
1479	RL(subseteq) SC. **1994**, 4, 1-11		36
1478	A combinatorial characterization of certain universal classes of hash functions. **1994**, 2, 161-166		1
1477	Combinatorial techniques for universal hashing. *Journal of Computer and System Sciences*, **1994**, 48, 337-346		25
1476	Locating P/poly optimally in the extended low hierarchy. **1994**, 134, 263-285		14
1475	An Integrity Check Value Algorithm for Stream Ciphers. **1993**, 40-48		27
1474	Secret-Key Reconciliation by Public Discussion. **1993**, 410-423		280
1473	A theory for memory-based learning. **1994**, 17, 143-167		7
1472	LFSR-based Hashing and Authentication. **1994**, 129-139		234
1471	Unique Binary-Search-Tree Representations and Equality Testing of Sets and Sequences. *SIAM Journal on Computing*, **1994**, 23, 24-44	1.1	5
1470	Communication-Space Tradeoffs for Unrestricted Protocols. *SIAM Journal on Computing*, **1994**, 23, 652-661	1.1	12
1469	Dynamic Perfect Hashing: Upper and Lower Bounds. *SIAM Journal on Computing*, **1994**, 23, 738-761	1.1	185
1468	.		16
1467	.		15

1466	Randomness-efficient oblivious sampling.		55
1465	Optimal Broadcast with Partial Knowledge. **1995**, 116-130		1
1464	Transformational design and implementation of a new efficient solution to the ready simulation problem. **1995**, 24, 189-220		51
1463	Using multiset discrimination to solve language processing problems without hashing. **1995**, 145, 189-228		32
1462	On quasilinear-time complexity theory. **1995**, 148, 325-349		17
1461	The optimal size of a signature. **1995**, 21, 67-75		
1460	Sublogarithmic searching without multiplications.		15
1459	References. **1995**, 447-466		
1458	Generalized privacy amplification. *IEEE Transactions on Information Theory*, **1995**, 41, 1915-1923	2.8	823
1457	On the structure of low sets [complexity classes].		3
1456	Committed Oblivious Transfer and Private Multi-Party Computation. **1995**, 110-123		76
1455	A2�odes from universal hash classes. **1995**, 311-318		
1454	Bucket Hashing and its Application to Fast Message Authentication. **1995**, 29-42		50
1453	A secure and efficient conference key distribution system. **1995**, 275-286		300
1452	Visual cryptography. **1995**, 1-12		874
1451	Towards average-case complexity analysis of NP optimization problems.		8
1450	On superlinear lower bounds in complexity theory.		0
1449	Implementing the hierarchical PRAM on the 2D mesh: analyses and experiments.		5

1448	.	2
1447	ChernoffHoeffding Bounds for Applications with Limited Independence. **1995**, 8, 223-250	145
1446	Introduction to special issue on randomized and derandomized algorithms. **1996**, 16, 359-366	
1445	Simulating BPP using a general weak random source. **1996**, 16, 367-391	94
1444	Efficient PRAM simulation on a distributed memory machine. **1996**, 16, 517-542	39
1443	Efficient cryptographic schemes provably as secure as subset sum. **1996**, 9, 199-216	96
1442	Software protection and simulation on oblivious RAMs. **1996**, 43, 431-473	820
1441	Discrepancy sets and pseudorandom generators for combinatorial rectangles.	11
1440	.	1
1439	Pseudorandom functions revisited: the cascade construction and its concrete security.	30
1438	On the knowledge complexity of /spl Nscr//spl Pscr/.	
1437	On selectable collisionful hash functions. **1996**, 287-298	2
1436	Fast rehashing in PRAM emulations. **1996**, 155, 349-363	
1435	Exploiting storage redundancy to speed up randomized shared memory simulations. **1996**, 162, 245-281	23
1434	Randomized algorithms. **1996**, 28, 33-37	68
1433	Comparing information without leaking it. **1996**, 39, 77-85	164
1432	An improvement of the digital cash protocol of Okamoto and Ohta. **1996**, 436-445	
1431	Keyed hash functions. **1996**, 201-214	13

1430	Oracles in □p are sufficient for exact learning. **1997**, 277-290		3
1429	A message authentication code based on latin squares. **1997**, 194-203		5
1428	Data Structures and Algorithms. **1997**,		2
1427	On the foundations of modern cryptography. **1997**, 46-74		17
1426	Efficient generation of shared RSA keys. **1997**, 425-439		126
1425	Quantum cryptanalysis of hash and claw-free functions. **1997**, 28, 14-19		54
1424	Unconditional security against memory-bounded adversaries. **1997**, 292-306		87
1423	Traceable visual cryptography. **1997**, 61-71		7
1422	Low-cost prevention of error-propagation for data compression with dynamic dictionaries.		2
1421	Accounting for memory bank contention and delay in high-bandwidth multiprocessors. *IEEE Transactions on Parallel and Distributed Systems*, **1997**, 8, 943-958	3.7	17
1420	Efficient hardware hashing functions for high performance computers. **1997**, 46, 1378-1381		127
1419	Error-Resilient Optimal Data Compression. *SIAM Journal on Computing*, **1997**, 26, 934-949	1.1	8
1418	MMH: Software message authentication in the Gbit/second rates. **1997**, 172-189		88
1417	Reliable communication over partially authenticated networks. **1997**, 245-259		4
1416	The complexity of generating test instances. **1997**, 375-386		
1415	Simulating Shared Memory in Real Time: On the Computation Power of Reconfigurable Architectures. **1997**, 137, 103-120		2
1414	Linking information reconciliation and privacy amplification. **1997**, 10, 97-110		129
1413	On the existence of statistically hiding bit commitment schemes and fail-stop signatures. **1997**, 10, 163-194		39

1412	Efficient construction of a small hitting set for combinatorial rectangles in high dimension. **1997**, 17, 215-234		30
1411	Perfect hashing. **1997**, 182, 1-143		79
1410	Approximation algorithms for multiple sequence alignment. **1997**, 182, 233-244		29
1409	Spatial match retrieval based on direction signatures using multiple key hashing scheme. **1997**, 12, 777-788		1
1408	A Reliable Randomized Algorithm for the Closest-Pair Problem. **1997**, 25, 19-51		103
1407	Recognizing Hamming graphs in linear time and space. **1997**, 63, 91-95		4
1406	Statistical secrecy and multibit commitments. *IEEE Transactions on Information Theory*, **1998**, 44, 1143-1158	2.8	29
1405	Sorting in Linear Time?. *Journal of Computer and System Sciences*, **1998**, 57, 74-93	1	56
1404	Approximating Hyper-Rectangles: Learning and Pseudorandom Sets. *Journal of Computer and System Sciences*, **1998**, 57, 376-388	1	24
1403	On probabilities of hash value matches. **1998**, 17, 171-176		11
1402	Randomized Data Structures for the Dynamic Closest-Pair Problem. *SIAM Journal on Computing*, **1998**, 27, 1036-1072	1.1	4
1401	New Collapse Consequences of NP Having Small Circuits. *SIAM Journal on Computing*, **1998**, 28, 311-324	1.1	46
1400	Min-wise independent permutations (extended abstract). **1998**,		185
1399	Simple Fast Parallel Hashing by Oblivious Execution. *SIAM Journal on Computing*, **1998**, 27, 1348-1375	1.1	2
1398	Optimal Broadcast with Partial Knowledge. *SIAM Journal on Computing*, **1998**, 28, 511-524	1.1	6
1397	.		29
1396	Unconditionally secure entity authentication.		
1395	Error resilient data compression with adaptive deletion.		

1394	. *IEEE Transactions on Parallel and Distributed Systems*, **1998**, 9, 1073-1087	3.7	1
1393	Provable security for block ciphers by decorrelation. **1998**, 249-275		49
1392	Cryptographic Primitives for Information Authentication State of the Art. **1998**, 49-104		13
1391	On contention resolution protocols and associated probabilistic phenomena. **1998**, 45, 324-378		14
1390	Sorting and searching on the word RAM. **1998**, 366-398		58
1389	A Derandomization Using Min-Wise Independent Permutations. **1998**, 15-24		8
1388	Complete problems for promise classes by optimal proof systems for test sets.		6
1387	A two-level signature file based on a block-oriented data model for spatial match retrieval. **1998**, 21, 467-478		4
1386	Protocols for asymmetric communication channels.		1
1385	Optimal lossless compression of a class of dynamic sources.		1
1384	Quantum cryptanalysis of hash and claw-free functions. **1998**, 163-169		76
1383	Secure and efficient metering. **1998**, 576-590		37
1382	Image density is complete for non-interactive-SZK. **1998**, 784-795		14
1381	On the foundations of oblivious transfer. **1998**, 361-374		25
1380	Using magnetic disk instead of main memory in the Mur ? verifier. **1998**, 172-183		36
1379	Simpler and faster dictionaries on the AC0 RAM. **1998**, 79-90		0
1378	Threshold traitor tracing. **1998**, 502-517		64
1377	Parsing and recognition of city, state, and ZIP codes in handwritten addresses. **1999**,		21

1376	Optimal bounds for the predecessor problem. **1999**,		30
1375	Space and time-efficient memory layout for multiple inheritance. **1999**,		20
1374	The State of Cryptographic Hash Functions. **1999**, 158-182		25
1373	Reliable communication over partially authenticated networks. **1999**, 220, 185-210		18
1372	CNN Algorithms for Video Authentication and Copyright Protection. **1999**, 23, 449-463		1
1371	How to Stretch Random Functions: The Security of Protected Counter Sums. **1999**, 12, 185-192		33
1370	Bucket Hashing and Its Application to Fast Message Authentication. **1999**, 12, 91-115		28
1369	Strongly universal hashing and identification codes via channels. *IEEE Transactions on Information Theory*, **1999**, 45, 2091-2095	2.8	18
1368	BPHSPACE(S)?DSPACE(S3/2). *Journal of Computer and System Sciences*, **1999**, 58, 376-403	1	39
1367	Lectures on Data Security. **1999**,		4
1366	Linear hash functions. **1999**, 46, 667-683		25
1365	Selected Areas in Cryptography. **1999**,		1
1364	An Optical Simulation of Shared Memory. *SIAM Journal on Computing*, **1999**, 28, 1829-1847	1.1	14
1363	A Pseudorandom Generator from any One-way Function. *SIAM Journal on Computing*, **1999**, 28, 1364-1396	1.1	876
1362	Space and time-efficient memory layout for multiple inheritance. **1999**, 34, 256-275		2
1361	Min-Wise Independent Permutations. *Journal of Computer and System Sciences*, **2000**, 60, 630-659	1	363
1360	Constructions of authentication codes from algebraic curves over finite fields. *IEEE Transactions on Information Theory*, **2000**, 46, 886-892	2.8	14
1359	Tracing traitors. *IEEE Transactions on Information Theory*, **2000**, 46, 893-910	2.8	184

1358	CBC MAC for Real-Time Data Sources. **2000**, 13, 315-338		82
1357	Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free. **2000**, 351-368		174
1356	Advances in Cryptology EUROCRYPT 2000. **2000**,		5
1355	Advances in Cryptology ASIACRYPT 2000. **2000**,		7
1354	ORACLES IN $Sigma^p_2$ ARE SUFFFICIENT FOR EXACT LEARNING. **2000**, 11, 613-632		3
1353	Inherently large traceability of broadcast encryption scheme.		2
1352	Information Security and Cryptology - ICISC9. **2000**,		6
1351	Selected Areas in Cryptography. **2000**,		4
1350	REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. **2000**, 159-174		106
1349	On RAM Priority Queues. *SIAM Journal on Computing*, **2000**, 30, 86-109	1.1	58
1348	Rigorous Time/Space Trade-offs for Inverting Functions. *SIAM Journal on Computing*, **2000**, 29, 790-803	1.1	27
1347	Contention Resolution in Hashing Based Shared Memory Simulations. *SIAM Journal on Computing*, **2000**, 29, 1703-1739	1.1	14
1346	On the Determinization of Weighted Finite Automata. *SIAM Journal on Computing*, **2000**, 30, 1502-1531	1.1	35
1345	A novel cache architecture to support layer-four packet classification at memory access speeds.		7
1344	Security against individual attacks for realistic quantum key distribution. *Physical Review A*, **2000**, 61,	2.6	460
1343	Efficient authentication and signing of multicast streams over lossy channels.		311
1342	Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness. **2000**, 49-61		22
1341	Quantum authentication of classical messages. *Physical Review A*, **2001**, 64,	2.6	75

1340	Analysis of a memory architecture for fast packet buffers.		35
1339	Using multiple hash functions to improve IP lookups.		86
1338	Cuckoo Hashing. **2001**, 121-133		79
1337	Literaturverzeichnis. **2001**, 325-332		
1336	Deterministic Dictionaries. **2001**, 41, 69-85		69
1335	Protocols for Asymmetric Communication Channels. *Journal of Computer and System Sciences*, **2001**, 63, 573-596	1	15
1334	Optimal encoding of non-stationary sources. **2001**, 135, 87-105		4
1333	Parallelizing the Mur? Verifier. **2001**, 18, 117-129		30
1332	Hash-based IP traceback. **2001**, 31, 3-14		138
1331	Approximate distance oracles. **2001**,		95
1330	Advances in Cryptology □EUROCRYPT 2001. **2001**,		13
1329	STACS 2001. **2001**,		2
1328	A data tracking scheme for general networks. **2001**,		11
1327	Compressed bloom filters. **2001**,		94
1326	On the cell probe complexity of membership and perfect hashing. **2001**,		14
1325	The faithfulness of abstract protocol analysis. **2001**,		18
1324	Hash-based IP traceback. **2001**,		271
1323	Streaming computation of combinatorial objects.		4

1322	Quantum pseudosignatures. **2002**, 49, 1269-1276		4
1321	.		23
1320	Expanders from symmetric codes. **2002**,		2
1319	Affinity-based management of main memory database clusters. **2002**, 2, 307-339		5
1318	Authenticated-encryption with associated-data. **2002**,		159
1317	Single-packet IP traceback. **2002**, 10, 721-734		233
1316	Compressed Bloom filters. **2002**, 10, 604-612		288
1315	A Functional Approach to External Graph Algorithms. **2002**, 32, 437-458		60
1314	Introduction to Cryptography. **2002**,		80
1313	Cost-effective flow table designs for high-speed routers: architecture and performance evaluation. **2002**, 37, 1089-1099		10
1312	Randomized Sorting in O(nloglogn) Time and Linear Space Using Addition, Shift, and Bit-wise Boolean Operations. **2002**, 42, 205-230		28
1311	Optimal Bounds for the Predecessor Problem and Related Problems. *Journal of Computer and System Sciences*, **2002**, 65, 38-72	1	98
1310	On the state of strength-three covering arrays. **2002**, 10, 217-238		92
1309	. **2003**, 36, 329-358		12
1308	Decorrelation: A Theory for Block Cipher Security. **2003**, 16, 249-286		106
1307	Optimal proof systems imply complete sets for promise classes. **2003**, 184, 71-92		38
1306	Secret-key agreement over unauthenticated public channels .II. Privacy amplification. *IEEE Transactions on Information Theory*, **2003**, 49, 839-851	2.8	90
1305	Secret-key agreement over unauthenticated public channels .I. Definitions and a completeness result. *IEEE Transactions on Information Theory*, **2003**, 49, 822-831	2.8	98

1304	Linear authentication codes: bounds and constructions. *IEEE Transactions on Information Theory*, **2003**, 49, 866-872	2.8	60
1303	Non-cryptographic primitive for pseudorandom permutation. **2003**, 306, 139-154		
1302	A derandomization using min-wise independent permutations. **2003**, 1, 11-20		4
1301	Chord: a scalable peer-to-peer lookup protocol for Internet applications. **2003**, 11, 17-32		1501
1300	Uniform hashing in constant time and linear space. **2003**,		24
1299	Tight lower bounds for the distinct elements problem.		20
1298	A Formally Verified Decentralized Key Management Architecture for Wireless Sensor Networks. **2003**, 27-39		16
1297	Dial-controlled hash: reducing path oscillation in multipath networks.		1
1296	What's hot and what's not. **2003**,		108
1295	Almost random graphs with simple hash functions. **2003**,		19
1294	Compact routing with name independence. **2003**,		17
1293	Time-space tradeoff lower bounds for integer multiplication and graphs of arithmetic functions. **2003**,		9
1292	Magic Functions. **2003**, 50, 852-921		72
1291	How to Re-use Round Function in Super-Pseudorandom Permutation. **2004**, 224-235		2
1290	The faithfulness of abstract protocol analysis: Message authentication*. **2004**, 12, 865-891		6
1289	Divide-and-concatenate: an architecture level optimization technique for universal hash functions. **2004**,		4
1288	CYSEP - a cyber-security processor for 10 Gbps networks and beyond.		1
1287	Using the BCH construction to generate robust linear hash functions.		1

1286	Selected Areas in Cryptography. **2004**,		3
1285	Universal hash functions over GF(2/sup n/).		2
1284	Compact name-independent routing with minimum stretch. **2004**,		30
1283	Reconciliation of a quantum-distributed Gaussian key. *IEEE Transactions on Information Theory*, **2004**, 50, 394-400	2.8	97
1282	Increasing Internet Capacity Using Local Search. **2004**, 29, 13-48		124
1281	The effect of side-information on smooth entropy. **2004**, 136, 151-157		
1280	Cuckoo hashing. **2004**, 51, 122-144		495
1279	Approximate caches for packet classification.		66
1278	Information Security and Privacy. **2004**,		3
1277	On the Use of GF-Inversion as a Cryptographic Primitive. **2004**, 234-247		7
1276	On Universal Classes of Extremely Random Constant-Time Hash Functions. *SIAM Journal on Computing*, **2004**, 33, 505-543	1.1	56
1275	Data stream algorithms for scalable bandwidth management. **2004**,		
1274	On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions. **2005**, 526-541		52
1273	A robust system for accurate real-time summaries of internet traffic. **2005**, 33, 85-96		7
1272	Fast hash table lookup using extended bloom filter. **2005**, 35, 181-192		102
1271	Bounds on the OBDD-size of integer multiplication via universal hashing. *Journal of Computer and System Sciences*, **2005**, 71, 520-534	1	14
1270	On the maximum admissible error and key compression degree in quantum cryptography on two nonorthogonal states. **2005**, 81, 599-604		
1269	Practical error-correction procedures in quantum cryptography. *Journal of Experimental and Theoretical Physics*, **2005**, 101, 230-252	1	5

1268	On the privacy-preserving cascade method for correcting errors in primary keys in quantum cryptography. **2005**, 82, 768-772		
1267	On the power of quantum memory. *IEEE Transactions on Information Theory*, **2005**, 51, 2391-2401	2.8	42
1266	CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. **2005**, 18, 111-131		34
1265	Efficient reliable communication over partially authenticated networks. **2005**, 18, 1-19		7
1264	Progress in Computational Complexity Theory. **2005**, 20, 735-750		1
1263	MRD Hashing. **2005**, 37, 229-242		
1262	Badger □A Fast and Provably Secure MAC. **2005**, 176-191		17
1261	Bibliography. **2005**, 504-509		
1260	A Practical and Secure Communication Protocol in the Bounded Storage Model. **2005**, 707-717		2
1259	Efficient packet classification with digest caches. **2005**, 33-54		5
1258	Segmented hash. **2005**,		32
1257	Name independent routing for growth bounded networks. **2005**,		20
1256	A NOVEL PROTOCOL-AUTHENTICATION ALGORITHM RULING OUT A MAN-IN-THE MIDDLE ATTACK IN QUANTUM CRYPTOGRAPHY. **2005**, 03, 225-231		11
1255	New approaches for deniable authentication. **2005**,		24
1254	Power optimization for universal hash function data path using divide-and-concatenate technique. **2005**,		
1253	A robust system for accurate real-time summaries of internet traffic. **2005**,		25
1252	Fast hash table lookup using extended bloom filter. **2005**,		102
1251	Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, **2005**, 72,	2.6	278

1250	An Efficient Equi-semi-join Algorithm for Distributed Architectures. **2005**, 755-763	7
1249	Approximate distance oracles. **2005**, 52, 1-24	308
1248	What’s hot and what’s not: tracking most frequent items dynamically. **2005**, 30, 249-278	155
1247	Energy scalable universal hashing. **2005**, 54, 1484-1495	32
1246	. **2005**, 24, 1740-1747	
1245	Information Security and Cryptology. **2005**,	4
1244	External double hashing with choice.	0
1243	Range-efficient computation of F/sub 0/ over massive data streams.	11
1242	On constructing parallel pseudorandom generators from one-way functions.	18
1241	Universally Composable Privacy Amplification Against Quantum Adversaries. **2005**, 407-425	119
1240	A Variant of Poly1305 MAC and Its Security Proof. **2005**, 375-380	1
1239	Design and Analysis of Randomized Algorithms. **2005**,	27
1238	Complexity Theory and Cryptology. **2005**,	3
1237	Cryptography and Coding. **2005**,	2
1236	New Proofs for NMAC and HMAC: Security Without Collision-Resistance. **2006**, 602-619	162
1235	OPMAC: One-Key Poly1305 MAC. **2006**, 78-87	
1234	An Improved Poly1305 MAC. **2006**, 284-292	
1233	Stream-Based Implementation of Hash Functions for Multi-Gigabit Message Authentication Codes. **2006**,	5

1232	Topics in Cryptology CT-RSA 2007. **2006**,		
1231	Information Security and Cryptology. **2006**,		0
1230	Virtually Pipelined Network Memory. **2006**,		3
1229	An Efficient One-key Carter-Wegman Message Authentication Code. **2006**,		1
1228	Parallel repetition of zero-knowledge proofs and the possibility of basing cryptography on NP-hardness.		8
1227	FUNCTION FIELDS OVER FINITE FIELDS AND THEIR APPLICATIONS TO CRYPTOGRAPHY. **2006**, 59-104		2
1226	Low-power bloom filter architecture for deep packet inspection. **2006**, 10, 210-212		33
1225	Reversible Sketch Based on the XOR-Based Hashing. **2006**,		2
1224	Compact Routing with Name Independence. **2006**, 20, 705-726		6
1223	Time-Space Lower Bounds for the Polynomial-Time Hierarchy on Randomized Machines. *SIAM Journal on Computing*, **2006**, 36, 563-594	1.1	12
1222	A High-Speed Hardware Architecture for Universal Message Authentication Code. **2006**, 24, 1831-1839		7
1221	Detection of Super Sources and Destinations in High-Speed Networks: Algorithms, Analysis and Evaluation. **2006**, 24, 1840-1852		32
1220	An energy-efficient and access latency optimized indexing scheme for wireless data broadcast. **2006**, 18, 1111-1124		38
1219	A low power lookup technique for multi-hashing network applications.		5
1218	Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets. **2006**, 232-250		72
1217	Bibliography. 249-258		
1216	Hash chains with diminishing ranges for sensors. **2006**, 4, 31		4
1215	EMMA: an efficient massive mapping algorithm using improved approximate mapping filtering. **2006**, 38, 857-64		

1214	Variationally universal hashing. **2006**, 100, 36-39		2
1213	Error-bounded probabilistic computations between MA and AM. *Journal of Computer and System Sciences*, **2006**, 72, 1043-1076	1	12
1212	A construction method for optimally universal hash families and its consequences for the existence of RBIBDs. **2006**, 363, 76-84		
1211	Some conservative estimates in quantum cryptography. *Journal of Experimental and Theoretical Physics*, **2006**, 103, 198-205	1	
1210	Parity graph-driven read-once branching programs and an exponential lower bound for integer multiplication. **2006**, 362, 86-99		9
1209	Secret sharing schemes with partial broadcast channels. **2006**, 41, 5-22		5
1208	Quantum cryptography beyond key exchange. **2006**, 21, 39-54		3
1207	Time-Space Tradeoff in Derandomizing Probabilistic Logspace. **2006**, 39, 189-208		4
1206	Energy-Efficient Pipelined Bloom Filters for Network Intrusion Detection. **2006**,		4
1205	Fast and robust TCP session lookup by digest hash. **2006**,		2
1204	High-throughput sketch update on a low-power stream processor. **2006**,		8
1203	On space-stretch trade-offs. **2006**,		12
1202	A Classical Introduction to Cryptography. **2006**,		1
1201	A XOR-Based Hierarchical Sketch for Identifying and Estimating Hierarchical Frequent Items Online. **2006**,		
1200	Efficient Protocols Achieving the Commitment Capacity of Noisy Correlations. **2006**,		11
1199	Derandomization of probabilistic auxiliary pushdown automata classes.		0
1198	Finding Hierarchical Frequent Items in Data Streams. **2006**,		
1197	Applied Cryptography and Network Security. **2006**,		1

1196	A New Interactive Hashing Theorem. **2007**,		12
1195	On the Extreme Parallelism Inside Next-Generation Network Processors. **2007**,		5
1194	Strong-diameter decompositions of minor free graphs. **2007**,		7
1193	Cryptographic Hardware and Embedded Systems - CHES 2007. **2007**,		8
1192	Pseudo-random number generation for sketch-based estimations. **2007**, 32, 11		11
1191	Time-decaying sketches for sensor data aggregation. **2007**,		12
1190	Modeling service discovery in ad-hoc networks. **2007**,		2
1189	Robust key generation from signal envelopes in wireless networks. **2007**,		129
1188	Combinatorial characterizations of authentication codes in verification oracle model. **2007**,		1
1187	Modeling cryptographic properties of voice and voice-based entity authentication. **2007**,		4
1186	Linear probing with constant independence. **2007**,		10
1185	Upper bounds of eavesdropper� performances in finite-length code with the decoy method. *Physical Review A*, **2007**, 76,	2.6	87
1184	Simple and Adaptive Identification of Superspreaders by Flow Sampling. **2007**,		19
1183	Design Strategies for Minimal Perfect Hash Functions. **2007**, 2-17		7
1182	FPGA Intrinsic PUFs and Their Use for IP Protection. **2007**, 63-80		446
1181	Privacy amplification for quantum key distribution. **2007**, 40, F99-F104		9
1180	Norm, Point, and Distance Estimation Over Multiple Signals Using Max-Stable Distributions. **2007**,		2
1179	Quantum technology and cryptology for information security. **2007**,		

1178	Power Optimization for Universal Hash Function Data Path Using Divide-and-Concatenate Technique. **2007**, 26, 1763-1769		
1177	Range-Efficient Counting of Distinct Elements in a Massive Data Stream. *SIAM Journal on Computing*, **2007**, 37, 359-379	1.1	14
1176	A Probabilistic Study on Combinatorial Expanders and Hashing. *SIAM Journal on Computing*, **2007**, 37, 83-111	1.1	3
1175	Introduction to Cryptography. **2007**,		66
1174	A Single Key MAC Based on Hash127. **2007**,		
1173	Applying Cuckoo Hashing for FPGA-based Pattern Matching in NIDS/NIPS. **2007**,		12
1172	Combining static and dynamic defect-tolerance techniques for nanoscale memory systems. **2007**,		2
1171	Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection. **2007**,		130
1170	A Scalable Bloom Filter for Membership Queries. **2007**,		11
1169	An Efficient Policy-based Packet Scheduler With Flow Cache. **2007**,		1
1168	Secure and Authenticated Communication in Chip-Level Microcomputer Bus Systems with Tree Parity Machines. **2007**,		8
1167	On Scalable Attack Detection in the Network. **2007**, 15, 14-25		37
1166	An introduction to modern cryptology. **2007**, 565-592		
1165	Key management for content access control in a hierarchy. **2007**, 51, 3197-3219		36
1164	A note on local randomness in polynomial random number and random function generators. **2007**, 186, 1360-1366		
1163	Efficient implementation of AhoCorasick pattern matching automata using Unicode. **2007**, 37, 669-690		5
1162	Entanglement-based quantum communication over 144 km. **2007**, 3, 481-486		651
1161	Source Coding Using Families of Universal Hash Functions. *IEEE Transactions on Information Theory*, **2007**, 53, 3226-3233	2.8	5

1160	On Defining Partition Entropy by Inequalities. *IEEE Transactions on Information Theory*, **2007**, 53, 3233-3239	2.8	6
1159	Public classical communication in quantum cryptography: Error correction, integrity, and authentication. *Journal of Experimental and Theoretical Physics*, **2007**, 104, 675-688	1	
1158	Biosequence Similarity Search on the Mercury System. **2007**, 49, 101-121		21
1157	In search of mathematical primitives for deriving universal projective hash families. **2008**, 19, 161-173		1
1156	Approximate colored range and point enclosure queries. **2008**, 6, 420-432		7
1155	Secure communication in microcomputer bus systems for embedded devices. *Journal of Systems Architecture*, **2008**, 54, 1065-1076	5.5	11
1154	Cryptographic robustness of practical quantum cryptography: BB84 key distribution protocol. *Journal of Experimental and Theoretical Physics*, **2008**, 107, 28-48	1	3
1153	Is there a fundamental limit on the key distribution distance in quantum cryptography?. **2008**, 88, 693-697		3
1152	Security Aspects of the Authentication Used in Quantum Cryptography. *IEEE Transactions on Information Theory*, **2008**, 54, 1735-1741	2.8	29
1151	The Commitment Capacity of the Gaussian Channel Is Infinite. *IEEE Transactions on Information Theory*, **2008**, 54, 2785-2789	2.8	14
1150	On the Oblivious-Transfer Capacity of Noisy Resources. *IEEE Transactions on Information Theory*, **2008**, 54, 2572-2581	2.8	38
1149	Wireless Information-Theoretic Security. *IEEE Transactions on Information Theory*, **2008**, 54, 2515-2534	2.8	1157
1148	Authenticating ad hoc networks by comparison of short digests. **2008**, 206, 250-271		25
1147	Algorithms and Data Structures. **2008**,		11
1146	Entangled quantum key distribution over two free-space optical links. **2008**, 16, 16840-53		58
1145	Uniform Hashing in Constant Time and Optimal Space. *SIAM Journal on Computing*, **2008**, 38, 85-96	1.1	47
1144	Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM Journal on Computing*, **2008**, 38, 97-139	1.1	905
1143	SECURITY OF QUANTUM KEY DISTRIBUTION. **2008**, 06, 1-127		237

1142	An Inter-Classes Obfuscation Method for Java Program. **2008**,		
1141	A practical scheme for string commitment based on the Gaussian channel. **2008**,		2
1140	. **2008**,		31
1139	Extracting classical randomness in a quantum world. **2008**,		1
1138	Complexity Attack Resistant Flow Lookup Schemes for IPv6: A Measurement Based Comparison. **2008**,		
1137	Hash property and Wyner-Ziv source coding by using sparse matrices and maximum-likelihood coding. **2008**,		0
1136	Biometric Template Security. **2008**, 2008, 579416		560
1135	Cryptography with constant computational overhead. **2008**,		83
1134	BackSpace: Formal Analysis for Post-Silicon Debug. **2008**,		40
1133	SAMPLING IN DYNAMIC DATA STREAMS AND APPLICATIONS. **2008**, 18, 3-28		18
1132	Robust resource allocation for online network monitoring. **2008**,		
1131	Cryptographic Hardware and Embedded Systems □CHES 2008. **2008**,		5
1130	Uniform deterministic dictionaries. **2008**, 4, 1-23		6
1129	Compact dictionaries for variable-length keys and data with applications. **2008**, 4, 1-25		10
1128	A dictionary implementation based on dynamic perfect hashing. *Journal of Experimental Algorithmics*, **2008**, 12, 1-25	1.1	0
1127	Handling data skew in parallel joins in shared-nothing systems. **2008**,		53
1126	Hashed samples. **2008**, 1, 201-212		33
1125	Embedding and similarity search for point sets under translation. **2008**,		

1124	Security and Cryptography for Networks. **2008**,		
1123	Distributed sampling for on-line SLA assessment. **2008**,		5
1122	. **2008**, 16, 705-717		78
1121	Brand and IP protection with physical unclonable functions. **2008**,		42
1120	Extracting Worm-Infected Hosts Using White List. **2008**,		2
1119	Quantum Merkle Puzzles. **2008**,		13
1118	Tomography increases key rates of quantum-key-distribution protocols. *Physical Review A*, **2008**, 78,	2.6	33
1117	Physical underpinnings of privacy. *Physical Review A*, **2008**, 78,	2.6	38
1116	Secret key agreement by reliability information of signals in Gaussian Maurer□ Model. **2008**,		2
1115	Cryptography from noisy storage. **2008**, 100, 220502		83
1114	Bibliography. 566-571		
1113	Bibliography. 549-574		
1112	Spillover reduction for linear distributed-parameter systems using dynamic extensions. **2009**,		
1111	Entanglement enhances security in quantum communication. *Physical Review A*, **2009**, 80,	2.6	23
1110	Efficient oblivious transfer from algebraic signaling over the Gaussian channel. **2009**,		3
1109	Physical Unclonable Functions and Their Applications to Vehicle System Security. **2009**,		6
1108	Optimal ratio between phase basis and bit basis in quantum key distributions. *Physical Review A*, **2009**, 79,	2.6	3
1107	Random number generation from multipath propagation: MIMO-based encryption key establishment. **2009**,		3

1106	Multichannel Protocols for User-Friendly and Scalable Initialization of Sensor Networks. **2009**, 228-247	4
1105	Secrecy Extraction from Increased Randomness in a Time-Variant MIMO Channel. **2009**,	4
1104	On secret key agreement from the additive white Gaussian noise channel. **2009**,	1
1103	Explicit construction of a small epsilon-net for linear threshold functions. **2009**,	7
1102	Divide and discriminate. **2009**,	7
1101	Entangled quantum key distribution with a biased basis choice. **2009**, 11, 045025	15
1100	K-Stage Pipelined Bloom Filter for Packet Classification. **2009**,	7
1099	Distributed authentication for randomly compromised networks. **2009**, 11, 085005	
1098	Type-based categorization of relational attributes. **2009**,	9
1097	Dynamic external hashing. **2009**,	2
1096	Locating XML Documents in a Peer-to-Peer Network Using Distributed Hash Tables. **2009**, 21, 1737-1752	17
1095	RESPONSE TO "VULNERABILITY OF ’A NOVEL PROTOCOL-AUTHENTICATION ALGORITHM RULING OUT A MAN-IN-THE-MIDDLE ATTACK IN QUANTUM CRYPTOGRAPHY’". **2009**, 07, 1401-1407	5
1094	Approximate counting by hashing in bounded arithmetic. **2009**, 74, 829-860	13
1093	Hierarchical Sampling from Sketches: Estimating Functions over Data Streams. **2009**, 53, 549-582	4
1092	Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions. **2009**, 11, 19-41	47
1091	Reducing Complexity Assumptions for Statistically-Hiding Commitment. **2009**, 22, 283-310	2
1090	On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions. **2009**, 22, 311-329	5
1089	New Approaches for Deniable Authentication. **2009**, 22, 572-615	27

1088	Dispersing hash functions. *Random Structures and Algorithms*, **2009**, 35, 70-82	0.8	0
1087	Quantum key distribution in a single-photon regime with nonorthogonal basis states. **2009**, 89, 370-376		1
1086	On one asymptotic property of time-shift quantum cryptography. **2009**, 90, 548-554		
1085	Indirect Branch Validation Unit. **2009**, 33, 461-468		1
1084	Universal hash functions for an infinite universe and hash trees. **2009**, 109, 461-462		
1083	The security of practical quantum key distribution. *Reviews of Modern Physics*, **2009**, 81, 1301-1350	40.5	1763
1082	Security of a two-parameter quantum cryptography system using time-shifted states against photon-number splitting attacks. *Journal of Experimental and Theoretical Physics*, **2009**, 109, 557-584	1	7
1081	SSL/TLS with Quantum Cryptography. **2009**,		2
1080	On the use of hash tables in real-time applications. **2009**,		1
1079	Continuous high speed coherent one-way quantum key distribution. **2009**, 17, 13326-34		38
1078	High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. **2009**, 11, 075003		186
1077	Identity and Privacy in the Internet Age. **2009**,		1
1076	Aggregated Authentication (AMAC) Using Universal Hash Functions. **2009**, 248-264		2
1075	Information Theoretic Security. **2009**,		
1074	Ensuring data storage security in Cloud Computing. **2009**,		216
1073	Fast Software Encryption. **2009**,		1
1072	High-Bandwidth Network Memory System Through Virtual Pipelines. **2009**, 17, 1029-1041		7
1071	Construction of wiretap channel codes by using sparse matrices. **2009**,		2

1070	Improving Signatures by Locality Exploitation for Transactional Memory. **2009**,		17
1069	A Fuzzy Extractor Based on Smooth Entropy. **2009**,		
1068	Choosing Best Hashing Strategies and Hash Functions. **2009**,		12
1067	A New Characterization of ACC^0 and Probabilistic CC^0. **2009**,		2
1066	Fuzzy matching of objects using fuzzy commitment. **2009**,		
1065	Coding theorem for general stationary memoryless channel based on hash property. **2009**,		
1064	Opportunities and Limits of Remote Timing Attacks. **2009**, 12, 1-29		102
1063	An efficient parallel algorithm for evaluating join queries on heterogeneous distributed systems. **2009**,		4
1062	A New Data Streaming Method for Locating Hosts with Large Connection Degree. **2009**,		9
1061	Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. **2009**, 58, 1198-1210		490
1060	Transparent code authentication at the processor level. **2009**, 3, 354		1
1059	Linear Probing with Constant Independence. *SIAM Journal on Computing*, **2009**, 39, 1107-1120	1.1	17
1058	Some Open Questions Related to Cuckoo Hashing. **2009**, 1-10		13
1057	Secret Communication over Fading Channels. **2009**, 281-309		
1056	Searching. **2009**, 1-16		1
1055	Quantum Information Theory and Its Difficulty. **2009**, 3, 44-56		
1054	PAMELA: Pattern Matching Engine with Limited-Time Update for NIDS/NIPS. **2009**, E92-D, 1049-1061		3
1053	On Risks of Using Cuckoo Hashing with Simple Universal Hash Classes. **2009**,		9

1052	Secret Key Agreement from Correlated Gaussian Sources by Rate Limited Public Communication. **2010**, E93-A, 1976-1983		23
1051	On the passive probing of fiber optic quantum communication channels. *Journal of Experimental and Theoretical Physics*, **2010**, 110, 561-567	1	3
1050	Quantum key distribution and 1 Gbps data encryption over a single fibre. **2010**, 12, 063027		131
1049	Cryptographic hash functions. **2010**, 5, 431-448		43
1048	Algorithmische Grundlagen verteilter Speichersysteme. **2010**, 33, 468-474		
1047	A New Characterization of ACC0 and Probabilistic CC0. **2010**, 19, 211-234		9
1046	Are PCPs Inherent in Efficient Arguments?. **2010**, 19, 265-304		11
1045	An Improved Version of Cuckoo Hashing: Average Case Analysis of Construction Cost and Search Operations. **2010**, 3, 47-60		4
1044	Information-Theoretically Secret Key Generation for Fading Wireless Channels. **2010**, 5, 240-254		242
1043	Hash property and coding theorems for sparse matrices and maximum-likelihood coding. *IEEE Transactions on Information Theory*, **2010**, 56, 2143-2167	2.8	20
1042	Hash Property and Fixed-Rate Universal Coding Theorems. *IEEE Transactions on Information Theory*, **2010**, 56, 2688-2698	2.8	7
1041	Minutiae and modified Biocode fusion for fingerprint-based key generation. **2010**, 33, 221-235		20
1040	Bounds on the efficiency of black-box commitment schemes. **2010**, 411, 1251-1260		1
1039	Recursive n-gram hashing is pairwise independent, at best. **2010**, 24, 698-710		15
1038	Enhancement of the robustness of phase-time quantum cryptography by block error correction. **2010**, 92, 490-495		
1037	References. **2010**, 271-278		
1036	Interactive low-complexity codes for synchronization from deletions and insertions. **2010**,		16
1035	The power of primes: security of authentication based on a universal hash-function family. **2010**, 4,		10

1034	Construction of wiretap codes from ordinary channel codes. **2010**,		25
1033	Leftover Hashing against quantum side information. **2010**,		10
1032	Distributed monitoring of conditional entropy for anomaly detection in streams. **2010**,		10
1031	Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Physical Review A*, **2010**, 82,	2.6	15
1030	Practical issues in quantum-key-distribution postprocessing. *Physical Review A*, **2010**, 81,	2.6	112
1029	Energy Friendly Integrity for Network Coding in Wireless Sensor Networks. **2010**,		8
1028	Fast Message Authentication Code for Multiple Messages with Provable Security. **2010**,		1
1027	Polar coding for secure transmission and key agreement. **2010**,		33
1026	Secure Wireless Communication with Dynamic Secrets. **2010**,		30
1025	Semi-join computation on distributed file systems using map-reduce-merge model. **2010**,		5
1024	A new TCB cache to efficiently manage TCP sessions for web servers. **2010**,		7
1023	Cache-oblivious hashing. **2010**,		4
1022	Broadband Quantum Cryptography. **2010**, 2, 1-97		5
1021	Ensuring data storage security in cloud computing using Sobol Sequence. **2010**,		11
1020	Quantum Readout of Physical Unclonable Functions. **2010**, 369-386		8
1019	Improving the Generalized Feistel. **2010**, 19-39		63
1018	An optimal algorithm for the distinct elements problem. **2010**,		112
1017	Securing Wireless Communications at the Physical Layer. **2010**,		110

1016	A new IP lookup cache for high performance IP routers. **2010**,		10
1015	Algorithms for Next Generation Networks. **2010**,		5
1014	Packet sampling for worm and botnet detection in TCP connections. **2010**,		8
1013	Information Security and Cryptology. **2010**,		
1012	Differential template attacks on PUF enabled cryptographic devices. **2010**,		51
1011	Time-decaying Sketches for Robust Aggregation of Sensor Data. *SIAM Journal on Computing*, **2010**, 39, 1309-1339	1.1	11
1010	Analysis of switching properties of different high voltage IGBTs operating under hard-switching conditions. **2010**,		
1009	. **2010**, 18, 81-94		2
1008	Decoding of the (47, 24, 11) Quadratic Residue Code with Hash Table. **2010**,		
1007	Explicit Construction of a Small $epsilon$-Net for Linear Threshold Functions. *SIAM Journal on Computing*, **2010**, 39, 3501-3520	1.1	16
1006	Construction of broadcast channel code based on hash property. **2010**,		3
1005	Misusing universal hash functions: security analysis of a hardware efficient stream cipher model using LFSR based hash function. **2010**,		3
1004	A Covert Timing Channel via Algorithmic Complexity Attacks: Design and Analysis. **2011**,		2
1003	Secure Multiplex Network Coding. **2011**,		18
1002	Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients. **2011**, 10, 205-215		105
1001	Unified Signatures for Improving Performance in Transactional Memory. **2011**,		6
1000	Balls and Bins: Smaller Hash Families and Faster Evaluation. **2011**,		6
999	Linear Probing with 5-wise Independence. **2011**, 53, 547-558		8

998	A Data Streaming Method for Monitoring Host Connection Degrees of High-Speed Links. **2011**, 6, 1086-1098		23
997	. **2011**, 19, 788-801		6
996	Non-crypto Hardware Hash Functions for High Performance Networking ASICs. **2011**,		13
995	SWHash: An Efficient Data Integrity Verification Scheme Appropriate for USB Flash Disk. **2011**,		
994	Synopses for Massive Data: Samples, Histograms, Wavelets, Sketches. **2011**, 4, 1-294		191
993	A Formalization of the Security Features of Physical Functions. **2011**,		96
992	Secure device-independent quantum key distribution with causally independent measurement devices. **2011**, 2, 238		210
991	Information Theoretic Security. **2011**,		1
990	Computability and Complexity Theory. **2011**,		18
989	A Three Dimensional Sharp Interface Cartesian Grid Method For Solving High Speed Multi-Material Impact Problems.. **2011**,		
988	Cancelable biometric template generation and protection schemes: A review. **2011**,		8
987	Fine-Grained DDoS Detection Scheme Based on Bidirectional Count Sketch. **2011**,		8
986	On the Power of the Randomized Iterate. *SIAM Journal on Computing*, **2011**, 40, 1486-1528	1.1	14
985	Encyclopedia of Cryptography and Security. **2011**, 929-934		1
984	References. 311-322		
983	Random Walks and Rapid Mixing. **2011**, 563-650		0
982	Hardware acceleration of transactional memory on commodity systems. **2011**, 39, 27-38		0
981	Bit Commitment From Nonsignaling Correlations. *IEEE Transactions on Information Theory*, **2011**, 57, 1770-1779	2.8	1

980	Exponential Decreasing Rate of Leaked Information in Universal Random Privacy Amplification. *IEEE Transactions on Information Theory*, **2011**, 57, 3989-4001	2.8	207
979	Leftover Hashing Against Quantum Side Information. *IEEE Transactions on Information Theory*, **2011** , 57, 5524-5535	2.8	152
978	Achieving Oblivious Transfer Capacity of Generalized Erasure Channels in the Malicious Model. *IEEE Transactions on Information Theory*, **2011**, 57, 5566-5571	2.8	16
977	Sharp lower bounds on the extractable randomness from non-uniform sources. **2011**, 209, 1184-1196		7
976	Leftover Hash Lemma, Revisited. **2011**, 1-20		47
975	Quantum key distribution with a reference quantum state. *Journal of Experimental and Theoretical Physics*, **2011**, 113, 743-754	1	1
974	Computation using noise-based logic: efficient string verification over a slow communication channel. **2011**, 79, 85-90		10
973	A trade-off between collision probability and key size in universal hashing using polynomials. **2011**, 58, 271-278		6
972	One-Way Protocol for Two-Bit Intrinsic Random Key Distribution with Entangled Photon Pairs. **2011** , 50, 663-670		1
971	Energy-Efficient Paths in Radio Networks. **2011**, 61, 298-319		1
970	Universally composable and customizable post-processing for practical quantum key distribution. **2011**, 30, 172-177		27
969	Deterministic extractors for small-space sources. *Journal of Computer and System Sciences*, **2011**, 77, 191-220	1	22
968	ON "THE POWER OF VERIFICATION QUERIES" IN UNCONDITIONALLY SECURE MESSAGE AUTHENTICATION. **2011**, 03, 287-303		
967	FUZZY UNIVERSAL HASHING AND APPROXIMATE AUTHENTICATION. **2011**, 03, 587-607		3
966	Hardware acceleration of transactional memory on commodity systems. **2011**,		10
965	Parallel evaluation of conjunctive queries. **2011**,		56
964	Understanding bloom filter intersection for lazy address-set disambiguation. **2011**,		4
963	Application-specific signatures for transactional memory in soft processors. **2011**, 4, 1-14		

962	FPGA Implementation of Secure Time Shared Hash Stream Cipher. **2011**,		1
961	Quantum key distribution with finite resources: Secret key rates via R▯yi entropies. *Physical Review A*, **2011**, 84,	2.6	10
960	Construction of multiple access channel codes based on hash property. **2011**,		1
959	Signal Sets for Secret Key Agreement With Public Discussion Based on Gaussian and Fading Channels. **2011**, 6, 523-531		4
958	Secure multiplex coding with a common message. **2011**,		5
957	Accelerating sketch-based network flow processing using Graphics Processing Unit. **2011**,		
956	Universally attainable error and information exponents, and equivocation rate for the broadcast channels with confidential messages. **2011**,		5
955	Construction of strongly secure wiretap channel code based on hash property. **2011**,		9
954	Long-term performance of the SwissQuantum quantum key distribution network in a field environment. **2011**, 13, 123001		168
953	Multiset signatures for transactional memory. **2011**,		6
952	Hardware acceleration of transactional memory on commodity systems. **2011**, 46, 27-38		5
951	Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey. **2011**, 19, 139-201		37
950	Private randomness expansion with untrusted devices. **2011**, 44, 095305		203
949	Compressed matrix multiplication. **2012**,		9
948	Field test of classical symmetric encryption with continuous variables quantum key distribution. **2012**, 20, 14030-41		78
947	The Power of Simple Tabulation Hashing. **2012**, 59, 1-50		23
946	Universal Sequencing on an Unreliable Machine. *SIAM Journal on Computing*, **2012**, 41, 565-586	1.1	26
945	. **2012**,		1

944	Quantum readout of Physical Unclonable Functions. **2012**, 10, 1250001		19
943	Lightweight Integrity for XOR Network Coding in Wireless Sensor Networks. **2012**, 245-258		2
942	QUANTUM KEY EVOLUTION AND ITS APPLICATIONS. **2012**, 10, 1250044		3
941	Thematic Data Index Construction Based on Urban Data. **2012**, 198-199, 596-600		1
940	Two-party key establishment: From passive to active security without introducing new assumptions. **2012**, 4, 1-17		
939	References. **2012**, 420-454		
938	Tabulation-Based 5-Independent Hashing with Applications to Linear Probing and Second Moment Estimation. *SIAM Journal on Computing*, **2012**, 41, 293-331	1.1	32
937	Precise evaluation of leaked information with universal2 privacy amplification in the presence of quantum attacker. **2012**,		4
936	Iterative Expansion and Color Coding. **2012**, 8, 1-22		8
935	Uniform random number generation by using sparse matrix. **2012**,		4
934	RAIDR: Retention-aware intelligent DRAM refresh. **2012**,		44
933	Overcoming weak expectations. **2012**,		5
932	Privacy amplification theorem for bounded storage eavesdropper. **2012**,		0
931	Robust Fuzzy Extractors and Authenticated Key Agreement From Close Secrets. *IEEE Transactions on Information Theory*, **2012**, 58, 6207-6222	2.8	49
930	An OpenCL Implementation of Sketch-Based Network Traffic Change Detection on GPU. **2012**,		
929	On the potential of PUF for pseudonym generation in vehicular networks. **2012**,		11
928	Expurgation exponent of leaked information in privacy amplification for binary sources. **2012**,		
927	Securing home networks using Physically Unclonable Functions. **2012**,		1

926	Tight finite-key analysis for quantum cryptography. **2012**, 3, 634		321
925	Tracking millions of flows in high speed networks for application identification. **2012**,		1
924	Toward Secure and Dependable Storage Services in Cloud Computing. **2012**, 5, 220-232		261
923	Resistance against Iterated Attacks by Decorrelation Revisited. **2012**, 741-757		2
922	Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer. **2012**, 25, 680-722		51
921	Quantum key distribution on composite photons, polarization qutrits. **2012**, 96, 336-341		9
920	On the resistance of relativistic quantum cryptography in open space at finite resources. **2012**, 96, 342-348		5
919	D-Cache: Universal Distance Cache for Metric Access Methods. **2012**, 24, 868-881		18
918	Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. **2012**, 14, 123018		44
917	Pseudorandomness. **2012**, 7, 1-336		118
916	Public key encryption without random oracle made truly practical. **2012**, 38, 975-985		1
915	SCD: A scalable coherence directory with flexible sharer set encoding. **2012**,		71
914	Near-Linear Unconditionally-Secure Multiparty Computation with a Dishonest Minority. **2012**, 663-680		54
913	Polar Coding for Secure Transmission and Key Agreement. **2012**, 7, 1472-1483		48
912	Functional verification of signature detection architectures for high speed network applications. **2012**, 9, 395-402		7
911	Clustering Streaming Graphs. **2012**,		4
910	Information and Communications Security. **2012**,		1
909	Entropy uncertainty relations and stability of phase-temporal quantum cryptography with finite-length transmitted strings. *Journal of Experimental and Theoretical Physics*, **2012**, 115, 969-985	1	3

908	Introduction to Hardware Security and Trust. **2012**,		99
907	Fast Software Encryption. **2012**,		2
906	Construction of Orthogonal Arrays of Index Unity Using Logarithm Tables for Galois Fields. **2012**,		2
905	Energy efficient authentication strategies for network coding. **2012**, 24, 1086-1107		1
904	Entanglement of the Antisymmetric State. **2012**, 311, 397-422		33
903	A Statistical Analysis of Probabilistic Counting Algorithms. **2012**, 39, 1-14		8
902	The universality of iterated hashing over variable-length strings. **2012**, 160, 604-617		4
901	Structures and lower bounds for binary covering arrays. **2012**, 312, 2958-2968		7
900	Low-contention data structures. **2012**, 72, 705-715		
899	A new multistage approach to detect subtle DDoS attacks. **2012**, 55, 198-213		41
898	Load-Balancing Multipath Switching System with Flow Slice. **2012**, 61, 350-365		10
897	Construction of Codes for the Wiretap Channel and the Secret Key Agreement From Correlated Source Outputs Based on the Hash Property. *IEEE Transactions on Information Theory*, **2012**, 58, 671-692	2.8	30
896	One-Shot Classical Data Compression With Quantum Side Information and the Distillation of Common Randomness or Secret Keys. *IEEE Transactions on Information Theory*, **2012**, 58, 1985-1991	2.8	37
895	Unconditional Security From Noisy Quantum Storage. *IEEE Transactions on Information Theory*, **2012** , 58, 1962-1984	2.8	86
894	Reverse Authentication in Financial Transactions and Identity Management. **2013**, 18, 712-727		2
893	Dual Universality of Hash Functions and Its Applications to Quantum Cryptography. *IEEE Transactions on Information Theory*, **2013**, 59, 4700-4717	2.8	35
892	Information Security and Privacy. **2013**,		
891	Efficient Public Key Cryptosystem Resilient to Key Leakage Chosen Ciphertext Attacks. **2013**, 84-100		25

890	Reflections on the security proofs of Boneh-Franklin identity-based encryption scheme. **2013**, 56, 1385-1401		
889	Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks. **2013**, 62, 1031-1043		18
888	Topics in Cryptology CT-RSA 2013. **2013**,		
887	From Oblivious AES to Efficient and Secure Database Join in the Multiparty Setting. **2013**, 84-101		23
886	On the quantum-mechanical bound on the loss of information through side channels in quantum cryptography. **2013**, 97, 604-610		
885	Experimental quantum key distribution with finite-key security analysis for noisy channels. **2013**, 4, 2363		30
884	On the relationships between perfect nonlinear functions and universal hash families. **2013**, 513, 85-95		3
883	Message transmission and key establishment: General equality for weak and strong capacities. **2013**, 18, 83-95		1
882	STRIP. **2013**,		38
881	A new multi-linear universal hash family. **2013**, 69, 351-367		8
880	Experimental bit commitment based on quantum communication and special relativity. **2013**, 111, 180504		54
879	Compressed matrix multiplication. **2013**, 5, 1-17		34
878	Efficient leakage-resilient public key encryption from DDH assumption. **2013**, 16, 797-806		23
877	Hardware Signature Designs to Deal with Asymmetry in Transactional Data Sets. *IEEE Transactions on Parallel and Distributed Systems*, **2013**, 24, 506-519	3.7	9
876	A Map-Reduce Framework for Clustering Metagenomes. **2013**,		9
875	Simple Tabulation, Fast Expanders, Double Tabulation, and High Independence. **2013**,		12
874	Efficient codes for Limited View adversarial channels. **2013**,		6
873	A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks. *IEEE Transactions on Information Theory*, **2013**, 59, 7693-7710	2.8	133

872	Exponential secrecy against unbounded adversary using joint encryption and privacy amplification. **2013**,		
871	An end-to-end exponentially secure secrecy scheme against an unbounded adversary. **2013**,		1
870	Efficacious applicability of foolproof security and reliable storage services in cloud computing. **2013**,		
869	Format-Preserving Fuzzy Query Mechanism. **2013**,		1
868	On Obfuscating Set-Membership Predicate Functions. **2013**,		
867	Tight Exponential Analysis of Universally Composable Privacy Amplification and Its Applications. *IEEE Transactions on Information Theory*, **2013**, 59, 7728-7746	2.8	42
866	THE PHYSICS OF QUANTUM INFORMATION: COMPLEMENTARITY, UNCERTAINTY, AND ENTANGLEMENT. **2013**, 11, 1330002		3
865	Unique permutation hashing. **2013**, 475, 59-65		1
864	Pseudorandom Generators for Combinatorial Shapes. *SIAM Journal on Computing*, **2013**, 42, 1051-1076	1.1	9
863	Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Physical Review A*, **2013**, 87,	2.6	101
862	Balls and Bins: Smaller Hash Families and Faster Evaluation. *SIAM Journal on Computing*, **2013**, 42, 1030-1050	1.1	11
861	Practical perfect hashing in nearly optimal space. **2013**, 38, 108-131		15
860	MISRs for Fast Authentication of Long Messages. **2013**,		2
859	Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices. **2013**, 31, 1687-1700		54
858	Improving Utilization of Hardware Signatures in Transactional Memory. *IEEE Transactions on Parallel and Distributed Systems*, **2013**, 24, 2230-2239	3.7	5
857	Secure Storage and Fuzzy Query over Encrypted Databases. **2013**, 439-450		4
856	Sparse extractor families for all the entropy. **2013**,		1
855	Leakage-resilient lossy trapdoor functions and public-key encryption. **2013**,		5

854	Network-aware data caching and prefetching for cloud-hosted metadata retrieval. **2013**,	3
853	Decoupling with unitary approximate two-designs. **2013**, 15, 053022	25
852	How to Approximate a Set without Knowing Its Size in Advance. **2013**,	8
851	Low-density random matrices for secret key extraction. **2013**,	2
850	File Deduplication with Cloud Storage File System. **2013**,	3
849	Efficient interactive algorithms for file synchronization under general edits. **2013**,	5
848	Channel code using a constrained Random number generator. **2013**,	1
847	Lossy source code using a constrained random number generator. **2013**,	1
846	LS-Sig: Locality-Sensitive Signatures for Transactional Memory. **2013**, 62, 322-335	7
845	Information Theoretically Secure Key Agreement and Related Topics. **2013**, 7, 38-50	
844	Security for Network Coding. **2013**, 115-146	
843	Bibliography. **2013**, 453-473	
842	References. **2014**, 458-479	
841	Explicit capacity-achieving coding scheme for the Gaussian wiretap channel. **2014**,	19
840	Fast implementation of length-adaptive privacy amplification in quantum key distribution. **2014**, 23, 090310	10
839	A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. **2014**, 16, 013047	59
838	Quantum Hashing via Universal Hashing Constructions and Freivalds Fingerprinting Schemas. **2014**, 42-52	1
837	A trustworthy key generation prototype based on DDR3 PUF for wireless sensor networks. **2014**, 14, 11542-56	10

836	Sparser Johnson-Lindenstrauss Transforms. **2014**, 61, 1-23	82
835	Generating Repudiable, Memorizable, and Privacy Preserving Security Questions Using the Propp Theory of Narrative. **2014**,	2
834	Balanced allocations and double hashing. **2014**,	1
833	Privacy amplification with asymptotically optimal entropy loss. **2014**, 61, 1-28	3
832	Design and Implementation of File Deduplication Framework on HDFS. **2014**, 10, 561340	4
831	Identifying global hot items in distributed dynamic data streams. **2014**,	
830	Embedded content aware router implementation using the Blackfin microcomputer. **2014**,	
829	Selected Areas in Cryptography -- SAC 2014. **2014**,	4
828	An experimental implementation of oblivious transfer in the noisy storage model. **2014**, 5, 3418	31
827	Security of Device-Independent Quantum Key Distribution Protocols. **2014**, 13-22	
826	Variable-length lossy source code using a constrained-random-number generator. **2014**,	
825	Strongly Universal String Hashing is Fast. **2014**, 57, 1624-1638	9
824	A Novel End-to-End Authentication Protocol for Satellite Mobile Communication Networks. **2014**, 755-766	
823	Efficient Authentication for Mobile and Pervasive Computing. **2014**, 13, 469-481	19
822	A New Interactive Hashing Theorem. **2014**, 27, 109-138	1
821	Cache-Oblivious Hashing. **2014**, 69, 864-883	1
820	Modes of operations for encryption and authentication using stream ciphers supporting an initialisation vector. **2014**, 6, 189-231	11
819	Lattice-based certificateless public-key encryption in the standard model. **2014**, 13, 315-333	7

818	Explicit and Efficient Hash Families Suffice for Cuckoo Hashing with a Stash. **2014**, 70, 428-456		14
817	Direct proof of security of Wegman□Carter authentication with partially known key. *Quantum Information Processing*, **2014**, 13, 2155-2170	1.6	9
816	Networks and Communications (NetCom2013). **2014**,		0
815	Channel Coding and Lossy Source Coding Using a Generator of Constrained Random Numbers. *IEEE Transactions on Information Theory*, **2014**, 60, 2667-2686	2.8	15
814	Bloom Filter Based Associative Deletion. *IEEE Transactions on Parallel and Distributed Systems*, **2014** , 25, 1986-1998	3.7	8
813	Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. *Physical Review A*, **2014**, 90,	2.6	44
812	General formula for secrecy capacity of wiretap channel with noncausal state. **2014**,		3
811	KEEP: Fast secret key extraction protocol for D2D communication. **2014**,		24
810	Using quantum key distribution for cryptographic purposes: A survey. **2014**, 560, 62-81		71
809	Delayed error verification in quantum key distribution. **2014**, 59, 2825-2828		43
808	Large Deviation Analysis for Quantum Security via Smoothing of R□yi Entropy of Order 2. *IEEE Transactions on Information Theory*, **2014**, 60, 6702-6732	2.8	15
807	A New Efficient and Secure POR Scheme Based on Network Coding. **2014**,		1
806	Communications and Multimedia Security. **2014**,		2
805	Separation of Reliability and Secrecy in Rate-Limited Secret-Key Generation. *IEEE Transactions on Information Theory*, **2014**, 60, 4941-4957	2.8	26
804	Fast Software Encryption. **2014**,		1
803	Secure Device Pairing: A Survey. **2014**, 16, 17-40		30
802	Asymmetric □4+2□protocol for quantum key distribution with finite resources. *Quantum Information Processing*, **2014**, 13, 5-20	1.6	2
801	A practical protocol for three-party authenticated quantum key distribution. *Quantum Information Processing*, **2014**, 13, 2355-2374	1.6	13

800	Construction of a key-dependent message secure symmetric encryption scheme in the ideal cipher model. **2014**, 8, 469-477		
799	Revisiting iterated attacks in the context of decorrelation theory. **2014**, 6, 279-311		1
798	A Two-Stage Methodology Using K-NN and False-Positive Minimizing ELM for Nominal Data Classification. **2014**, 6, 432-445		26
797	The Spammed Code Offset Method. **2014**, 9, 875-884		11
796	Algorithmen und Datenstrukturen. **2014**,		2
795	Real-time detection of changes in network with OpenFlow based on NetFPGA implementation. **2014**, 38, 431-442		6
794	Handling Data-skew Effects in Join Operations Using MapReduce. *Procedia Computer Science*, **2014**, 29, 145-158	1.6	17
793	The Slepian-Wolf Theorem. **2014**, 7, 227-241		
792	Triangle counting in streamed graphs via small vertex covers. **2014**,		1
791	Secret Key Agreement for Massive MIMO Systems with Two-Way Training under Pilot Contamination Attack. **2015**,		5
790	One-hashing bloom filter. **2015**,		12
789	Analog of differentialphase quantum cryptography on coherent states with provable cryptographic security. **2015**, 102, 396-403		
788	. **2015**,		
787	Practical Relativistic Bit Commitment. **2015**, 115, 030502		28
786	DLS: a cloud-hosted data caching and prefetching service for distributed metadata access. **2015**, 2, 183		4
785	An Elliptic Curve Algorithm for Iris Pattern Recognition. **2015**,		
784	On the security of fiber optic quantum cryptography systems without the control of the intensity of quasi-single-photon coherent states. **2015**, 101, 579-585		6
783	Error Performance Analysis of Asymmetric Slepian-Wolf Coding for Ordered Random Variables. **2015**, E98.A, 992-999		

782	ND-POR: A POR Based on Network Coding and Dispersal Coding. **2015**, E98.D, 1465-1476		2
781	An adaptive algorithm for searching in flow tables of openflow switches. **2015**,		0
780	An Evaluation of Streaming Algorithms for Distinct Counting Over a Sliding Window. **2015**, 2,		1
779	Calculation of key reduction for B92 QKD protocol. **2015**,		3
778	Remote Data Auditing in Cloud Computing Environments. **2015**, 47, 1-34		77
777	Variable-Length Lossy Source Code Using a Constrained-Random-Number Generator. *IEEE Transactions on Information Theory*, **2015**, 61, 3574-3592	2.8	6
776	Identifying Global Icebergs in Distributed Streams. **2015**,		6
775	Hardware implementation of key functionalities of NIPS for high speed network. **2015**,		1
774	Distinct element counting in distributed dynamic data streams. **2015**,		1
773	Efficiently Summarizing Data Streams over Sliding Windows. **2015**,		12
772	Traitor Deterring Schemes. **2015**,		14
771	Hashing for Statistics over K-Partitions. **2015**,		6
770	Message Authentication Code over a wiretap channel. **2015**,		4
769	Boosting distinct random sampling for basic counting on the union of distributed streams. **2015**, 602, 60-79		
768	Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. **2015**, 6, 8795		97
767	CRC-Based Message Authentication for 5G Mobile Technology. **2015**,		12
766	Cryptography and Coding. **2015**,		2
765	More efficient privacy amplification with less random seeds. **2015**,		3

764	Precise Evaluation of Leaked Information with Secure Randomness Extraction in the Presence of Quantum Attacker. **2015**, 333, 335-350		10
763	Parallel Compact Hash Algorithms for Computational Meshes. **2015**, 37, C31-C53		6
762	Pseudorandom generators from regular one-way functions: New constructions with improved parameters. **2015**, 569, 58-69		1
761	Efficient bit sifting scheme of post-processing in quantum key distribution. *Quantum Information Processing*, **2015**, 14, 3785-3811	1.6	4
760	Towards Scalability and Data Skew Handling in GroupBy-Joins using MapReduce Model. *Procedia Computer Science*, **2015**, 51, 70-79	1.6	10
759	Quantum hashing via ?-universal hashing constructions and classical fingerprinting. **2015**, 36, 89-96		7
758	Quantum blind signature with an offline repository. **2015**, 13, 1550016		3
757	Security of quantum key distribution with a laser reference coherent state, resistant to loss in the communication channel. **2015**, 12, 065201		4
756	Bit-string oblivious transfer based on quantum state computational distinguishability. *Physical Review A*, **2015**, 91,	2.6	8
755	Security Bounds for Efficient Decoy-State Quantum Key Distribution. **2015**, 21, 197-204		15
754	Tight Bounds for Sliding Bloom Filters. **2015**, 73, 652-672		8
753	Security Enhancement in Distributed Networks Using Link-Based Mapping Scheme for Network Intrusion Detection with Enhanced Bloom Filter. **2015**, 84, 821-839		3
752	Introduction to Cryptography. **2015**,		18
751	Secret-Key Distribution Based on Bounded Observability. **2015**, 103, 1762-1780		11
750	Quantum Wiretap Channel With Non-Uniform Random Number and Its Exponent and Equivocation Rate of Leaked Information. *IEEE Transactions on Information Theory*, **2015**, 61, 5595-5622	2.8	21
749	STES: A Stream Cipher Based Low Cost Scheme for Securing Stored Data. **2015**, 64, 2691-2707		6
748	Secret Key Agreement With Large Antenna Arrays Under the Pilot Contamination Attack. **2015**, 14, 6579-6594		17
747	Low-Complexity Interactive Algorithms for Synchronization From Deletions, Insertions, and Substitutions. *IEEE Transactions on Information Theory*, **2015**, 61, 5670-5689	2.8	14

746	Path-Quality Monitoring in the Presence of Adversaries: The Secure Sketch Protocols. **2015**, 23, 1729-1741	3
745	On the Size of Source Space in a Secure MAC. **2015**, 10, 2007-2015	2
744	Enhanced dual Bloom filter based on SSD for efficient directory parsing in cloud storage system. **2015**,	2
743	Design and implementation of dynamic key based stream cipher for cryptographic processor. **2015**,	1
742	. **2015**, 103, 1781-1795	25
741	String Processing and Information Retrieval. **2015**,	
740	On the Complexity of Constructing Pseudorandom Functions (Especially when They Don� Exist). **2015**, 28, 509-532	
739	Universally composable three-party password-authenticated key exchange with contributiveness. **2015**, 28, 1100-1111	4
738	On Weak Keys and Forgery Attacks Against Polynomial-Based MAC Schemes. **2015**, 28, 769-795	7
737	A survey on secret key generation mechanisms on the physical layer in wireless networks. **2015**, 8, 332-341	31
736	New Proofs for NMAC and HMAC: Security without Collision Resistance. **2015**, 28, 844-878	24
735	Multi-partite squash operation and its application to device-independent quantum key distribution. **2016**, 18, 103043	
734	Experimental realization of an entanglement access network and secure multi-party computation. **2016**, 6, 29453	14
733	Toward hardware support for a flexible sketch-based network traffic monitoring system. **2016**,	0
732	The smooth entropy formalism for von Neumann algebras. **2016**, 57, 015213	14
731	. **2016**,	7
730	Authenticated encryption: how reordering can impact performance. **2016**, 9, 6173-6188	
729	Bitvectors. 64-102	

728	Linear Hashing Is Awesome. **2016**,		1
727	Racer: TSO consistency via race detection. **2016**,		4
726	Triangle Counting in Dynamic Graph Streams. **2016**, 76, 259-278		10
725	On the Security of Key Extraction From Measuring Physical Quantities. **2016**, 11, 1796-1806		13
724	A joint Shannon cipher and privacy amplification approach to attaining exponentially decaying information leakage. **2016**, 357, 6-22		4
723	Information Security Applications. **2016**,		5
722	A Novel NTT-Based Authentication Scheme for 10-GHz Quantum Key Distribution Systems. **2016**, 1-1		8
721	Concealed data aggregation in wireless sensor networks: A comprehensive survey. **2016**, 103, 207-227		17
720	New techniques and tighter bounds for local computation algorithms. *Journal of Computer and System Sciences*, **2016**, 82, 1180-1200	1	10
719	AG codes, Weierstra□points and universal hashing. **2016**, 431-445		
718	Study on the security of the authentication scheme with key recycling in QKD. *Quantum Information Processing*, **2016**, 15, 3815-3831	1.6	4
717	Role of Quantum Information Theory in Information Theory. **2016**, 10, 4-13		1
716	A hash-based co-clustering algorithm for categorical data. **2016**, 64, 24-35		7
715	Join Sizes, Frequency Moments, and Applications. **2016**, 87-102		1
714	Data Stream Management. **2016**,		51
713	Sketch-guided filtering support for detecting superspreaders in high-speed networks. **2016**, 52, 1459-1461		0
712	Provable Security. **2016**,		
711	Efficient Verifiable Computation of XOR for Biometric Authentication. **2016**, 284-298		6

710	. **2016**,		5
709	Quantum cryptography: Theoretical protocols for quantum key distribution and tests of selected commercial QKD systems in commercial fiber networks. **2016**, 14, 1630002		1
708	MMH? with arbitrary modulus is always almost-universal. **2016**, 116, 481-483		6
707	AMON: An Open Source Architecture for Online Monitoring, Statistical Analysis, and Forensics of Multi-Gigabit Streams. **2016**, 34, 1834-1848		15
706	More Efficient Privacy Amplification With Less Random Seeds via Dual Universal Hash Function. *IEEE Transactions on Information Theory*, **2016**, 62, 2213-2232	2.8	39
705	Post-Quantum Cryptography. **2016**,		8
704	Experimental demonstration of kilometer-range quantum digital signatures. *Physical Review A*, **2016**, 93,	2.6	48
703	Attacks on quantum key distribution protocols that employ non-ITS authentication. *Quantum Information Processing*, **2016**, 15, 327-362	1.6	10
702	Security Analysis of $varepsilon $ -Almost Dual Universal2 Hash Functions: Smoothing of Min Entropy Versus Smoothing of R�yi Entropy of Order 2. *IEEE Transactions on Information Theory*, **2016**, 62, 3451-3476	2.8	17
701	Attacks on practical quantum key distribution systems (and how to prevent them). **2016**, 57, 366-387		36
700	Quantum Collision-Resistance of Non-uniformly Distributed Functions. **2016**, 79-85		4
699	Faster 64-bit universal hashing using carry-less multiplications. **2016**, 6, 171-185		10
698	Decoding of binary quadratic residue codes with hash table. **2016**, 10, 122-130		6
697	Efficient One-Sided Adaptively Secure Computation. **2017**, 30, 321-371		2
696	An FPGA-Based 4 Mbps Secret Key Distillation Engine for Quantum Key Distribution Systems. **2017**, 86, 1-15		11
695	Equivocations, Exponents, and Second-Order Coding Rates Under Various R�yi Information Measures. *IEEE Transactions on Information Theory*, **2017**, 63, 975-1005	2.8	15
694	Regular and almost universal hashing: an efficient implementation. **2017**, 47, 1299-1323		2
693	An Improved Upper Bound for the Universal TSP on the Grid. **2017**,		1

692	Optimal CUR Matrix Decompositions. *SIAM Journal on Computing*, **2017**, 46, 543-589	1.1	21
691	Quantum random number generators. *Reviews of Modern Physics*, **2017**, 89,	40.5	233
690	Universal Secure Multiplex Network Coding With Dependent and Non-Uniform Messages. *IEEE Transactions on Information Theory*, **2017**, 63, 3773-3782	2.8	14
689	Robust ORAM: Enhancing Availability, Confidentiality and Integrity. **2017**,		2
688	Universal Multiparty Data Exchange and Secret Key Agreement. *IEEE Transactions on Information Theory*, **2017**, 63, 4057-4074	2.8	7
687	Optimized Quantization in Zero Leakage Helper Data Systems. **2017**, 12, 1957-1966		5
686	Oblivious transfer based on single-qubit rotations. **2017**, 50, 205301		5
685	Information-theoretic physical layer security for satellite channels. **2017**,		5
684	. **2017**,		2
683	. *IEEE Transactions on Information Theory*, **2017**, 63, 2560-2595	2.8	2
682	A New Look at Counters: Don�Run Like Marathon in a Hundred Meter Race. **2017**, 66, 1851-1864		1
681	Efficiently Correcting Matrix Products. **2017**, 79, 428-443		2
680	Symmetric Blind Information Reconciliation for Quantum Key Distribution. **2017**, 8,		27
679	. *IEEE Transactions on Information Theory*, **2017**, 63, 6819-6826	2.8	7
678	Index Structures for Fast Similarity Search for Binary Vectors. **2017**, 53, 799-820		6
677	Introduction to Quantum Key Distribution. **2017**, 1-17		11
676	Algorithmen und Datenstrukturen. **2017**,		6
675	Packing a Knapsack of Unknown Capacity. **2017**, 31, 1477-1497		8

674	Secure wireless communication under spatial and local Gaussian noise assumptions. **2017**,		6
673	Verifiable Random Functions from Non-interactive Witness-Indistinguishable Proofs. **2017**, 567-594		22
672	Private Set Projections & Variants. **2017**,		3
671	Technical Perspective: Building a better hash function. **2017**, 60, 93-93		12
670	A Group Theoretic Approach to Quantum Information. **2017**,		16
669	Deterministic and Efficient Quantum Key Distribution Using Entanglement Parity Bits and Ancillary Qubits. *IEEE Access*, **2017**, 5, 25565-25575	3.5	2
668	Hashing, Load Balancing and Multiple Choice. **2017**, 12, 275-379		6
667	Two-party function computation on the reconciled data. **2017**,		
666	Robust secure goodput for massive MIMO and optical fiber wiretap channels. **2017**,		2
665	Tighter bounds on entropy of secret keys in authentication codes. **2017**,		1
664	. **2017**,		6
663	. **2017**, 9, 1-8		11
662	BPTree. **2017**,		9
661	. **2017**, 60,		1
660	Literaturverzeichnis. **2017**,		
659	Minimum and Maximum Entropy Distributions for Binary Systems with Known Means and Pairwise Correlations. *Entropy*, **2017**, 19,	2.8	1
658	Efficient Asymmetric Index Encapsulation Scheme for Anonymous Content Centric Networking. **2017**, 2017, 1-9		1
657	Finite-block-length analysis in classical and quantum information theory. **2017**, 93, 99-124		4

656	Abstract Super Points from Core Network by Unique Candidate List. **2017**,		
655	High Speed Network Super Points Detection Based on Sliding Time Window by GPU. **2017**,		1
654	Distributed Scheme to Authenticate Data Storage Security in Cloud Computing. **2017**, 9, 59-66		0
653	A Write-Friendly and Cache-Optimized Hashing Scheme for Non-Volatile Memory Systems. *IEEE Transactions on Parallel and Distributed Systems*, **2018**, 29, 985-998	3.7	12
652	Progress in Cryptology AFRICACRYPT 2018. **2018**,		1
651	Analysis of Remaining Uncertainties and Exponents Under Various Conditional Ryi Entropies. *IEEE Transactions on Information Theory*, **2018**, 64, 3734-3755	2.8	9
650	Sectional MinHash for near-duplicate detection. **2018**, 99, 203-212		10
649	On rate-1 and beyond-the-birthday bound secure online ciphers using tweakable block ciphers. **2018**, 10, 731-753		4
648	Secure uniform random-number extraction via incoherent strategies. *Physical Review A*, **2018**, 97,	2.6	16
647	On the (Im-)Possibility of Extending Coin Toss. **2018**, 31, 1120-1163		
646	Efficient robust secret sharing from expander graphs. **2018**, 10, 79-99		2
645	Efficient Signature Scheme for Delivering Authentic Control Commands in the Smart Grid. **2018**, 9, 4323-4334		17
644	Efficient Detection for Malicious and Random Errors in Additive Encrypted Computation. **2018**, 67, 16-31		6
643	Mathematical Modelling for Next-Generation Cryptography. **2018**,		
642	Uniform Random Number Generation and Secret Key Agreement for General Sources by Using Sparse Matrices. **2018**, 177-198		1
641	Sample(x)=(a*x. *SIAM Journal on Computing*, **2018**, 47, 2510-2526	1.1	
640	A (k, n)-Threshold Progressive Visual Secret Sharing without Expansion. **2018**, 2, 28		1
639	Inverted Leftover Hash Lemma. **2018**,		1

638	Privacy Amplification: Recent Developments and Applications. **2018**,		1
637	CABLE: A CAche-Based Link Encoder for Bandwidth-Starved Manycores. **2018**,		2
636	m-Bonsai: A Practical Compact Dynamic Trie. **2018**, 29, 1257-1278		4
635	Secure Computation-and-Forward Communication with Linear Codes. **2018**,		1
634	Converging Blockchain and Social Business for Socio-Economic Development. **2018**,		8
633	A Write-efficient and Consistent Hashing Scheme for Non-Volatile Memory. **2018**,		3
632	A Reciprocity Approach for Shared Secret Key Generation Extracted from Received Signal Strength in The Wireless Networks. **2018**,		3
631	Enhancing Channel Reciprocity of Secret Key Generation Scheme by Using Modified Polynomial Regression Method. **2018**,		1
630	Venilia, On-line Learning and Prediction of Vessel Destination. **2018**,		2
629	An Implementation of Shared Key Generation Extracted from Received Signal Strength in Vehicular Ad-Hoc Communication. **2018**,		2
628	Secret Sharing over a Public Channel from Correlated Random Variables. **2018**,		8
627	On an Almost-Universal Hash Function Family with Applications to Authentication and Secrecy Codes. **2018**, 29, 357-375		7
626	Towards a Smart Contract-Based, Decentralized, Public-Key Infrastructure. **2018**, 299-321		7
625	A Secure and Efficient Certificateless Authentication Scheme With Unsupervised Anomaly Detection in VANETs. *IEEE Access*, **2018**, 6, 74260-74276	3.5	28
624	Progress in Cryptology □INDOCRYPT 2018. **2018**,		
623	Hierarchical Secret Sharing Schemes Secure Against Rushing Adversary: Cheater Identification and Robustness. **2018**, 578-594		4
622	Low Computational Cost Bloom Filters. **2018**, 26, 2254-2267		4
621	One-step estimation of networked population size: Respondent-driven capture-recapture with anonymity. **2018**, 13, e0195959		4

620	Versatile Cybersecurity. **2018**,		1
619	Cryptographic Program Obfuscation: Practical Solutions and Application-Driven Models. **2018**, 141-167		2
618	Bounded Independence Plus Noise Fools Products. *SIAM Journal on Computing*, **2018**, 47, 493-523	1.1	3
617	Heavy-Hitter Detection Using a Hardware Sketch with the Countmin-CU Algorithm. **2018**,		5
616	Secure Opportunistic Multipath Key Exchange. **2018**,		3
615	Free space optical secret key agreement. **2018**, 26, 23305-23332		8
614	Universal Hashing via Integer Arithmetic Without Primes, Revisited. **2018**, 257-279		2
613	Methods of Big Data Analytics. **2018**, 285-322		
612	Bibliography. **2018**, 387-393		
611	Engine Torque Output Control Using Torque Maps - For Automotive Application. **2018**,		1
610	Measuring the X-MET▯ maximum power: A preliminary study. **2018**,		0
609	Data Streams with Bounded Deletions. **2018**,		4
608	Analysis of Channel-Based User Authentication by Key-Less and Key-Based Approaches. **2018**, 17, 5700-5712		11
607	. *IEEE Transactions on Information Theory*, **2018**, 64, 6054-6069	2.8	1
606	Quantum Key Distribution As a Scheme with Bernoulli Tests. *Journal of Experimental and Theoretical Physics*, **2018**, 126, 741-752	1	6
605	A secret key distribution technique based on semiconductor superlattice chaos devices. **2018**, 63, 1034-1036		7
604	Minimum Circuit Size, Graph Isomorphism, and Related Problems. *SIAM Journal on Computing*, **2018**, 47, 1339-1372	1.1	9
603	Composable security analysis of continuous-variable measurement-device-independent quantum key distribution with squeezed states for coherent attacks. *Physical Review A*, **2018**, 98,	2.6	20

602	Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs. **2018**, 2018, 1-13		25
601	Commitment and Oblivious Transfer in the Bounded Storage Model With Errors. *IEEE Transactions on Information Theory*, **2018**, 64, 5970-5984	2.8	2
600	Hamming Metric Multi-Granularity Locality-Sensitive Bloom Filter. **2018**, 26, 1660-1673		2
599	Continuous-Variable Quantum Key Distribution with Gaussian Modulation□The Theory of Practical Implementations. *Advanced Quantum Technologies*, **2018**, 1, 1800011	4.3	93
598	Bernstein Bound on WCS is Tight. **2018**, 213-238		5
597	On Privacy Amplification, Lossy Compression, and Their Duality to Channel Coding. *IEEE Transactions on Information Theory*, **2018**, 64, 7792-7801	2.8	4
596	Hardness-Preserving Reductions via Cuckoo Hashing. **2019**, 32, 361-392		2
595	Decay-Based DRAM PUFs in Commodity Devices. **2019**, 16, 462-475		21
594	A Feasible FPGA Weightless Neural Accelerator. **2019**,		2
593	Progress in Cryptology □LATINCRYPT 2017. **2019**,		
592	Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. **2019**, 10, 3140		30
591	Improving Parameter Estimation of Entropic Uncertainty Relation in Continuous-Variable Quantum Key Distribution. *Entropy*, **2019**, 21,	2.8	8
590	An Image Authentication Scheme Using Merkle Tree Mechanisms. **2019**, 11, 149		5
589	Secret-Key Generation in Many-to-One Networks: An Integrated Game-Theoretic and Information-Theoretic Approach. *IEEE Transactions on Information Theory*, **2019**, 65, 5144-5159	2.8	6
588	Error Correction by Structural Simplicity: Correcting Samplable Additive Errors. **2019**, 62, 1265-1276		
587	High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution. **2019**, 9, 15733		8
586	Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic. *Entropy*, **2019**, 21, 887	2.8	19
585	Frontiers in Cyber Security. *Communications in Computer and Information Science*, **2019**,	0.3	

584	Analysis of SparseHash: An efficient embedding of set-similarity via sparse projections. **2019**, 128, 93-99		2
583	Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor. *IEEE Access*, **2019**, 7, 151459-151474	3.5	17
582	Sequential and Parallel Algorithms and Data Structures. **2019**,		5
581	Secure D2D Group Authentication Employing Smartphone Sensor Behavior Analysis. **2019**, 11, 969		14
580	On the Practicality of a Smart Contract PKI. **2019**,		8
579	Bounded Independence versus Symmetric Tests. **2019**, 11, 1-27		
578	Secrecy Amplification of Distributed Encrypted Sources With Correlated Keys Using Post-Encryption-Compression. **2019**, 14, 3042-3056		1
577	An Efficient Key Generation for the Internet of Things Based Synchronized Quantization. **2019**, 19,		3
576	Algorithmen und Datenstrukturen. **2019**,		2
575	Efficient quantum-based security protocols for information sharing and data protection in 5G networks. **2019**, 100, 893-906		57
574	Distributed Maximal Independent Set using Small Messages. **2019**, 805-820		11
573	Error correction in quantum cryptography based on artificial neural networks. *Quantum Information Processing*, **2019**, 18, 1	1.6	26
572	Linear Hashing Is Awesome. *SIAM Journal on Computing*, **2019**, 48, 736-741	1.1	
571	High-Speed and Adaptive FPGA-Based Privacy Amplification in Quantum Key Distribution. *IEEE Access*, **2019**, 7, 21482-21490	3.5	9
570	Wiretap Channels: Nonasymptotic Fundamental Limits. *IEEE Transactions on Information Theory*, **2019**, 65, 4069-4093	2.8	37
569	Key Establishment □la Merkle in a Quantum World. **2019**, 32, 601-634		
568	A Simple Secret Key Generation by Using a Combination of Pre-Processing Method with a Multilevel Quantization. *Entropy*, **2019**, 21,	2.8	7
567	Foiling covert channels and malicious classical post-processing units in quantum key distribution. **2019**, 5,		13

566	Implementation and security analysis of practical quantum secure direct communication. *Light: Science and Applications*, **2019**, 8, 22	16.7	117
565	The Joys of Hashing. **2019**,		1
564	L p Samplers and Their Applications. **2019**, 52, 1-31		2
563	Derandomizing Isolation in Space-Bounded Settings. *SIAM Journal on Computing*, **2019**, 48, 979-1021	1.1	1
562	An Implementation of Shared Symmetric Key Generation Extracted from Received Signal Strength in Vehicle to Infrastructure Communication. **2019**,		0
561	A New Radar-Embedded Communication Waveform Based on Singular Value Decomposition. **2019**,		
560	Hazard Perception Training and Assessment of Young Drivers in Mauritius: Investigating the Acceptance of the MauHazard Tool. **2019**,		0
559	Mechatronics Arc Generator for Photovoltaic Arc Fault Detector Testing. **2019**,		1
558	. **2019**,		
557	Modeling of Multidimensional Problems in Nonlinear Heat Conductivity in Non-Divergence Case. **2019**,		1
556	Importance of Modern Educational Technologies in Russian Districts. **2019**,		
555	Energy Demand Assessment for water in the residential sector in Mexico. **2019**,		
554	A Stable Parameter Area Calculation Method for Advanced Auto-tuning of a Feedback Controller. **2019**,		1
553	Low-Dispersive Transition from Circular Metallic to Circular Dielectric Waveguides at W-Band Frequencies. **2019**,		2
552	Continuous-Source Fuzzy Extractors: Source uncertainty and insecurity. **2019**,		2
551	. **2019**,		2
550	Node-Aware Improvements to Allreduce. **2019**,		1
549	The Generation of Random Numbers Using the Quantum Tunnel Effect in Transistors. **2019**,		

548	Networked Yaw Rate Tracking Control of Four-Wheel-Independent-Drive Electric Vehicle in Steering Process. **2019**,	
547	Automatic Generation of Pull Request Descriptions. **2019**,	22
546	. **2019**,	
545	. **2019**,	
544	Staff Listing. **2019**, 14, 2-2	
543	A Cross-Layer CQI Feedback Reduction Technique for MVD Transmission in Crowd Event Scenarios. **2019**,	0
542	A Shared Secret Key Generation between Vehicle and Roadside Based Preprocessing Method. **2019** ,	1
541	A Novel Controllable Image Segmentation Method Using the Inverse GAMMA Distribution Function Based on Histogram Specification. **2019**,	
540	Satellite and Underwater Sonar Image Matching Using Deep Learning. **2019**,	2
539	Comprehensive Quality Control Method and Effect Analysis of Brightness Temperature Data of Ground-based Microwave Radiometer. **2019**,	
538	Fast Factorized Backprojection Imaging Algorithm Integrated With Motion Trajectory Estimation for Bistatic Forward-Looking SAR. **2019**, 12, 3949-3965	15
537	Implementation of Sound Effects on Audio Signals. **2019**,	
536	FPGA-Based Object Detection for Autonomous Driving System. **2019**,	0
535	Blind Visual Motif Removal From a Single Image. **2019**,	5
534	Performance assessment of primary frequency regulation based on static characteristics. **2019**,	
533	Estimation of Disease Code from Electronic Patient Records. **2019**,	5
532	Infrastructure Requirements for Cybersecurity. **2019**,	0
531	Model of Onboard Heterogeneous Data Storage System Functioning with the Consideration of Different Information Importance. **2019**,	

530	Image thresholding segmentation based on oriented genetic algorithm and maximum entropy. **2019**,		
529	A Learning Model to Improve Learning Outcome on Experiential Learning in a Multi-Phase Internship: a Case Study of the Internship Program of a Thai University. **2019**,		0
528	Measurement Investigation on Acoustic Noise Caused by □Ringing□Capacitors on Mobile Devices. **2019**,		5
527	Survey of integrability of procedural modeling techniques for generating a complete city. **2019**,		1
526	. **2019**,		37
525	Can We Overcome the n log n Barrier for Oblivious Sorting?. **2019**, 2419-2438		5
524	Reciprocity Enhancement in V2V Key Generation System by using HPK Method. **2019**,		1
523	Performance Analysis of Addressing Mechanisms in Inter-Operable IoT Device with Low-Power Wake-Up Radio. **2019**, 19,		1
522	Blockchain-based secure and fair crowdsourcing scheme. **2019**, 15, 155014771986489		10
521	On blockchain based secure network coding for mobile small cells. **2019**,		1
520	On the Relationship Between Statistical Zero-Knowledge and Statistical Randomized Encodings. **2019**, 28, 573-616		
519	Transactions on Large-Scale Data- and Knowledge-Centered Systems XL. **2019**,		
518	Channel Code Using Constrained-Random-Number Generator Revisited. *IEEE Transactions on Information Theory*, **2019**, 65, 500-510	2.8	0
517	Using hashing and lexicographic order for Frequent Itemsets Mining on data streams. **2019**, 125, 58-71		8
516	A blockchain based access control framework for the security and privacy of IoT with strong anonymity unlinkability and intractability guarantees. **2019**, 115, 211-258		11
515	Evaluating Bernstein□Rabin□Winograd polynomials. **2019**, 87, 527-546		
514	A parallelizable chaos-based true random number generator based on mobile device cameras for the Android platform. **2019**, 78, 15929-15949		5
513	Analysis of Robin Hood and Other Hashing Algorithms Under the Random Probing Model, With and Without Deletions. **2019**, 28, 600-617		

512	On the feasibility of deriving cryptographic keys from MEMS sensors. **2020**, 10, 67-83		2
511	. **2020**, 17, 1079-1093		25
510	Risk Assessment Approach to Estimate Security of Cryptographic Keys in Quantum Cryptography. **2020**, 114-124		
509	Verifiable Random Functions from Non-interactive Witness-Indistinguishable Proofs. **2020**, 33, 459-493		3
508	Secure Authentication and Key Management With Blockchain in VANETs. *IEEE Access*, **2020**, 8, 2482-2498	3.5	43
507	Data Integrity Threats and Countermeasures in Railway Spot Transmission Systems. **2020**, 4, 1-26		8
506	Four-State Non-malleable Codes with Explicit Constant Rate. **2020**, 33, 1044-1079		1
505	Communication for Generating Correlation: A Unifying Survey. *IEEE Transactions on Information Theory*, **2020**, 66, 5-37	2.8	9
504	Transactions on Large-Scale Data- and Knowledge-Centered Systems XLVI. **2020**,		
503	High-Speed Privacy Amplification Scheme Using GMP in Quantum Key Distribution. **2020**, 12, 1-13		2
502	Independent Forward Progress of Work-groups. **2020**,		2
501	Performance Improvement Based on Modified Lossless Quantization (MLQ) for Secret Key Generation Extracted from Received Signal Strength. **2020**,		0
500	RSS-based Secret Key Establishment using Middle-Point Quantization and Clover Filter Algorithm. **2020**,		
499	Algorithms and Data Structures. **2020**,		1
498	Network Information Theoretic Security. **2020**,		0
497	BlockRobot: Increasing Privacy in Human Robot Interaction by Using Blockchain. **2020**,		2
496	Explicit Construction of Multiple Access Channel Resolvability Codes from Source Resolvability Codes. **2020**,		3
495	Flow-Aware Elephant Flow Detection for Software-Defined Networks. *IEEE Access*, **2020**, 8, 72585-72597	3.5	18

494	Secure Network Code for Adaptive and Active Attacks With No-Randomness in Intermediate Nodes. *IEEE Transactions on Information Theory*, **2020**, 66, 1428-1448	2.8	6
493	PushdownDB: Accelerating a DBMS Using S3 Computation. **2020**,		3
492	Killing Rainbows. **2020**, 40, 5-7		
491	Multiple Private Key Generation for Continuous Memoryless Sources With a Helper. **2020**, 15, 2629-2640		2
490	Artificial intelligence algorithm for optimal time series data model. *IEEE Access*, **2020**, 1-1	3.5	
489	Leftover Hashing From Quantum Error Correction: Unifying the Two Approaches to the Security Proof of Quantum Key Distribution. *IEEE Transactions on Information Theory*, **2020**, 66, 3465-3484	2.8	4
488	A Quantum Multiparty Packing Lemma and the Relay Channel. *IEEE Transactions on Information Theory*, **2020**, 66, 3500-3519	2.8	5
487	ChainLink: Indexing Big Time Series Data For Long Subsequence Matching. **2020**,		4
486	Mining Discriminative K-Mers in DNA Sequences Using Sketches and Hardware Acceleration. *IEEE Access*, **2020**, 8, 114715-114732	3.5	1
485	Toward Practical Quantum Secure Direct Communication: A Quantum-Memory-Free Protocol and Code Design. **2020**, 68, 5778-5792		26
484	Unmanned Aerial Vehicle Communications: Path-Loss Modeling and Evaluation. **2020**, 15, 121-128		5
483	Lightweight Blockchain Consensus Protocols for Vehicular Social Networks. **2020**, 69, 5736-5748		13
482	. *IEEE Access*, **2020**, 8, 8861-8875	3.5	7
481	On Security Against Pollution Attacks in Network Coding Enabled 5G Networks. *IEEE Access*, **2020**, 8, 38416-38437	3.5	8
480	Error Bounds for PD-Controlled Mechanical Systems Under Bounded Disturbances Using Interval Arithmetic. **2020**, 5, 1231-1238		1
479	Randomness Extraction via a Quantum Generalization of the Conditional Collision Entropy. *IEEE Transactions on Information Theory*, **2020**, 66, 1171-1177	2.8	0
478	Distributed Linux Build System for Elbrus Hardware Platform. **2020**,		
477	Implementing a Smart Contract PKI. **2020**, 67, 1425-1443		6

476	Lightweight Authentication for Quantum Key Distribution. *IEEE Transactions on Information Theory*, **2020**, 66, 6354-6368	2.8	8
475	When Are Fuzzy Extractors Possible?. *IEEE Transactions on Information Theory*, **2020**, 66, 5282-5298	2.8	5
474	Linear-time algorithms for phylogenetic tree completion under Robinson-Foulds distance. **2020**, 15, 6		
473	An Improved Controlled-Frequency-Band Impedance Measurement Scheme for Railway Traction Power System. **2021**, 68, 2184-2195		4
472	KEEP: Secure and Efficient Communication for Distributed IoT Devices. **2021**, 8, 12758-12770		1
471	. *IEEE Transactions on Information Theory*, **2021**, 67, 1-9	2.8	0
470	Privacy-Preserving IP Verification. **2021**, 1-1		
469	Designing tweakable enciphering schemes using public permutations. **2021**,		
468	Finite-size security of continuous-variable quantum key distribution with digital signal processing. **2021**, 12, 252		13
467	Privacy in the Cloud: A Survey of Existing Solutions and Research Challenges. *IEEE Access*, **2021**, 9, 10473-10497	3.5	3
466	Elements of Quantum Information Theory. **2021**, 7-33		
465	Quantum Key Distribution. **2021**, 703-784		
464	Digest-based Security Protocol for IoT devices. **2021**, 1748, 042019		
463	Improved Channel Reciprocity for Secure Communication in Next Generation Wireless Systems. **2021**, 67, 2619-2630		1
462	Measurement-device-independent quantum key distribution with leaky sources. **2021**, 11, 1678		6
461	Revisiting Construction of Online Cipher in Hash-ECB-Hash Structure. **2021**, 491-503		
460	BlockHammer: Preventing RowHammer at Low Cost by Blacklisting Rapidly-Accessed DRAM Rows. **2021**,		3
459	An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications. **2021**, 2, 5-22		15

458	Secure Computation-and-Forward With Linear Codes. **2021**, 2, 139-148		1
457	Approximation in (Poly-) Logarithmic Space. **2021**, 83, 2303-2331		1
456	Optimizing the decoy-state BB84 QKD protocol parameters. *Quantum Information Processing*, **2021**, 20, 1	1.6	1
455	Lossless fuzzy extractor enabled secure authentication using low entropy noisy sources. **2021**, 58, 102695		
454	Efficient Distributed Algorithms in the k-machine model via PRAM Simulations. **2021**,		0
453	DOTMIX-Pro: faster and more efficient variants of DOTMIX for dynamic-multithreading platforms. **2022**, 78, 945		1
452	Introducing structure to expedite quantum searching. *Physical Review A*, **2021**, 103,	2.6	2
451	Quantum key distribution with PRF(Hash, Nonce) achieves everlasting security. *Quantum Information Processing*, **2021**, 20, 1	1.6	2
450	Low-Complexity Secret Sharing Schemes Using Correlated Random Variables and Rate-Limited Public Communication. **2021**,		2
449	. **2021**,		1
448	JIZHI: A Fast and Cost-Effective Model-As-A-Service System for Web-Scale Online Inference at Baidu. **2021**,		2
447	Secure two-party input-size reduction: Challenges, solutions and applications. **2021**, 567, 256-277		
446	Cryptanalysis and Improvement in Multi-Party Quantum Key Distribution Protocol with New Bell States Encoding Mode. **2021**, 60, 3599-3608		
445	Measure-resend authenticated semi-quantum key distribution with single photons. *Quantum Information Processing*, **2021**, 20, 1	1.6	1
444	Lower Bounds on OBDD Proofs with Several Orders. **2021**, 22, 1-30		
443	Network Information Theoretic Security with Omnipresent Eavesdropping. *IEEE Transactions on Information Theory*, **2021**, 1-1	2.8	1
442	Semantic Security via Seeded Modular Coding Schemes and Ramanujan Graphs. *IEEE Transactions on Information Theory*, **2021**, 67, 52-80	2.8	4
441	Quantum Key Distribution Protocols. **2021**, 91-116		

440	HalftimeHash: Modern Hashing Without 64-Bit Multipliers or Finite Fields. **2021**, 101-114	
439	Reducing Complexity Assumptions for Statistically-Hiding Commitment. **2005**, 58-77	20
438	An Incremental Heap Canonicalization Algorithm. **2005**, 28-42	18
437	HCTR: A Variable-Input-Length Enciphering Mode. **2005**, 175-188	50
436	Efficient Multi-party Computation with Dispute Control. **2006**, 305-328	52
435	On the (Im-)Possibility of Extending Coin Toss. **2006**, 504-521	10
434	A Tight Bound for EMAC. **2006**, 168-179	13
433	Hardness of Distinguishing the MSB or LSB of Secret Keys in Diffie-Hellman Schemes. **2006**, 240-251	8
432	Provably Secure MACs from Differentially-Uniform Permutations and AES-Based Implementations. **2006**, 226-241	21
431	Redistribution of Mechanical Secret Shares. **2003**, 238-252	1
430	On the Universal Hash Functions in Luby-Rackoff Cipher. **2003**, 226-237	4
429	Structural Properties of One-Way Hash Functions. **1990**, 285-302	7
428	On the Pseudorandomness of Top-Level Schemes of Block Ciphers. **2000**, 289-302	31
427	New Block Cipher DONUT Using Pairwise Perfect Decorrelation. **2000**, 262-270	2
426	CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. **2000**, 197-215	82
425	Almost Independent and Weakly Biased Arrays: Efficient Constructions and Cryptologic Applications. **2000**, 533-543	13
424	Efficient Minimal Perfect Hashing in Nearly Minimal Space. **2001**, 317-326	31
423	New Bounds on the OBDD-Size of Integer Multiplication via Universal Hashing. **2001**, 563-574	8

422	Does Encryption with Redundancy Provide Authenticity?. **2001**, 512-528	15
421	Fast Universal Hashing with Small Keys and No Preprocessing: The PolyR Construction. **2001**, 73-89	17
420	Performance Tuning an Algorithm for Compressing Relational Tables. **2002**, 398-407	2
419	Unconditionally-Secure Oblivious Transfer. **2001**, 35-41	1
418	On the Effectiveness of D-BSP as a Bridging Model of Parallel Computation. **2001**, 579-588	5
417	Counting Distinct Elements in a Data Stream. **2002**, 1-10	107
416	Cryptanalysis of a Pseudorandom Generator Based on Braid Groups. **2002**, 1-13	5
415	A Block-Cipher Mode of Operation for Parallelizable Message Authentication. **2002**, 384-397	120
414	Universal Electronic Cash. **1991**, 324-337	114
413	Universal hashing and authentication codes. **1991**, 74-85	76
412	On the Importance of Memory Resources in the Security of Key Exchange Protocols. **1991**, 11-15	1
411	On the Design of Provably-Secure Cryptographic Hash Functions. **1991**, 412-431	9
410	Practical Approaches to Attaining Security against Adaptively Chosen Ciphertext Attacks. **1992**, 292-304	13
409	On the Existence of Statistically Hiding Bit Commitment Schemes and Fail-Stop Signatures. **1993**, 250-265	40
408	On Families of Hash Functions via Geometric Codes and Concatenation. **1993**, 331-342	60
407	Another Method for Attaining Security Against Adaptively Chosen Ciphertext Attacks. **1993**, 420-434	12
406	Efficient Strongly Universal and Optimally Universal Hashing. **1999**, 262-272	7
405	UMAC: Fast and Secure Message Authentication. **1999**, 216-233	146

404	Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions. **1999**, 252-269	43
403	Hash and Displace: Efficient Evaluation of Minimal Perfect Hash Functions. **1999**, 49-54	10
402	Tracing Traitors. **1994**, 257-270	291
401	Feistel Ciphers with L2-Decorrelation. **1999**, 1-14	12
400	Key Preassigned Traceability Schemes for Broadcast Encryption. **1999**, 144-156	40
399	Computational Alternatives to Random Number Generators. **1999**, 72-80	15
398	Resistance Against General Iterated Attacks. **1999**, 255-271	14
397	Software Performance of Universal Hash Functions. **1999**, 24-41	31
396	Pseudorandom Function Tribe Ensembles Based on One-Way Permutations: Improvements and Applications. **1999**, 432-445	16
395	Secure Hash-and-Sign Signatures Without the Random Oracle. **1999**, 123-139	178
394	Dynamic external hashing with guaranteed single access retrieval. **1989**, 187-201	2
393	Grow and post index trees: Role, techniques and future potential. **1991**, 181-206	8
392	High performance universal hashing, with applications to shared memory simulations. **1992**, 250-269	1
391	The complexity of graph connectivity. **1992**, 112-132	14
390	Sibling intractable function families and their applications. **1993**, 124-138	10
389	Quasilinear time complexity theory. **1994**, 97-108	2
388	Graphs, hypergraphs and hashing. **1994**, 153-165	5
387	Approximation algorithms for multiple sequence alignment. **1994**, 43-53	7

386	New collapse consequences of NP having small circuits. **1995**, 196-207	12
385	Improved probabilistic verification by hash compaction. **1995**, 206-224	46
384	Universal hashing and k-wise independent random variables via integer arithmetic without primes. **1996**, 567-580	16
383	Lower bounds for static dictionaries on RAMs with bit operations but no multiplication. **1996**, 442-453	7
382	Parallelizing the Mur? verifier. **1997**, 256-267	73
381	Trans-dichotomous algorithms without multiplication �some upper and lower bounds. **1997**, 426-439	4
380	Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing. **1996**, 201-215	80
379	Bucket Hashing with a Small Key Size. **1997**, 149-162	14
378	Smooth Entropy and R�yi Entropy. **1997**, 193-208	14
377	Information-Theoretically Secure Secret-Key Agreement by NOT Authenticated Public Discussion. **1997**, 209-225	43
376	Efficient Cryptographic Protocols Based on Noisy Channels. **1997**, 306-317	60
375	Encyclopedia of Algorithms. **2008**, 212-215	3
374	A New Scheme for Memory-Efficient Probabilistic Verification. **1996**, 333-348	21
373	A General-Purpose Shared-Memory Model for Parallel Computation. **1999**, 1-17	5
372	A Survey of Approximation Algorithms for the Permanent. **1990**, 75-91	1
371	High Sets for NP. **1997**, 139-156	4
370	The Strong Secret Key Rate of Discrete Random Triples. **1994**, 271-285	80
369	On the Security of Compressed Encodings. **1984**, 209-230	11

368	Encyclopedia of Algorithms. **2016**, 1662-1664	3
367	Hash-Based Techniques for High-Speed Packet Processing. **2010**, 181-218	34
366	Linear-Time Algorithms for Some Phylogenetic Tree Completion Problems Under Robinson-Foulds Distance. **2018**, 209-226	2
365	Simple and More Efficient PRFs with Tight Security from LWE and Matrix-DDH. **2018**, 490-518	6
364	Tweakable HCTR: A BBB Secure Tweakable Enciphering Scheme. **2018**, 47-69	2
363	Differentially Private Sketches for Jaccard Similarity Estimation. **2020**, 18-32	3
362	Barriers for Succinct Arguments in the Random Oracle Model. **2020**, 47-76	5
361	Authentication Codes and Algebraic Curves. **2001**, 239-244	1
360	A Survey of Hard Core Functions. **2001**, 227-255	9
359	Universal Hash-Function Families: From Hashing to Authentication. **2014**, 459-474	1
358	Triangle Counting in Dynamic Graph Streams. **2014**, 306-318	16
357	Weak-Key and Related-Key Analysis of Hash-Counter-Hash Tweakable Enciphering Schemes. **2015**, 3-19	3
356	Improved Practical Compact Dynamic Tries. **2015**, 324-336	6
355	Shannon Entropy Versus Renyi Entropy from a Cryptographic Viewpoint. **2015**, 257-274	4
354	Tweak-Length Extension for Tweakable Blockciphers. **2015**, 77-93	16
353	Efficient Beyond-Birthday-Bound-Secure Deterministic Authenticated Encryption with Minimal Stretch. **2016**, 317-332	4
352	Efficient Asymmetric Index Encapsulation Scheme for Named Data. **2016**, 191-203	1
351	On Privacy-Preserving Biometric Authentication. **2017**, 169-186	6

350	Efficient Unconditionally Secure Signatures Using Universal Hashing. **2018**, 143-162	3
349	Universal Test for Quantum One-Way Permutations. **2004**, 839-850	1
348	Routing with Improved Communication-Space Trade-Off. **2004**, 305-319	20
347	Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel. **2005**, 47-59	40
346	Approximating Energy Efficient Paths in Wireless Multi-hop Networks. **2003**, 230-241	4
345	A Robust Scheme for Multilevel Extendible Hashing. **2003**, 220-227	5
344	A Linear-Time Majority Tree Algorithm. **2003**, 216-227	22
343	A Concrete Security Analysis for 3GPP-MAC. **2003**, 154-169	6
342	True Random Number Generators Secure in a Changing Environment. **2003**, 166-180	55
341	Constructing Efficient Dictionaries in Close to Sorting Time. **2008**, 84-95	18
340	How to Protect Yourself without Perfect Shredding. **2008**, 511-523	8
339	Composable Security in the Bounded-Quantum-Storage Model. **2008**, 604-615	8
338	Conditional Computational Entropy, or Toward Separating Pseudoentropy from Compressibility. **2007**, 169-186	45
337	Oblivious-Transfer Amplification. **2007**, 555-572	38
336	On-Line Predictive Load Shedding for Network Monitoring. **2007**, 1108-1119	7
335	The Candidate Key Protocol for Generating Secret Shared Keys from Similar Sensor Data Streams. **2007**, 1-15	20
334	A Subliminal-Free Variant of ECDSA. **2006**, 375-387	5
333	Domain Extension of Public Random Functions: Beyond the Birthday Barrier. **2007**, 187-204	23

332	Message Authentication on 64-Bit Architectures. **2006**, 327-341	19
331	Improving the Security of MACs Via Randomized Message Preprocessing. **2007**, 414-433	7
330	New Bounds for PMAC, TMAC, and XCBC. **2007**, 434-451	18
329	FPGA-Based Cuckoo Hashing for Pattern Matching in NIDS/NIPS. **2007**, 334-343	2
328	Fast Evaluation of Union-Intersection Expressions. **2007**, 739-750	6
327	Efficient Helper Data Key Extractor on FPGAs. **2008**, 181-197	107
326	On Notions of Security for Deterministic Encryption, and Efficient Constructions without Random Oracles. **2008**, 335-359	137
325	Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms. **2008**, 144-161	54
324	An Improved Robust Fuzzy Extractor. **2008**, 156-171	13
323	Dynamic Routing and Location Services in Metrics of Low Doubling Dimension. **2008**, 379-393	7
322	Basing PRFs on Constant-Query Weak PRFs: Minimizing Assumptions for Efficient Symmetric Cryptography. **2008**, 161-178	5
321	Security Bounds for Quantum Cryptography with Finite Resources. **2008**, 83-95	14
320	Round Efficient Unconditionally Secure Multiparty Computation Protocol. **2008**, 185-199	5
319	Quantum Cryptography. **2012**, 1521-1543	1
318	Weaknesses of Cuckoo Hashing with a Simple Universal Hash Class: The Case of Large Universes. **2009**, 217-228	2
317	Key Agreement from Close Secrets over Unsecured Channels. **2009**, 206-223	23
316	Counting Flows over Sliding Windows in High Speed Networks. **2009**, 79-91	5
315	Security of Truncated MACs. **2009**, 96-114	4

314	Homomorphic MACs: MAC-Based Integrity for Network Coding. **2009**, 292-305	147
313	Applications of a Splitting Trick. **2009**, 354-365	9
312	Beyond-Birthday-Bound Security Based on Tweakable Block Cipher. **2009**, 308-326	37
311	MAC Reforgeability. **2009**, 345-362	21
310	Fast and Secure CBC-Type MAC Algorithms. **2009**, 375-393	13
309	CDs Have Fingerprints Too. **2009**, 348-362	27
308	Towards True Random Number Generation in Mobile Environments. **2009**, 179-189	13
307	Information Theoretically Secure Multi Party Set Intersection Re-visited. **2009**, 71-91	6
306	Public Key Encryption without Random Oracle Made Truly Practical. **2009**, 107-120	1
305	Entanglement Based Quantum Key Distribution Using a Bright Sagnac Entangled Photon Source. **2010**, 108-116	5
304	Universal Sequencing on a Single Machine. **2010**, 230-243	11
303	How to Thwart Birthday Attacks against MACs via Small Randomness. **2010**, 230-249	18
302	Towards Reliable Remote Healthcare Applications Using Combined Fuzzy Extraction. **2010**, 387-407	3
301	Cryptographic Extraction and Key Derivation: The HKDF Scheme. **2010**, 631-648	132
300	Contributory Password-Authenticated Group Key Exchange with Join Capability. **2011**, 142-160	9
299	Secret Keys from Channel Noise. **2011**, 266-283	5
298	Communication Optimal Multi-valued Asynchronous Byzantine Agreement with Optimal Resilience. **2011**, 206-226	6
297	An Almost-Optimal Forward-Private RFID Mutual Authentication Protocol with Tag Control. **2011**, 69-84	4

296	A Sample of Samplers: A Computational Perspective on Sampling. **2011**, 302-332	13
295	Collision-Free Hashing from Lattice Problems. **2011**, 30-39	6
294	Encyclopedia of Algorithms. **2015**, 1-2	2
293	Analysis of the Initial and Modified Versions of the Candidate 3GPP Integrity Algorithm 128-EIA3. **2012**, 230-242	3
292	A Morphological Analyzer Using Hash Tables in Main Memory (MAHT) and a Lexical Knowledge Base. **2012**, 80-91	1
291	From Non-adaptive to Adaptive Pseudorandom Functions. **2012**, 357-368	10
290	Hardness Preserving Constructions of Pseudorandom Functions. **2012**, 369-382	8
289	Size-Hiding in Private Set Intersection: Existential Results and Constructions. **2012**, 378-394	6
288	Explicit and Efficient Hash Families Suffice for Cuckoo Hashing with a Stash. **2012**, 108-120	5
287	Short-Output Universal Hash Functions and Their Use in Fast and Secure Data Authentication. **2012**, 326-345	7
286	On Security of Universal Hash Function Based Multiple Authentication. **2012**, 303-310	1
285	New Universal Hash Functions. **2012**, 99-108	8
284	Instance-Based Matching of Large Ontologies Using Locality-Sensitive Hashing. **2012**, 49-64	23
283	Quantum Security Analysis via Smoothing of Renyi Entropy of Order 2. **2013**, 128-140	4
282	Overcoming Weak Expectations. **2013**, 1-22	39
281	Hardness Preserving Reductions via Cuckoo Hashing. **2013**, 40-59	9
280	Quantum Key Distribution in the Classical Authenticated Key Exchange Framework. **2013**, 136-154	17
279	A Short Universal Hash Function from Bit Rotation, and Applications to Blockcipher Modes. **2013**, 221-238	10

278	On Weak Keys and Forgery Attacks Against Polynomial-Based MAC Schemes. **2014**, 287-304	20
277	Fast Pseudorandomness for Independence and Load Balancing. **2014**, 859-870	3
276	Cryptography from Compression Functions: The UCE Bridge to the ROM. **2014**, 169-187	9
275	Amplifying Privacy in Privacy Amplification. **2014**, 183-198	8
274	Enhancing Privacy with Quantum Networks. **2014**, 147-153	1
273	Forging Attacks on Two Authenticated Encryption Schemes COBRA and POET. **2014**, 126-140	6
272	Graph-Induced Multilinear Maps from Lattices. **2015**, 498-527	108
271	Pipelineable On-line Encryption. **2015**, 205-223	16
270	On the Minimum Number of Multiplications Necessary for Universal Hash Functions. **2015**, 489-508	8
269	Privacy with Imperfect Randomness. **2015**, 463-482	8
268	Quicksort, Largest Bucket, and Min-Wise Hashing with Limited Independence. **2015**, 828-839	2
267	Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications. **2016**, 514-532	4
266	On the Relationship Between Statistical Zero-Knowledge and Statistical Randomized Encodings. **2016**, 449-477	6
265	Efficient Fuzzy Extraction of PUF-Induced Secrets: Theory and Applications. **2016**, 412-431	36
264	When Are Fuzzy Extractors Possible?. **2016**, 277-306	14
263	DABS-Storm: A Data-Aware Approach for Elastic Stream Processing. **2019**, 58-93	2
262	Linking information reconciliation and privacy amplification. **1995**, 266-274	4
261	The Nature of Computation. **2011**,	142

260	Performance comparison of extendible hashing and linear hashing techniques. **1991**, 17, 19-26	2
259	On the k -Independence Required by Linear Probing and Minwise Independence. **2016**, 12, 1-27	6
258	Weighted Similarity Estimation in Data Streams. **2015**,	4
257	NEMESYS. **2019**,	4
256	Sharp threshold results for computational complexity. **2020**,	2
255	Combinatorial power in multimedia processors. **2003**, 31, 5-11	5
254	Data Structures. **2014**, 1-20	5
253	Finite-key analysis for twin-field quantum key distribution based on generalized operator dominance condition. **2020**, 28, 22594-22605	1
252	Secret Key Agreement by Soft-Decision of Signals in Gaussian Maurer's Model. **2009**, E92-A, 525-534	16
251	Further More on Key Wrapping. **2012**, E95-A, 8-20	2
250	An Efficient Hybrid Cryptographic Scheme for Wireless Sensor Network with Network Coding. **2013** , E96.A, 1889-1894	2
249	A largely self-contained and complete security proof for quantum key distribution. *Quantum - the Open Journal for Quantum Science*, 1, 14	42
248	Theoretical and Experimental Analysis of Cryptographic Hash Functions. **2019**, 1, 125-133	3
247	Quantum cryptography and V A Kotel'nikov's one'time key and sampling theorems. **2006**, 176, 777	3
246	New Developments in Quasigroup-Based Cryptography. 286-317	1
245	A Scalable DDoSDetection Framework with Victim Pinpoint Capability. **2011**, 6,	7
244	An Efficient Data Fingerprint Query Algorithm Based on Two-Leveled Bloom Filter. **2013**, 8,	2
243	A Generic Construction of Fuzzy Signature. **2021**, 23-41	

242	Information-Theoretically Secure String Commitments Based on Packet Reordering Channels. *IEEE Access*, **2021**, 9, 139928-139945	3.5	
241	Novel Non-cryptographic Hash Functions for Networking and Security Applications on FPGA. **2021**,		1
240	Side Channels of Information Leakage in Quantum Cryptography: Nonstrictly Single-Photon States, Different Quantum Efficiencies of Detectors, and Finite Transmitted Sequences. *Journal of Experimental and Theoretical Physics*, **2021**, 133, 272-304	1	1
239	Method for Authentication of Diffie - Hellman Values Based on Pre-Distributed Random Sequences and Wegman - Carter One-Time Pad Algorithm. **2021**, 7, 79-90		
238	Toward an omniopticon: the potential of blockchain technology toward influencing vulnerable populations in contested markets. **2021**, ahead-of-print,		1
237	Intra and inter-flow link aggregation in SDN. 1		1
236	Pseudorandomness. **2000**, 687-704		1
235	On Distribution-Specific Learning with Membership Queries versus Pseudorandom Generation. **2000**, 336-347		
234	A Technique for Boosting the Security of Cryptographic Systems with One-Way Hash Functions. **2000**, 76-81		
233	External Perfect Hashing. **2000**, 187-208		
232	Difference Distribution Attack on DONUT and Improved DONUT. **2001**, 37-48		
231	Efficient Oblivious Transfer in the Bounded-Storage Model. **2002**, 143-159		6
230	Provable Security of 3GPP Integrity Algorithm f9. **2002**, 9C, 573-580		
229	Single-Path Authenticated-Encryption Scheme Based on Universal Hashing. **2003**, 94-109		1
228	Montgomery Prime Hashing for Message Authentication. **2003**, 50-67		
227	Square Hash with a Small Key Size. **2003**, 522-531		2
226	Authentication Codes.		
225	A Construction Method for Optimally Universal Hash Families and Its Consequences for the Existence of RBIBDs. **2004**, 23-32		

224	Thin Client Access to a Visualization Environment. **2004**, 258-263	
223	An Improved Communication-Randomness Tradeoff. **2004**, 444-454	
222	Flow Monitoring in High-Speed Networks with 2D Hash Tables. **2004**, 1093-1097	4
221	Predecessor Queries in Constant Time?. **2005**, 238-248	2
220	Approximate Colored Range Queries. **2005**, 360-369	
219	Unconditionally Secure Information Authentication in Presence of Erasures. **2005**, 304-321	1
218	Bounds on the Efficiency of Black-Box□Commitment Schemes. **2005**, 128-139	5
217	Practical Quantum Cryptography. **2005**, 145-162	
216	New Constructions of Universal Hash Functions Based on Function Sums. **2006**, 416-425	1
215	Non-degrading Erasure-Tolerant Information Authentication with an Application to Multicast Stream Authentication over Lossy Channels. **2006**, 324-338	2
214	Enhancing Network Intrusion Detection with Integrated Sampling and Filtering. **2006**, 272-289	4
213	Unconditionally Secure Authentication in Quantum Key Distribution.	
212	Reducing Complexity Assumptions for Statistically-Hiding Commitment*.	
211	Encyclopedia of Algorithms. **2008**, 682-683	
210	A fast real-time memory authentication protocol. **2008**,	3
209	Reducing Complexity Assumptions for Oblivious Transfer. **2009**, 110-124	
208	On a Construction of Short Digests for Authenticating Ad Hoc Networks. **2009**, 863-876	
207	A Simple, Fast, and Compact Static Dictionary. **2009**, 852-861	

(2011-2009)

206	Secret Key Generation Among Multiple Terminals with Applications to Wireless Systems. **2009**, 231-260	
205	Optimal State Merging without Decoupling. **2009**, 76-84	4
204	Statistically-Hiding Quantum Bit Commitment from Approximable-Preimage-Size Quantum One-Way Function. **2009**, 33-46	6
203	Efficient Oblivious Transfer Protocols Achieving a Non-zero Rate from Any Non-trivial Noisy Correlation. **2009**, 183-194	2
202	Trade-Offs in Information-Theoretic Multi-party One-Way Key Agreement. **2009**, 65-75	4
201	Sketch-Based Anomalies Detection with IP Address Traceability. **2009**, 20, 2899-2906	2
200	Security with Noisy Data. **2010**, 48-50	
199	License Distribution Protocols from Optical Media Fingerprints. **2010**, 201-222	
198	Quantum Key Distribution. **2010**, 23-47	0
197	Preliminaries. **2010**, 3-21	
196	Efficient Password-Based Authenticated Key Exchange Protocol in the UC Framework. **2010**, 144-153	
195	Tweakable Pseudorandom Permutation from Generalized Feistel Structure. **2010**, E93-A, 13-21	
194	Quantum-Resilient Randomness Extraction. **2011**, 52-57	
193	Towards a Universal Sketch for Origin-Destination Network Measurements. **2011**, 201-213	1
192	On the Circuit Complexity of Perfect Hashing. **2011**, 26-29	
191	Encyclopedia of Cryptography and Security. **2011**, 513-514	
190	Security of Hash-then-CBC Key Wrapping Revisited. **2011**, 413-430	
189	Authenticated Encryption. **2011**, 52-61	1

188	Unified Locality-Sensitive Signatures for Transactional Memory. **2011**, 326-337	1
187	When Formulas Freeze: Phase Transitions in Computation. **2011**, 723-818	
186	The Grand Unified Theory of Computation. **2011**, 223-299	
185	Interaction and Pseudorandomness. **2011**, 506-562	
184	Memory, Paths, and Games. **2011**, 300-350	
183	The Deep Question: P vs. NP. **2011**, 173-222	
182	The Basics. **2011**, 15-40	
181	Needles in a Haystack: the Class NP. **2011**, 94-126	
180	Counting, Sampling, and Statistical Physics. **2011**, 651-722	
179	Memory Integrity Protection. **2012**, 305-324	
178	Insights and Algorithms. **2011**, 41-93	
177	Prologue. **2011**, 1-14	
176	Optimization and Approximation. **2011**, 351-449	
175	Quantum Computation. **2011**, 819-910	
174	Randomized Algorithms. **2011**, 450-505	
173	Who is the Hardest One of All? NP-Completeness. **2011**, 127-172	
172	The Stream Cipher Core of the 3GPP Encryption Standard 128-EEA3: Timing Attacks and Countermeasures. **2012**, 269-288	0
171	Resistance against Adaptive Plaintext-Ciphertext Iterated Distinguishers. **2012**, 528-544	1

170	Independence of Tabulation-Based Hash Classes. **2012**, 506-517	2
169	References. 327-336	
168	Count-Min Sketches for Estimating Password Frequency within Hamming Distance Two. **2013**, 388-402	
167	Vertex Deletion for 3D Delaunay Triangulations. **2013**, 253-264	0
166	Message Transmission and Key Establishment: Conditions for Equality of Weak and Strong Capacities. **2013**, 78-94	
165	Pseudorandom Generators from Regular One-Way Functions: New Constructions with Improved Parameters. **2013**, 261-279	4
164	Authentication Codes. **2013**, 155-190	
163	Insider-Proof Encryption with Applications for Quantum Key Distribution. **2014**, 122-141	
162	A Novel Bloom Filter Based Variant of Elliptic Curve Digital Signature Algorithm for Wireless Sensor Networks. **2014**, 125-137	
161	Boosting the basic counting on distributed streams. **2014**,	
160	Security Analysis of Public Key Encryptions Based on Conjugacy Search Problem. **2014**, 554-563	
159	Towards Single Probe Retrieval. **1980**, 389-399	
158	A compendium of key search references. **1990**, 24, 26-42	1
157	Locating P/poly optimally in the extended low hierarchy. **1993**, 28-37	4
156	Performance analysis of superimposing-coded signature files. **1993**, 115-129	
155	Non-interactive generation of shared pseudorandom sequences. **1993**, 385-396	1
154	Simulations between different models of parallel computers. **1993**, 16-30	
153	Information authentication: Hash functions and digital signatures. **1993**, 87-131	3

152	On the Basic Averaging Arguments for Linear Codes. **1994**, 251-261	6
151	On helping and interactive proof systems. **1994**, 137-145	
150	Randomized PRAM simulation using T9000 transputers. **1996**, 736-743	
149	Derandomization via small sample spaces. **1996**, 1-3	
148	Sorting and searching revisted. **1996**, 185-197	3
147	Polynomial time samplable distributions. **1996**, 566-578	1
146	Communication efficient parallel searching. **1997**, 233-254	1
145	MRD Hashing. **1998**, 134-149	1
144	Limits and Possibilities of Sequential Hashing with Supertrace. **1998**, 75-90	
143	Visual Cryptography □How to Use Images to Share a Secret. **1998**, 3-12	
142	The Search for the Holy Grail in Quantum Cryptography. **1999**, 183-216	0
141	Some Practical Randomized Algorithms and Data Structures. **2014**, 1-24	
140	Quantum Error Correction and Quantum Cryptography. **2015**, 231-268	
139	A Novel Distributed Secret Key Extraction Technique for Wireless Network. **2014**, 39A, 708-717	1
138	[illegible]**2015**, 6, 135-151	
137	Encyclopedia of Algorithms. **2015**, 1-5	
136	FORTIFYING SECURITY AND INTEGRITY IN CLOUD. **2015**, 3, 313-316	
135	Cuckoo Hashing. **2016**, 478-481	

134	How Much Randomness Can Be Extracted from Memoryless Shannon Entropy Sources?. **2016**, 75-86		2
133	Entanglement and Locality Restrictions. **2017**, 357-490		
132	Practical Evaluation of Lempel-Ziv-78 and Lempel-Ziv-Welch Tries. **2017**, 191-207		4
131	[illegible] **2017**, 8, 5-40		
130	[illegible] [illegible] **2017**, 8, 117-130		
129	A flexible continuous-variable QKD system using off-the-shelf components. **2017**,		3
128	Ubiquitous Weak-Key Classes of BRW-Polynomial Function. **2018**, 33-50		
127	Most Memory Efficient Distributed Super Points Detection on Core Networks. **2018**, 153-167		
126	Cryptographic Password Obfuscation. **2018**, 497-512		3
125	On the Construction of (n, k)-schemes of Visual Cryptography Using a Class of Linear Hash Functions Over a Binary Field. **2018**, 18, 227-239		0
124	My Genome Belongs to Me: Controlling Third Party Computation on Genomic Data. *Proceedings on Privacy Enhancing Technologies*, **2019**, 2019, 108-132	3.2	4
123	Physical-Layer Security. **2019**, 93-161		
122	Post-Quantum Pseudorandom Functions from Mersenne Primes. *Communications in Computer and Information Science*, **2019**, 128-142	0.3	
121	Fast Locality-Sensitive Hashing Frameworks for Approximate Near Neighbor Search. **2019**, 3-17		5
120	Parallelizable MACs Based on the Sum of PRPs with Security Beyond the Birthday Bound. **2019**, 131-151		4
119	Improved XKX-Based AEAD Scheme: Removing the Birthday Terms. **2019**, 228-246		2
118	Fast Identification of Heavy Hitters by Cached and Packed Group Testing. **2019**, 241-257		
117	Dual Hashing-Based Algorithms for Discrete Integration. **2019**, 161-176		1

116	Hardware Based Cyber System Using High Performance Crypto Hash Bloom Filter for Network Security and Privacy Preserving Applications. **2020**, 39-59	
115	Computationally efficient index generation unit using a Bloom filter. **2019**,	
114	Basic Techniques for Data Security. **2020**, 11-27	
113	Quantum Encryption with Certified Deletion. **2020**, 92-122	7
112	Fast hashing with strong concentration bounds. **2020**,	
111	Nearly optimal static Las Vegas succinct dictionary. **2020**,	0
110	PRACTICAL UMAC ALGORITHM ON HYBRID CRYPTO-CODE CONSTRUCTIONS OF McELISE ON SHORTENED MEC. **2020**, 4, 106-115	
109	Safest Secure and Consistent Data Services in the Storage of Cloud Computing. **2020**, 433-447	0
108	The circulant hash revisited. **2020**, 15, 250-257	
107	A Key-Agreement Scheme for Cyber-Physical Systems. **2021**, 1-6	
106	A blockchain-based integrated document management framework for construction applications. **2022**, 133, 104001	11
105	A Lattice-Based Certificateless Public Key Encryption with Equality Test in Standard Model. **2020**, 50-65	
104	Unprovability of Leakage-Resilient Cryptography Beyond the Information-Theoretic Limit. **2020**, 621-642	
103	Load-Aware Shedding in Stream Processing Systems. **2020**, 121-153	0
102	Towards Closing the Security Gap of Tweak-aNd-Tweak (TNT). **2020**, 567-597	1
101	Super-Linear Time-Memory Trade-Offs for Symmetric Encryption. **2020**, 335-365	3
100	Enabling Efficient Multi-keyword Search Over Fine-Grained Authorized Healthcare Blockchain System. **2020**, 27-41	3
99	Quantum Key Distribution Networks. 61-96	

98	Randomized Algorithms and Complexity Classes. **2005**, 261-310		
97	Other Public-Key Cryptosystems and Protocols. **2005**, 361-412		
96	A Construction for One Way Hash Functions and Pseudorandom Bit Generators. **1991**, 431-445		1
95	Local Randomness in Candidate One-Way Functions. **1992**, 408-419		
94	Parallel Processing of Group-By Join Queries on Shared Nothing Machines. *Communications in Computer and Information Science*, **2008**, 230-241	0.3	
93	Two Improved Range-Efficient Algorithms for F0 Estimation. **2007**, 659-669		0
92	On Optimal Probabilistic Asynchronous Byzantine Agreement. **2007**, 86-98		
91	High-speed implementation of privacy amplification for continuous-variable quantum key distribution. **2020**,		0
90	A Simple Quantum Statistical Interpretation of the Key Secrecy Criterion in Quantum Cryptography. *Journal of Experimental and Theoretical Physics*, **2020**, 131, 394-409	1	
89	Equivalence of Three Classical Algorithms With Quantum Side Information: Privacy Amplification, Error Correction, and Data Compression. *IEEE Transactions on Information Theory*, **2021**, 1-1	2.8	0
88	Bespoke Cache Enclaves: Fine-Grained and Scalable Isolation from Cache Side-Channels via Flexible Set-Partitioning. **2021**,		1
87	Are van Emde Boas trees viable on the GPU?. **2021**,		
86	A Modular Quantum Key Distribution Software Stack for Rapid Experimental Prototyping. **2021**,		0
85	Differential properties of authenticated encryption mode based on universal hash function (XTSMAC). **2021**,		
84	. **2021**,		
83	. **2021**,		0
82	Privacy-preserving FairSwap: Fairness and privacy interplay. *Proceedings on Privacy Enhancing Technologies*, **2022**, 2022, 417-439	3.2	0
81	Differentially Private Sparse Vectors with Low Error, Optimal Space, and Fast Access. **2021**,		0

80	Private Classical Communication over Quantum Multiple-Access Channels. *IEEE Transactions on Information Theory*, **2021**, 1-1	2.8	2
79	Long-term secure distributed storage using quantum key distribution network with third-party verification. *IEEE Transactions on Quantum Engineering*, **2021**, 1-1	2.9	0
78	Quantum Speedup for Graph Sparsification, Cut Approximation and Laplacian Solving. **2020**,		1
77	An Improved Secure Router Discovery Mechanism to Prevent Fake RA Attack in Link Local IPv6 Network. *Communications in Computer and Information Science*, **2021**, 248-276	0.3	
76	Design of Short Blocklength Wiretap Channel Codes: Deep Learning and Cryptography Working Hand in Hand. **2021**,		1
75	On Commitment over General Compound Channels. **2022**,		
74	Three-wise independent random walks can be slightly unbounded. *Random Structures and Algorithms*,	0.8	
73	Digital Signatures with Quantum Candies.. *Entropy*, **2022**, 24,	2.8	
72	Memory-Saving and High-Speed Privacy Amplification Algorithm Using LFSR-Based Hash Function for Key Generation. *Electronics (Switzerland)*, **2022**, 11, 377	2.6	1
71	Multiple Access Channel Resolvability Codes from Source Resolvability Codes. *IEEE Transactions on Information Theory*, **2022**, 1-1	2.8	
70	Secure list decoding and its application to bit-string commitment. *IEEE Transactions on Information Theory*, **2022**, 1-1	2.8	0
69	A Food anti-counterfeiting traceability system based on Blockchain and Internet of Things. *Procedia Computer Science*, **2022**, 199, 629-636	1.6	3
68	Quantum-Inspired Secure Wireless Communication Protocol Under Spatial and Local Gaussian Noise Assumptions. *IEEE Access*, **2022**, 10, 29040-29068	3.5	0
67	DHash: Dynamic Hash Tables with Non-blocking Regular Operations. *IEEE Transactions on Parallel and Distributed Systems*, **2022**, 1-1	3.7	
66	Authentication of variable length messages in quantum key distribution.. *EPJ Quantum Technology*, **2022**, 9, 8	6.9	2
65	Bounds on semi-device-independent quantum random-number expansion capabilities. *Physical Review A*, **2022**, 105,	2.6	0
64	Quantum key distribution using universal hash functions over finite fields. *Quantum Information Processing*, **2022**, 21, 1	1.6	
63	Device-independent secret key rates via a postselected Bell inequality. *Physical Review A*, **2022**, 105,	2.6	

62	The Pursuit of Uniqueness: Extending Valiant-Vazirani Theorem to the Probabilistic and Quantum Settings. *Quantum - the Open Journal for Quantum Science*, 6, 668		0
61	A write-optimal and concurrent persistent dynamic hashing with radix tree assistance. *Journal of Systems Architecture*, **2022**, 125, 102462	5.5	0
60	Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states.. *Light: Science and Applications*, **2022**, 11, 83	16.7	7
59	Binary Fuse Filters: Fast and Smaller Than Xor Filters. *Journal of Experimental Algorithmics*, **2022**, 27, 1-15	1.1	0
58	Secure Physical Layer Network Coding versus Secure Network Coding.. *Entropy*, **2021**, 24,	2.8	1
57	Position-based Hash Embeddings For Scaling Graph Neural Networks. **2021**,		0
56	RUDBA: Reusable User-Device Biometric Authentication Scheme for Multi-service Systems. **2021**,		
55	Quantum Communication Using Semiconductor Quantum Dots. *Advanced Quantum Technologies*, 2100116	4.3	9
54	Optimum ratio between two bases in the Bennett-Brassard 1984 protocol with second-order analysis. *Physical Review A*, **2022**, 105,	2.6	
53	Nearly Optimal Static Las Vegas Succinct Dictionary. *SIAM Journal on Computing*, STOC20-174-STOC20-249	1.1	
52	A scalable architecture for reprioritizing ordered parallelism. **2022**,		
51	Physical-Layer Security for Wireless and Optical Channels. **2022**, 713-760		0
50	Approximate Range Thresholding. **2022**,		
49	LARP: A Lightweight Auto-Refreshing Pseudonym Protocol for V2X. **2022**,		
48	A Modified Key Sifting Scheme With Artificial Neural Network Based Key Reconciliation Analysis in Quantum Cryptography. *IEEE Access*, **2022**, 10, 72743-72757	3.5	0
47	Security in quantum cryptography. *Reviews of Modern Physics*, **2022**, 94,	40.5	4
46	Secure random number generation from parity symmetric radiations. *Communications Physics*, **2022** , 5,	5.4	
45	SEMIGROUPS OF BINARY OPERATIONS AND MAGMA-BASED CRYPTOGRAPHY. *Vestnik of Samara University Natural Science Series*, **2020**, 26, 23-51	0.4	0

44	Secret Key-based Authentication With Passive Eavesdropper for Scalar Gaussian Sources. **2022**,	0
43	High-Speed Privacy Amplification Algorithm Using Cellular Automate in Quantum Key Distribution. **2022**, 11, 2426	1
42	Embedding Compression with Hashing for Efficient Representation Learning in Large-Scale Graph. **2022**,	
41	Quantum key distribution. **2022**, 215-272	0
40	Privacy-Preserving Record Linkage Using Local Sensitive Hash and´Private Set Intersection. **2022**, 398-424	0
39	Review of the k-Vector and Its Relation to Classical Data Structures. 1-7	0
38	Unconditionally secure digital signatures implemented in an eight-user quantum network*. **2022**, 24, 093038	0
37	Privacy Amplification Strategies in Sequential Secret Key Distillation Protocols Based on Machine Learning. **2022**, 14, 2028	1
36	Quantum network security dependent on connection density between trusted nodes.	0
35	Large-Scale and High-Speed FPGA-Based Privacy Amplification for Quantum Key Distribution. **2022**, 1-8	1
34	The Complexity of´the´Co-occurrence Problem. **2022**, 38-52	0
33	SoftSpokenOT: Quieter OT Extension from Small-Field Silent VOLE in´the´Minicrypt Model. **2022**, 657-687	0
32	Improving binary diffing speed and accuracy using community detection and locality-sensitive hashing: an empirical study.	0
31	Algorithms and data structures for hyperedge queries.	0
30	Explicit Wiretap Channel Codes via Source Coding, Universal Hashing, and Distribution Approximation, When the Channels□Statistics are Uncertain. **2022**, 1-1	1
29	Tight Exponential Analysis for Smoothing the Max-Relative Entropy and for Quantum Privacy Amplification. **2022**, 1-1	0
28	Commitment over Multiple-Access Channels. **2022**,	0
27	Twin-Field Quantum Key Distribution with Partial Phase Postselection. **2022**, 18,	0

(2023-2022)

26	Private Randomness Agreement and its Application in Quantum Key Distribution Networks. **2022**, 1-1	0
25	A Framework for Fault Tolerance in RISC-V. **2022**,	0
24	VEA: An FPGA-Based Voxel Encoding Accelerator for 3D Object Detection with LiDAR. **2022**,	0
23	Unconditional Proofs-of-Work and Other Possibilities of Thermodynamic Cryptography. **2022**,	0
22	Commitment over Unreliable Noisy Channels: When Awareness Meets Control. **2022**,	0
21	Quantum Speedup for Graph Sparsification, Cut Approximation, and Laplacian Solving. **2022**, 51, 1703-1742	0
20	Mathematical Tools. **2011**, 911-943	0
19	Copyright Page. **2011**, iv-iv	0
18	Figure Credits. **2011**, xii-xiv	0
17	Dedication. **2011**, v-v	0
16	Preface. **2011**, xv-xvii	0
15	QKD parameter estimation by two-universal hashing. 7, 894	0
14	Short Blocklength Wiretap Channel Codes via Deep Learning: Design and Performance Evaluation. **2023**, 1-1	0
13	Relaxed Locally Decodable and Correctable Codes: Beyond Tensoring. **2022**,	0
12	Linear Hashing with □guarantees and two-sided Kakeya bounds. **2022**,	0
11	MSLCFinder: An Algorithm in Limited Resources Environment for Finding Top-k Elephant Flows. **2023**, 13, 575	0
10	No Repetition. **2022**, 15, 3989-4001	0
9	Executing Efficient Retrieval Over´Blockchain Medical Data Based on´Exponential Skip Bloom Filter. **2023**, 334-348	0

8	Provably Secure Randomness Generation from Switching Probability of Magnetic Tunnel Junctions. **2023**, 19,	0
7	Optimized algorithms and architectures for fast non-cryptographic hash functions in hardware. **2023**, 98, 104782	0
6	Weightless Neural Networks for Efficient Edge Inference. **2022**,	0
5	Quantum Key Distribution with Continuous-Variable Systems. **2023**, 33-102	0
4	CoDi$: Randomized Caches Through Confusion and Diffusion. **2023**, 11, 17265-17282	0
3	Security of device-independent quantum key distribution protocols: a review. 7, 932	0
2	Counterfeit Protection In Supplychain Using Blockchain: A Review. **2023**,	0
1	Optimal Bounds for Noisy Sorting. **2023**,	0