A method for obtaining digital signatures and public-key cryptosystems

DOI: 10.1145/359340.359342
Communications of the ACM, 1978, 21, 120-126.

#	Paper	IF	Citations
2293	IEEE Standard for Identity-Based Cryptographic Techniques using Pairings.		1
2292	Research on secure scheme of smart card application system.		
2291	.		
2290	Two fast RSA implementations using high-radix montgomery algorithm.		2
2289	Atomic broadcast in a real-time environment. **1990**, 51-71		4
2288	Bibliography. 278-286		
2287	Fast algorithms for common-multiplicand multiplication and exponentiation by performing complements.		3
2286	Achieving user privacy in mobile networks.		11
2285	WEDDS: the WITS encrypted data delivery system.		3
2284	An investigation into the design of energy-efficient session negotiation protocols for wireless networks.		
2283	A practical version of Wong's watermarking technique.		1
2282	On the security of joint signature and hybrid encryption.		1
2281	Applying coloured Petri nets to analyze fail silent nodes in distributed systems.		
2280	Logging and signing document-transfers on the WWW-a trusted third party gateway.		0
2279	The Dielectric Behaviour of Magnesium Manganese Ferrite. **1958**, 71, 131-133		18
2278	The implementation of reliable distributed multiprocess systems. **1978**, 2, 95-114		54
2277	Hiding information and signatures in trapdoor knapsacks. **1978**, 24, 525-530		365

2276	Using encryption for authentication in large networks of computers. *Communications of the ACM*, **1978**, 21, 993-999	2.5	1372
2275	Operating Systems Principles for Data Flow Networks. **1978**, 11, 86-96		7
2274	The use of public key cryptography in communication system design. **1978**, 16, 20-23		8
2273	Recent progress in secure computation.		2
2272	Some Open Problems In Cryptography. **1978**,		
2271	Secure communications over insecure channels. *Communications of the ACM*, **1978**, 21, 294-299	2.5	364
2270	On digital signatures. **1978**, 12, 12-14		15
2269	Privacy and security in transnational data processing systems. **1979**,		
2268	. **1979**,		911
2267	Data Security. **1979**, 11, 227-249		95
2266	Cryptology in Transition. **1979**, 11, 285-303		48
2265	Secure personal computing in an insecure network. *Communications of the ACM*, **1979**, 22, 476-482	2.5	12
2264	WFS a simple shared file system for a distributed environment. **1979**,		23
2263	An Efficient One-Way Enciphering Algorithm. **1979**, 5, 97-107		1
2262	Encryption and Secure Computer Networks. **1979**, 11, 331-356		66
2261	Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages. **1979**, 5, 169-178		31
2260	Digital signatures An overview. **1979**, 3, 87-94		6
2259	A note on the complexity of cryptography (Corresp.). **1979**, 25, 232-233		40

2258	Structured Design of Substitution-Permutation Encryption Networks. **1979**, C-28, 747-753		94
2257	Secure information storage and retrieval using new results in cryptography. **1979**, 8, 181-186		0
2256	Cryptology: The Mathematics of Secure Communication. **1979**, 1, 233-249		15
2255	Critical remarks on Critical Remarks on Some Public-Key Cryptosystems by T. Herlestam. **1979**, 19, 274-275		11
2254	Some remarks concerning the M.I.T. public-key cryptosystem. **1979**, 19, 525-538		26
2253	Special Feature An Introduction to Algorithm Design. **1979**, 12, 66-78		5
2252	Uniform Bounds for a Class of Algebraic Mappings. **1979**, 8, 348-356		3
2251	Symmetric and Asymmetric Encryption. **1979**, 11, 305-330		98
2250	How to share a secret. *Communications of the ACM*, **1979**, 22, 612-613	2.5	7167
2249	Microprocessors And Data Encryption. **1979**,		2
2248	On some developments in cryptography and their applications to computer science. **1979**, 121-130		
2247	Relativized cryptography. **1979**,		16
2246	Succinct certificates for the solvability of binary quadratic Diophantine equations. **1979**,		7
2245	A subexponential algorithm for the discrete logarithm problem with applications to cryptography. **1979**,		79
2244	Privacy and authentication: An introduction to cryptography. **1979**, 67, 397-427		225
2243	Computational complexity of decision problems in elementary number theory. **1980**, 211-227		1
2242	Cryptographic techniques for satellite networks. **1980**,		
2241	An improved Monte Carlo factorization algorithm. **1980**, 20, 176-184		114

2240	Worst-case complexity bounds for algorithms in the theory of integral quadratic forms. **1980**, 1, 142-186		54
2239	A progress report on information privacy and data security. **1980**, 31, 75-83		5
2238	Buck's prime number coding scheme. **1980**, 31, 219-220		1
2237	A cryptographic system based on finite field transforms. **1980**, 89, 75-93		
2236	A note on a signature system based on probabilistic logic. **1980**, 11, 110-113		3
2235	A cryptosystem for multiple communication. **1980**, 10, 180-183		7
2234	A trapdoor multiple mapping (Corresp.). **1980**, 26, 100-102		2
2233	Deliberate noise in a modern cryptographic system (Corresp.). **1980**, 26, 102-104		6
2232	A modification of the RSA public-key encryption procedure (Corresp.). **1980**, 26, 726-729		148
2231	Reaching Agreement in the Presence of Faults. **1980**, 27, 228-234		1260
2230	Secure Communications in the Presence of Pervasive Deceit. **1980**,		1
2229	Technical correspondence. *Communications of the ACM*, **1980**, 23, 35-40	2.5	
2228	Recent trends in cryptology. **1980**, 26, 162		
2227	A time-luck tradeoff in cryptography. **1980**,		0
2226	On distinguishing prime numbers from composite numbers. **1980**,		16
2225	On the generation of cryptographically strong pseudo-random sequences. **1981**, 544-550		29
2224	Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, **1981**, 24, 84-90	2.5	2486
2223	Integrating the Data Encryption Standard into Computer Networks. **1981**, 29, 762-772		8

2222	Security Requirements and Protocols for a Broadcast Scenario. **1981**, 29, 778-786	9
2221	Cryptographic Authentication of Time-Invariant Quantities. **1981**, 29, 773-777	63
2220	Space-bounded probabilistic turing machine complexity classes are closed under complement (Preliminary Version). **1981**,	10
2219	Recent directions in algorithmic research. **1981**, 123-134	6
2218	Some cryptographic principles of authentication in electronic funds transfer systems. **1981**, 11, 73-88	1
2217	Digital signature schemes for computer communication networks. **1981**, 11, 37-41	4
2216	An efficient algorithm for constructing a cryptosystem which is harder to break than two other cryptosystems. **1981**, 7, 447-450	17
2215	Uniform complexity and digital signatures. **1981**, 16, 99-110	4
2214	A user authentication scheme for shared data based on a trap-door one-way function. **1981**, 12, 63-67	5
2213	Recent developments in primality testing. **1981**, 3, 97-105	53
2212	Asymptotically fast factorization of integers. **1981**, 36, 255-255	63
2211	On the security of public key protocols. **1981**,	229
2210	A database encryption system with subkeys. **1981**, 6, 312-328	89
2209	Network Protocols. **1981**, 13, 453-489	60
2208	Protocols for secure computations. **1982**,	1673
2207	The implementation of a cryptography-based secure office system. **1982**,	2
2206	Why and how to establish a private code on a public network. **1982**,	37
2205	Digital Signitures with Blindfolded Arbitrators Who Cannot Form Alliances. **1982**,	3

2204	On a quantitative definition of information and its impact on the field of communications. **1982**, 45, 1213-1260		1
2203	Cryptographic sealing for information secrecy and authentication. *Communications of the ACM*, **1982**, 25, 274-286	2.5	19
2202	Cryptographic protocols. **1982**,		54
2201	Comment: Extension of RSA crypto-structure: a Galois approach. **1982**, 18, 582		2
2200	A Monte Carlo factoring algorithm with finite storage. **1982**, 19-33		
2199	A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. **1982**,		69
2198	The Byzantine Generals Problem. **1982**, 4, 382-401		2871
2197	How to generate cryptographically strong sequences of pseudo random bits. **1982**,		103
2196	. **1982**,		5
2195	. **1982**, AES-18, 318-322		
2194	Theory and application of trapdoor functions. **1982**,		698
2193	Polynomfunktionen auf primen Restklassen. **1982**, 39, 431-435		3
2192	Ber die mathematischen Grundlagen einiger Chiffrierverfahren. **1982**, 29, 277-287		1
2191	Cryptography old and new. **1982**, 1, 177-186		1
2190	The public cryptography study group. **1982**, 1, 249-254		
2189	Applying public key distribution to local area networks. **1982**, 1, 268-274		1
2188	A conference key distribution system. **1982**, 28, 714-720		307
2187	On the security of ping-pong protocols. **1982**, 55, 57-68		59

2186	The influence of computers in the development of number theory. **1982**, 8, 75-93	12
2185	Cryptography and teleinformatics. **1982**, 1, 27-33	
2184	A tutorial on public key cryptography. **1982**, 1, 72-79	1
2183	Integrity and security standards based on cryptography. **1982**, 1, 255-260	2
2182	Refined analysis and improvements on some factoring algorithms. **1982**, 3, 101-127	14
2181	Mathematics: High-speed tests for primes. **1983**, 302, 661-661	
2180	On the security of public key protocols. **1983**, 29, 198-208	2508
2179	A Computer Algorithm for Calculating the Product AB Modulo M. **1983**, C-32, 497-500	92
2178	Trapdoor knapsacks without superincreasing structure. **1983**, 17, 7-11	3
2177	Ein Effizienzvergleich der Faktorisierungsverfahren von Morrison-Brillhart und Schroeppel. **1983**, 30, 91-110	2
2176	Exponentiation modulo a polynomial for data security. **1983**, 12, 337-346	2
2175	The NP-completeness column: An ongoing guide. **1983**, 4, 87-100	9
2174	Transaction protection by beacons. **1983**, 27, 256-267	82
2173	On the security of multi-party ping-pong protocols. **1983**,	54
2172	Randomized byzantine generals. **1983**,	202
2171	Cryptographic solution to a problem of access control in a hierarchy. **1983**, 1, 239-248	344
2170	Coin flipping by telephone a protocol for solving impossible problems. **1983**, 15, 23-27	172
2169	The consensus problem in unreliable distributed systems (a brief survey). **1983**, 127-140	89

2168 Authenticated Algorithms for Byzantine Agreement. **1983**, 12, 656-666 269

2167 Digital signatures: A tutorial survey. **1983**, 16, 15-24 26

2166 Protecting Public Keys and Signature Keys. **1983**, 16, 27-35 16

2165 Protocols for Data Security. **1983**, 16, 39-51 25

2164 Applying the RSA Digital Signature to Electronic Mail. **1983**, 16, 55-62 19

2163 A Microprocessor-based Cryptoprocessor. **1983**, 3, 5-15 2

2162 Security Mechanisms in High-Level Network Protocols. **1983**, 15, 135-171 157

2161 How to exchange (secret) keys. **1983**, 18

2160 How to exchange (secret) keys. **1983**, 1, 175-193 121

2159 On the generation of cryptographically strong pseudorandom sequences. **1983**, 1, 38-44 137

2158 Algorithms for Public Key Cryptosystems: Theory and Application. **1983**, 22, 45-108 2

2157 Network security considerations in BLN. **1983**, 13, 124-127

2156 John R. Pasta, 1918-1981-An Unusual Path Toward Computer Science. **1983**, 5, 224-238 4

2155 An overview of computational complexity. *Communications of the ACM*, **1983**, 26, 400-408 2.5 82

2154 An optimally secure relativized cryptosystem. **1983**, 15, 28-33 1

2153 Overview of analogue signal encryption. **1983**, 130, 399 5

2152 Factorization and Primality Tests. **1984**, 91, 333-352 21

2151 Proof Checking The RSA Public Key Encryption Algorithm. **1984**, 91, 181-189 20

2150	The Computation of Catalan Numbers. **1984**, 57, 195-208		2
2149	How to expose an eavesdropper. *Communications of the ACM*, **1984**, 27, 393-394	2.5	81
2148	Digital signatures with RSA and other public-key cryptosystems. *Communications of the ACM*, **1984**, 27, 388-392	2.5	55
2147	Applied Abstract Algebra. **1984**,		24
2146	The Prisoners□Problem and the Subliminal Channel. **1984**, 51-67		328
2145	A Mechanical Proof of the Unsolvability of the Halting Problem. **1984**, 31, 441-458		25
2144	Contemporary evolution in cryptographic techniques. **1984**, 15, 191-196		
2143	Data encryption protocols for electronic mail. **1984**,		
2142	On the concealability of messages by the williams public-key encryption scheme. **1984**, 10, 15-24		1
2141	Protection and resource control in distributed operating systems. **1984**, 8, 421-432		6
2140	A note on the mathematics of public-key cryptosystems. **1984**, 3, 45-47		1
2139	Probabilistic encryption. **1984**, 28, 270-299		2119
2138	. **1984**, 30, 694-694		
2137	Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme. **1984**, 30, 594-601		21
2136	A polynomial-time algorithm for breaking the basic Merkle - Hellman cryptosystem. **1984**, 30, 699-704		81
2135	Computing Logarithms in Finite Fields of Characteristic Two. **1984**, 5, 276-285		40
2134	How to Generate Cryptographically Strong Sequences of Pseudorandom Bits. **1984**, 13, 850-864		770
2133	Flipping Coins In Many Pockets (Byzantine Agreement On Uniformly Random Values).		7

2132 RSA/Rabin Bits are 1/2 + 1 / Poly (Log N) Secure. **1984**, 14

2131 Complexity Measures For Public-Key Cryptosystems. 13

2130 How To Construct Randolli Functions. 25

2129 A "Paradoxical" Solution To The Signature Problem. **1984**, 36

2128 An interview with Richard Roe. **1984**, 2, 97-104

2127 . **1984**, 2, 460-466 4

2126 An extended-precision operand computer for integer factoring. **1984**,

2125 Proof Checking the RSA Public Key Encryption Algorithm. **1984**, 91, 181 11

2124 A Monte Carlo factoring algorithm with linear storage. **1984**, 43, 289-289 30

2123 On improvements to password security. **1985**, 19, 53-60 9

2122 A fair protocol for signing contracts. **1985**, 43-52 15

2121 The NP-completeness column: An ongoing guide. **1985**, 6, 291-305 17

2120 On the verifiability of two-party algebraic protocols. **1985**, 40, 101-130 4

2119 Standards for data security the state of the art. **1985**, 8, 231-234

2118 Number-theoretic functions which are equivalent to number of divisors. **1985**, 20, 151-153 6

2117 A secure and useful keyless cryptosystem **1985**, 21, 35-38 6

2116 An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information. **1984**, 289-299 94

2115 Group parity check system for important information. **1985**, 68, 35-39

2114	Design of public key cryptosystems using idempotent elements. **1985**, 4, 297-308		1
2113	A public key cryptosystem and a signature scheme based on discrete logarithms. **1985**, 31, 469-472		3225
2112	Encryption and Error-Correction Coding Using D Sequences. **1985**, C-34, 803-809		12
2111	The design of special purpose hardware are to factor large integers. **1985**, 37, 337-341		3
2110	An Update on Quantum Cryptography. **1984**, 475-480		37
2109	Bounds on information exchange for Byzantine agreement. **1985**, 32, 191-204		113
2108	A randomized protocol for signing contracts. *Communications of the ACM*, **1985**, 28, 637-647	2.5	742
2107	. **1985**, 64, 491-532		15
2106	Advances in Cryptology. **1985**,		17
2105	Modular multiplication without trial division. **1985**, 44, 519-519		716
2104	Strong Primes are Easy to Find. **1984**, 216-223		23
2103	A robust and verifiable cryptographically secure election scheme. **1985**,		180
2102	Verifiable secret sharing and achieving simultaneity in the presence of faults. **1985**,		332
2101	A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. **1984**, 10-18		645
2100	Randomized Byzantine Agreement. **1985**, SE-11, 539-546		9
2099	Streets of Byzantium: Network Architectures for Fast Reliable Broadcasts. **1985**, SE-11, 546-554		51
2098	Security in high-level network protocols. **1985**, 23, 12-24		15
2097	Message authentication. **1985**, 23, 29-40		28

2096	On the Cryptographic Applications of Random Functions (Extended Abstract). **1984**, 276-288		46
2095	Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, **1985**, 28, 1030-1044	2.5	966
2094	A Simple Unpredictable Pseudo-Random Number Generator. **1986**, 15, 364-383		550
2093	Direct sequence spread spectrum access to local area networks. **1986**, 9, 7-15		0
2092	How to construct random functions. **1986**, 33, 792-807		1156
2091	REASONING ABOUT KNOWLEDGE: AN OVERVIEW. **1986**, 1-17		38
2090	The NP-completeness column: An ongoing guide. **1986**, 7, 584-601		12
2089	On a public-key cryptosystem based on iterated morphisms and substitutions. **1986**, 48, 283-296		12
2088	Authentication: A concise survey. **1986**, 5, 243-250		2
2087	A Proposed Standard Format for RSA Cryptosystems. **1986**, 19, 21-34		9
2086	Two varieties of finite automaton public key cryptosystem and digital signatures. **1986**, 1, 9-18		16
2085	Security in electronic mail. **1986**, 9, 96-99		
2084	Software Authorization Systems. **1986**, 3, 34-41		4
2083	Use of trapdoor structures in cryptography. **1986**, 19, 153-173		
2082	On the Security of Ping-Pong Protocols when Implemented using the RSA (Extended Abstract). **1985**, 58-72		7
2081	Another Birthday Attack. **1985**, 14-17		21
2080	Direct Sequence Spread Spectrum Access to Local Area Networks. **1987**,		1
2079	Some Variations on RSA Signatures & their Security. **1987**, 49-59		2

2078	Public protection of software. **1987**, 5, 371-393	24
2077	Techniques to increase the computational throughput of bit-serial architectures.	11
2076	An algebra to represent security policies for cryptography-based secure storage systems. **1987**, 23, 9-23	
2075	Replicated distributed processing. **1987**, 325-337	3
2074	A model to order the encryption algorithms according to their quality. **1987**, 17, 30-47	
2073	An O (log n) expected rounds randomized byzantine generals protocol. **1987**, 34, 910-920	54
2072	A practical scheme for non-interactive verifiable secret sharing. **1987**,	463
2071	Covert Channels in LAN's. **1987**, SE-13, 292-296	125
2070	A computer dial access system based on public-key techniques. **1987**, 25, 73-79	4
2069	Matching Secrets in the Absence of a Continuously Available Trusted Authority. **1987**, SE-13, 289-292	2
2068	Electronic document authentication. **1987**, 1, 17-23	18
2067	Methods of factoring large integers. **1987**, 281-303	1
2066	A Digital Signature Scheme Secure Against Adaptive Chosen Message Attack**This research was supported by NSF grant MCS-80-06938, an IBM/MIT Faculty Development Award, and DARPA contract N00014-85-K-0125.. **1987**, 287-310	1
2065	Cryptology: From Caesar Ciphers to Public-key Cryptosystems. **1987**, 18, 2-17	10
2064	Open Problems in Number Theoretic Complexity. **1987**, 237-262	5
2063	Verifying the authentication of an information system user. **1987**, 6, 152-157	13
2062	TeleTrusT-OSIS and communication security. **1987**, 6, 206-218	2
2061	Design and administration of distributed and hierarchical information networks under partial orderings. **1987**, 6, 219-228	2

2060 Simulating authenticated broadcasts to derive simple fault-tolerant algorithms. **1987**, 2, 80-94 132

2059 Belief, awareness, and limited reasoning. **1987**, 34, 39-76 394

2058 On the distribution in short intervals of integers having no large prime factor. **1987**, 25, 249-273 12

2057 Automating the computation of authenticators for interbank telex messages. **1987**, 6, 396-402

2056 A cryptographic checksum for integrity protection. **1987**, 6, 505-510 32

2055 Strategies for extending the useful lifetime of DES. **1987**, 6, 300-313 3

2054 Implementing the RSA cryptosystem. **1987**, 6, 342-350 8

2053 Teletrust. **1987**, 13, 235-239 1

2052 A single public-key authentication scheme for multiple users. **1987**, 18, 14-24 4

2051 Reductions among number theoretic problems. **1987**, 72, 167-179 13

2050 Partitioned encryption and achieving simultaneity by partitioning. **1987**, 26, 81-88 5

2049 Optimization Models for Configuring Distributed Computer Systems. **1987**, C-36, 773-793 15

2048 An efficient solution of the congruence<tex>x^2 + ky^2 = mpmod{n}</tex>. **1987**, 33, 702-709 40

2047 . **1988**, 30, 407-412 1

2046 Zero-knowledge proofs of identity. **1988**, 1, 77-94 582

2045 A key distribution system equivalent to factoring. **1988**, 1, 95-105 127

2044 Is the Data Encryption Standard a group? (Results of cycling experiments on DES). **1988**, 1, 3-36 46

2043 The generation of random numbers that are probably prime. **1988**, 1, 53-64 24

2042	Some weak points of one fast cryptographic checksum algorithm and its improvement. **1988**, 7, 503-505	8
2041	Two secure file servers. **1988**, 7, 409-414	2
2040	Keeping security in perspective. **1988**, 4, 23-26	
2039	Partial information in public key cryptography. **1988**, 20, 261-263	
2038	Design, development and application of an intelligent token. **1988**, 11, 299-303	
2037	Computer networks and distributed systems. **1988**, 28, 419-467	3
2036	On using primes for public key encryption systems. **1988**, 1, 225-227	4
2035	A nonlinear public key cryptosystem. **1988**, 15, 81-84	1
2034	Key Distribution Systems Based on Identification Information. **1988**, 194-202	28
2033	A public-key cryptosystem based on the difficulty of solving a system of nonlinear equations. **1988**, 19, 10-18	4
2032	L□at de l□art en mati□e de techniques □cl□publique. **1988**, 43, 489-505	0
2031	. **1988**, 76, 578-593	55
2030	. **1988**, 37, 1654-1657	94
2029	. **1988**, 76, 533-549	139
2028	. **1988**, 76, 560-577	98
2027	. **1988**, 76, 603-620	82
2026	. **1988**, 76, 621-627	13
2025	Security standards for data networks. **1988**, 10, 7-11	

2024	Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. **1988**, 419-453	249
2023	.	0
2022	A Cryptography Processor. **1988**,	4
2021	. **1988**, 34, 901-909	118
2020	.	3
2019	A Pipeline Architecture for Factoring Large Integers with the Quadratic Sieve Algorithm. **1988**, 17, 387-403	32
2018	RSA and Rabin Functions: Certain Parts are as Hard as the Whole. **1988**, 17, 194-209	199
2017	A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. **1988**, 17, 281-308	1676
2016	Complexity Measures for Public-Key Cryptosystems. **1988**, 17, 309-335	195
2015	Solving Simultaneous Modular Equations of Low Degree. **1988**, 17, 336-341	104
2014	A Digital Signature Based on a Conventional Encryption Function. **1988**, 369-378	409
2013	Privacy Amplification by Public Discussion. **1988**, 17, 210-229	557
2012	Cryptographic Computation: Secure Fault-Tolerant Protocols and the Public-Key Model (Extended Abstract). **1988**, 135-155	45
2011	. **1988**,	27
2010	.	3
2009	Cryptosystems based on permutation polynomials. **1988**, 23, 237-250	1
2008	.	4
2007	.	5

2006	A digital multisignature scheme using bijective public-key cryptosystems. **1988**, 6, 432-441	84
2005	Fault tolerant distributed services. **1988**,	1
2004	The parallel complexity of exponentiating polynomials over finite fields. **1988**, 35, 651-667	18
2003	Fast RSA-Hardware: Dream or Reality?. **1988**, 257-264	10
2002	A Generalized Birthday Attack. **1988**, 129-156	28
2001	Advances in Cryptology EUROCRYPT 88. **1988**,	2
2000	Bibliography. **1988**, 453-468	
1999	On generalized Rédei functions. **1988**, 11, 625-634	
1998	Computational Approaches to Bargaining and Choice. **1989**, 1, 407-426	3
1997	A Course in Number Theory and Cryptography (Neil Koblitz). **1989**, 31, 508-510	
1996	Constructing Replicated Systems Using Processors With Point To Point Communication Links.	3
1995	A logic of authentication. **1989**, 23, 1-13	39
1994	Decentralizing a global naming service for improved performance and fault tolerance. **1989**, 7, 147-183	33
1993	Optimized software implementations of the modular exponentiation on general purpose microprocessors. **1989**, 8, 621-630	3
1992	Password authentication using public-key cryptography. **1989**, 18, 1001-1017	10
1991	Security architecture for data transfer through TCP/IP protocols. **1989**, 8, 709-720	0
1990	A remark on hash functions for message authentication. **1989**, 8, 55-58	2
1989	Factoring with the quadratic sieve on large vector computers. **1989**, 27, 267-278	7

1988	Security issues in the use of smart cards. **1989**, 12, 25-30	1
1987	The RSA Public Key Crypto-System. **1989**, 43-57	
1986	. **1989**, 24, 1071-1075	5
1985	. **1989**, 7, 290-294	25
1984	. **1989**, 7, 435-447	4
1983	. **1989**, 7, 481-485	83
1982	. **1989**, 7, 486-498	27
1981	. **1989**, 7, 505-516	2
1980	. **1989**, 7, 517-524	9
1979	. **1989**, 7, 534-539	14
1978	Secure communication in internet environments: a hierarchical key management scheme for end-to-end encryption. **1989**, 37, 1014-1023	19
1977	VLSI crypto-technology-application requirements.	1
1976	Application of a key generation and distribution algorithm for secure communication in open systems interconnection architecture.	3
1975	.	
1974	A new architecture for fast modular multiplication.	1
1973	.	1
1972	Collision-free hashfunctions based on blockcipher algorithms.	16
1971	.	4

1970	.	
1969	.	0
1968	Means and Measures for Data Security. **1989**, 22, 1-6	0
1967	Constructing replicated systems using processors with point-to-point communication links. **1989**, 17, 177-184	
1966	Secure cryptographic initialisation of remote terminals in an electronic funds transfer/point of sale system. **1990**, 451-462	
1965	Anonymous one-time signatures and flexible untraceable electronic cash. **1990**, 294-305	12
1964	Codemakers versus Codebreakers. **1990**, 15, 349-356	
1963	A fast modular-multiplication module for smart cards. **1990**, 406-409	4
1962	. **1990**, 36, 40-46	194
1961	. **1990**, 36, 47-53	16
1960	. **1990**, 36, 553-558	326
1959	A proposal on digital watermark in document image communication and its application to realizing a signature. **1990**, 73, 22-33	4
1958	Identity-based conference key distribution systems. **1990**, 21, 60-67	
1957	Proposal for Cryptographic Key Distribution System Based on Identification Information. **1990**, 21, 76-84	
1956	A scheme for providing security services in ISO-OSI computer network architecture. **1990**, 16, 35-41	
1955	Approaching encryption at ISDN speed using partial parallel modulus multiplication. **1990**, 29, 177-184	6
1954	A cryptographic key generation scheme for multilevel data security. **1990**, 9, 539-546	106
1953	A key management algorithm for secure communication in open systems interconnection architecture. **1990**, 9, 77-84	3

1952	Cryptanalysis of a fast cryptographic checksum algorithm. **1990**, 9, 257-262	5
1951	The combinatorics of authentication and secrecy codes. **1990**, 2, 23-49	100
1950	Design of an RSA Encryption Processor Based on Signed-Digit Multivalued Arithmetic Circuits. **1990**, 21, 21-31	3
1949	A Method for Rapid RSA Key Generation. **1990**, 21, 11-20	
1948	The management and control of system security. **1990**, 1990, 7-17	
1947	A cartesian product construction for unconditionally secure authentication codes that permit arbitration. **1990**, 2, 77-104	54
1946	An efficient probabilistic encryption scheme. **1990**, 34, 123-129	6
1945	Secure network bootstrapping: An algorithm for authentic key exchange and digital signitures. **1990**, 9, 145-152	1
1944	Security for open communication: The DFN mail security project report. **1990**, 19, 196-200	
1943	Automatically increasing the fault-tolerance of distributed algorithms. **1990**, 11, 374-419	64
1942	Security, veriflability, and universality in distributed computing. **1990**, 11, 492-521	6
1941	Network management issues in support of X.32 services. **1990**, 13, 347-353	
1940	Cryptography. **1990**, 717-755	31
1939	Parallel algorithms for integer factorisation. **1990**, 26-37	7
1938	Record encryption in distributed databases. **1990**, 386-395	
1937	Speeding up the computations on an elliptic curve using addition-subtraction chains. **1990**, 24, 531-543	127
1936	Secure user access control for public networks. **1990**, 45-57	0
1935	ID based public key cryptosystems based on Okamoto and Tanaka's ID based one way communication scheme. **1990**, 26, 666-668	3

1934	Remote evaluation. **1990**, 12, 537-564	92
1933	.	33
1932	.	0
1931	.	0
1930	New public-key cryptosystem. **1990**, 21, 205-215	
1929	A logic of authentication. **1990**, 8, 18-36	1385
1928	Multiplication of large integers by the use of modular arithmetic. **1990**, 7, 7-20	1
1927	.	0
1926	A Survey of Hardware Implementations of RSA. **1989**, 368-370	49
1925	On the formal analysis of PKCS authentication protocols. **1990**, 105-121	9
1924	On-Line/Off-Line Digital Signatures. **1989**, 263-275	112
1923	Number-Theoretic Algorithms. **1990**, 4, 119-172	10
1922	Advances in Cryptology [CRYPTO]88. **1990**,	16
1921	.	12
1920	.	
1919	. **1990**,	80
1918	.	0
1917	.	1

1916 . **1990**, 0

1915 . **1990**, 2

1914 . 7

1913 . 6

1912 .

1911 . **1990**,

1910 A simplified and an efficient packet level Internet access control scheme.

1909 Untraceable Electronic Cash. **1990**, 319-327 452

1908 . **1990**, 278

1907 Meet-in-the-middle attack on digital signature schemes. **1990**, 140-154 1

1906 . **1990**, 39, 605-614 10

1905 An Identity-Based Key-Exchange Protocol. **1989**, 29-37 102

1904 A verification of brickell's fast modular multiplication algorithm. **1990**, 33, 153-169 11

1903 Cryptography Based Data Security. **1990**, 30, 171-222 1

1902 . **1990**, 10

1901 Addition Machines. **1990**, 19, 329-340 10

1900 A Certified Digital Signature. **1989**, 218-238 529

1899 . **1990**, 16, 100-104

1898	. **1990**, 16, 647-659	11
1897	. **1990**, 16, 710-722	36
1896	On Counting Lattice Points in Polyhedra. **1991**, 20, 695-707	13
1895	. **1991**, 40, 646-653	5
1894	. **1991**, 39, 324-335	73
1893	. **1991**, 29, 42-48	6
1892	.	49
1891	.	2
1890	. **1991**,	
1889	.	1
1888	.	7
1887	.	0
1886	.	0
1885	.	0
1884	.	16
1883	A password authentication scheme based on discrete logarithms. **1991**, 41, 31-38	1
1882	.	0
1881	.	

1880 . 78

1879 . 1

1878 .

1877 . 15

1876 .

1875 . 1

1874 .

1873 . 6

1872 . 7

1871 Interactive identification and digital signatures. **1991**, 70, 73-86 18

1870 EDI□ strategic weapon in international trade. **1991**, 24, 46-53 24

1869 Self-certified public keys. **1991**, 490-497 197

1868 Espionage and sabotage in the computer world. **1991**, 5, 155-202 2

1867 Fast modular multiplication using 2-power radix. **1991**, 39, 21-28 7

1866 Protection and security issues for future systems. **1991**, 183-201 1

1865 Authentication in distributed systems. **1991**, 25, 165-182 24

1864 Current trends in distributed systems. **1991**, 204-224 1

1863 A high-performance software implementation of the Data Encryption Algorithm (DEA). **1991**, 14, 343-362

1862	Secure transfer of identity and privilege attributes in an open systems environment. **1991**, 10, 117-127	1
1861	Optimized implementation of RSA cryptosystem. **1991**, 10, 263-267	6
1860	Key distribution system for mail systems using ID-related information directory. **1991**, 10, 25-33	10
1859	Security in open networks and distributed systems. **1991**, 22, 323-346	17
1858	Secure control of transit internetwork traffic. **1991**, 22, 363-382	7
1857	Piloting ODA The PODA project. **1991**, 11, 183-193	2
1856	A digital signature scheme on a document for MH facsimile transmission. **1991**, 74, 30-37	
1855	A survey of identification schemes. **1991**, 167-179	
1854	On an Implementation of the Mohan-Adiga Algorithm. **1991**, 496-500	2
1853	A cryptographic approach to the secret ballot. **1991**, 36, 34-40	9
1852	Password authentication using Newton's interpolating polynomials. **1991**, 16, 97-102	6
1851	Performance evaluation of a multivalued rsa encryption vlsi. **1991**, 22, 12-21	1
1850	Construction and evaluation of the identity transformers for cryptographic key distribution. **1991**, 22, 1-13	
1849	Bit-level systolic arrays for modular multiplication. **1991**, 3, 215-223	19
1848	Efficient signature generation by smart cards. **1991**, 4, 161-174	1581
1847	An implementation for a fast public-key cryptosystem. **1991**, 3, 63-79	130
1846	Applying a formal analysis technique to the CCITT X.509 strong two-way authentication protocol. **1991**, 3, 81-98	30
1845	One-way permutations on elliptic curves. **1991**, 3, 187-199	33

1844	Hardware speedups in long integer multiplication. **1991**, 19, 106-113		19
1843	High-radix and bit recoding techniques for modular exponentiation. **1991**, 40, 139-156		18
1842	.		0
1841	.		0
1840	.		6
1839	Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. **1991**, 38, 690-728		612
1838	A faster modular multiplication algorithm. **1991**, 40, 63-68		20
1837	Superimposing encrypted data. *Communications of the ACM*, **1991**, 34, 48-54	2.5	11
1836	A Cryptographic Library for the Motorola DSP56000. **1991**, 230-244		49
1835	Advances in Cryptology □EUROCRYPT □0. **1991**,		4
1834	Identity-based Non-interactive Common-key Generation.		1
1833	.		
1832	An Ultra-high Speed Public Key Encryption Processor.		7
1831	Responses to NIST's proposal. *Communications of the ACM*, **1992**, 35, 41-54	2.5	37
1830	A Record-Oriented Cryptosystem for Database Sharing. **1992**, 35, 658-660		3
1829	Systematic Design of Two-Party Authentication Protocols. **1991**, 44-61		36
1828	Computer Security □ESORICS 92. **1992**,		0
1827	Cryptographic Primitives And Quantum Theory.		1

1826	.	4
1825	New Public-Key Schemes Based on Elliptic Curves over the Ring Zn. **1991**, 252-266	58
1824	Integrity Primitives for Ibc.	0
1823	Authentication in distributed systems. **1992**, 10, 265-310	373
1822	.	1
1821	Using public domain multiprecision arithmetic packages for computer security software applications on a personal computer. **1992**, 18, 9-12	1
1820	Attack on server assisted authentication protocols. **1992**, 28, 1473	21
1819	Operating MSDOS in a Controlled Environment. **1992**, 25, 221-224	
1818	Verification and modelling of authentication protocols. **1992**, 141-154	1
1817	Computing A*B (mod N) efficiently in ANSI C. **1992**, 27, 95-98	6
1816	SPX: Global Authentication Using Public Key Certificates. **1992**, 1, 295-316	1
1815	.	449
1814	. **1992**,	53
1813	. **1992**,	5
1812	On Addition Chains 1. **1992**, 45, 145-160	1
1811	. **1992**, 30, 30-35	2
1810	A Calculus for Access Control in Distributed Systems. **1991**, 1-23	6
1809	Security and X.400 systems. **1992**, 1992, 10-15	

1808 . **1992**, 41, 542-549 26

1807 . **1992**, 41, 949-956 42

1806 . **1992**, 41, 887-891 38

1805 . **1992**, 27, 109-112 22

1804 .

1803 A High Performance RSA Encryption Processor in SOI and Bulk CMOS Technologies. **1992**,

1802 Message authentication with one-way hash functions. **1992**, 22, 29-38 81

1801 Secret ballot elections and public-key cryptosystems. **1992**, 8, 295-303 4

1800 Associating metrics to certification paths. **1992**, 175-189 10

1799 Authentication and authenticated key exchanges. **1992**, 2, 107-125 593

1798 A concurrent solution to computer security. **1992**, 6, 191-201

1797 Which new RSA-signatures can be computed from certain given RSA-signatures?. **1992**, 5, 41-52 14

1796 COSINE Sub-Project P8: security services. **1992**, 25, 476-482 2

1795 Piloting authentication and security services within OSI applications for RTD information (PASSWORD). **1992**, 25, 483-489 5

1794 MHS security□ concise survey. **1992**, 25, 490-495

1793 Requirements for cryptographic hash functions. **1992**, 11, 427-437 3

1792 Asymmetric user authentication. **1992**, 11, 173-183 2

1791 A software authentication system for information integrity. **1992**, 11, 747-752 3

1790	An RSA based public-key cryptosystem for secure communication. **1992**, 102, 147-153	
1789	. **1992**,	42
1788	Two distributed problems involving involving byzantine processes. **1992**, 95, 169-185	
1787	. **1992**, 25, 39-52	88
1786	A digital multisignature method for facsimile-mail service. **1992**, 75, 47-57	
1785	Model programs for computational science: A programming methodology for multicomputers. **1993**, 5, 407-423	25
1784	Placement of cryptographic key distribution within OSI: design alternatives and assessment. **1993**, 26, 217-225	1
1783	Privacy enhanced mail in more detail. **1993**, 25, 63-71	
1782	Operating system protection through program evolution. **1993**, 12, 565-584	155
1781	The Digital Signature Standard: Overview and current status. **1993**, 12, 437-446	1
1780	More efficient software implementations of (generalized) DES. **1993**, 12, 477-500	6
1779	Cryptographic Application Programming Interfaces (APIs). **1993**, 12, 640-645	3
1778	Authentication and delegation with smart-cards. **1993**, 21, 93-113	42
1777	The discrete logarithm modulo a composite hides 0(n) Bits. **1993**, 47, 376-404	40
1776	Access control in a hierarchy using a one-way trap door function. **1993**, 26, 71-76	19
1775	The design of dynamic access control scheme with user authentication. **1993**, 25, 27-32	7
1774	A design of a fast pipelined modular multiplier based on a diminished-radix algorithm. **1993**, 6, 183-208	3
1773	Mathematical problems in cryptology. **1993**, 67, 3373-3406	

1772 . **1993**, 39, 1121-1132 737

1771 . **1993**, 39, 733-742 1175

1770 Cancellation and reassignment of votes in secret ballot elections. **1993**, 9, 427-435 3

1769 Cryptographic protocols for Vickrey auctions. **1993**, 2, 363-373 20

1768 An improved binary algorithm for RSA. **1993**, 25, 15-24 19

1767 Public key management for X.25 network security. **1993**, 12, 128-133

1766 Implementing and proving security services for the RARE/COSINE community. **1993**, 26, 263-267

1765 . **1993**, 41, 1777-1779 3

1764 . **1993**, 39, 905-910 166

1763 . **1993**, 13, 74-81 15

1762 On the Existence of Pseudorandom Generators. **1993**, 22, 1163-1175 71

1761 Small-Bias Probability Spaces: Efficient Constructions and Applications. **1993**, 22, 838-856 343

1760 A public key extension to the Common Cryptographic Architecture. **1993**, 32, 461-485 0

1759 . **1993**, 4

1758 Optical memory card applicability for implementing a portable medical record. **1993**, 18, 271-8 2

1757 . **1993**,

1756 . **1993**,

1755 . 80

1754	. **1993**,	
1753	.	
1752	Authentication method with impersonal token cards.	4
1751	Some remarks on protecting weak keys and poorly-chosen secrets from guessing attacks.	8
1750	.	
1749	.	2
1748	Secure delegation of tasks in distributed systems.	2
1747	.	22
1746	. **1993**,	1
1745	.	2
1744	A modular multiplication algorithm with triangle additions.	7
1743	.	3
1742	Byzantine agreement with a minimum number of messages both in the faultless and worst case.	1
1741	. **1993**, 42, 376-378	132
1740	. **1993**, 42, 693-699	119
1739	. **1993**, 11, 648-656	226
1738	. **1993**, 11, 679-693	83
1737	. **1993**, 11, 694-701	25

1736 . **1993**, 11, 725-729 28

1735 . **1993**, 11, 757-760 15

1734 . **1993**, 11, 778-784 31

1733 Parallel implementation of the rsa public-key cryptosystem. **1993**, 48, 153-155 9

1732 Programmable active memories: a performance assessment. **1993**, 119-130 24

1731 . 32

1730 On Rsa Signatures.

1729 Public-key cryptosystem based on the discrete logarithm problem. **1993**, 469-476

1728 A fast logic for modular multiplication. **1993**, 74, 851-855 1

1727 Integrating security in inter-domain routing protocols. **1993**, 23, 36-51 18

1726 Clipping Clipper. *Communications of the ACM*, **1993**, 36, 15-17 2.5 5

1725 Open commit protocols tolerating commission failures. **1993**, 18, 289-332 6

1724 Digital signatures. **1993**, 4

1723 Augmented encrypted key exchange. **1993**, 280

1722 Lower bounds on messages and rounds for network authentication protocols. **1993**, 21

1721 A generic multicast-key determination protocol. 2

1720 A calculus for access control in distributed systems. **1993**, 15, 706-734 317

1719 .

1718	. **1993**, 1, 56-70	12
1717	.	
1716	An Efficient Digital Signature Scheme Based on an Elliptic Curve over the Ring Zn. **1992**, 54-65	1
1715	.	
1714	Algorithm 719: Multiprecision translation and execution of FORTRAN programs. **1993**, 19, 288-319	111
1713	Advances in Cryptology [CRYPTO]92. **1993**,	7
1712	Speeding up Elliptic Cryptosystems by Using a Signed Binary Window Method. **1992**, 345-357	42
1711	Secure and efficient off-line digital money (extended abstract). **1993**, 265-276	48
1710	A fast modular multiplication algorithm. **1993**, 49, 11-17	
1709	A novel method for key exchange and authentication with cellular network applications.	1
1708	Coding. **1993**, 14-1-14-13	3
1707	Optimality of Asynchronous Two-Party Secure Data-Exchange Protocols*. **1993**, 2, 191-209	2
1706	Logarithmic speed modular multiplication. **1994**, 30, 1397-1398	11
1705	Factoring. **1994**, 28-38	2
1704	Mathematical Certificates. **1994**, 67, 21-28	
1703	Using four-prime RSA in which some of the bits are specified. **1994**, 30, 2118-2119	3
1702	Anonymous credit cards. **1994**,	20
1701	.	

1700	. **1994**, 6, 188-191		1
1699	Advances in Cryptology □EUROCRYPT ▯3. **1994**,		14
1698	A server-aided computation protocol for rsa enciphering algorithm. **1994**, 53, 149-155		2
1697	Secure distributed computing: Theory and practice. **1994**, 53-73		
1696	Standardizing information technology security. **1994**, 2, 64-71		
1695	Cryptography policy. *Communications of the ACM*, **1994**, 37, 109-117	2.5	15
1694	A Course in Number Theory and Cryptography. **1994**,		231
1693	Security of RSA-type cryptosystems over elliptic curves against Hastad attack. **1994**, 30, 1843-1844		8
1692	Towards the Equivalence of Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms. **1994**, 271-281		69
1691	On randomization in sequential and distributed algorithms. **1994**, 26, 7-86		33
1690	How to securely replicate services. **1994**, 16, 986-1009		42
1689	Multiplication of signed-digit numbers. **1994**, 30, 840		12
1688	A security architecture for fault-tolerant systems. **1994**, 12, 340-371		25
1687	Technique for authentication, access control and resource management in open distributed systems. **1994**, 30, 124-125		9
1686	Iterative modular multiplication algorithm without magnitude comparison. **1994**, 30, 2017-2018		12
1685	Meet your destiny. **1994**,		12
1684	Broadcast Encryption. **1993**, 480-491		569
1683	.		0

1682	.	
1681	.	6
1680	A new service for digital mobile communications.	
1679	.	7
1678	.	75
1677	Authentication and protection of public keys. **1994**, 13, 581-585	2
1676	A dynamic cryptographic key generation and information broadcasting scheme in information systems. **1994**, 13, 601-610	2
1675	Digital signatures and their uses. **1994**, 13, 385-391	2
1674	Functional inversion and communication complexity. **1994**, 7, 153-170	
1673	Efficient data structures for Boolean functions. **1994**, 136, 347-372	26
1672	On dynamic threshold schemes. **1994**, 52, 201-206	11
1671	Exponentiation using canonical recoding. **1994**, 129, 407-417	24
1670	Secure end-to-end delegations in distributed systems. **1994**, 17, 230-238	5
1669	Attacks on an ID-based signature scheme based on Rabin's public key cryptosystem. **1994**, 17, 674-676	
1668	Modern key agreement techniques. **1994**, 17, 458-465	23
1667	SESAME: The solution to security for open distributed systems. **1994**, 17, 501-518	40
1666	Montgomery modular-multiplication method and systolic arrays suitable for modular exponentiation. **1994**, 77, 40-51	8
1665	A new method for breaking the Lu-Lee cryptosystem. **1994**, 77, 50-56	

1664 Multiple-length division revisited: A tour of the minefield. **1994**, 24, 579-601 2

1663 Cryptographic limitations on learning Boolean formulae and finite automata. **1994**, 41, 67-95 329

1662 Conducting secret ballot elections in computer networks: Problems and solutions. **1994**, 51, 185-194 3

1661 Authenticated encryption schemes with low communication costs. **1994**, 30, 1212-1213 95

1660 Number Theory and Cryptography. **1994**, 211-236

1659 . 1854

1658 . **1994**, 32, 33-38 654

1657 . **1994**, 32, 70-74 23

1656 Homomorphic Zero-Knowledge Threshold Schemes over any Finite Abelian Group. **1994**, 7, 667-679 63

1655 More Flexible Exponentiation with Precomputation. **1994**, 95-107 134

1654 . 1

1653 . **1994**, 5, 449-458 9

1652 .

1651 Efficient Routing and Broadcasting in Recursive Interconnection Networks. **1994**, 9

1650 An engineering approach to secure system analysis, design, and integration. **1994**, 73, 40-51 2

1649 . 1

1648 . 4

1647 . 1

1646	Authentication in the Taos operating system. **1994**, 12, 3-32	112
1645	The ESPRIT project CAFE High security digital payment systems. **1994**, 217-230	30
1644	.	4
1643	Network security in a heterogeneous environment. **1994**, 73, 52-60	1
1642	Issues and Mechanisms for Trustworthy Systems: Creating Transparent Mistrust. **1994**, 73, 30-39	3
1641	Prudent engineering practice for cryptographic protocols. **1994**,	65
1640	.	3
1639	. **1994**,	1
1638	The Travelling Salesman Cipher. **1994**, 40, 151-154	
1637	. **1994**,	4
1636	Fast square-and-multiply exponentiation for RSA. **1994**, 30, 1396-1397	20
1635	The game of matrix rings for cryptography. **1994**, 25, 121-124	
1634	Providing auditing while protecting privacy. **1994**, 10, 59-71	2
1633	Cryptography for PC/workstation security. **1994**, 20, 21-26	
1632	Efficient electronic money. **1995**, 151-163	17
1631	Authentication protocols for personal communication systems. **1995**, 25, 256-261	11
1630	O(n)-depth circuit algorithm for modular exponentiation.	6
1629	Programming Satan's computer. **1995**, 426-440	45

1628 Near optimal unconditionally secure authentication. **1995**, 244-253 11

1627 Efficient exponentiation using precomputation and vector addition chains. **1995**, 389-399 45

1626 A symmetric cipher using autonomous and non-autonomous cellular automata. 1

1625 Integrated authentications based on identities.

1624 Key-spoofing attacks on nested signature blocks. **1995**, 31, 1043-1044 3

1623 An attack on the Needham-Schroeder public-key authentication protocol. **1995**, 56, 131-133 361

1622 On the security of the Lucas function. **1995**, 53, 243-247 14

1621 Analysis of sliding window techniques for exponentiation. **1995**, 30, 17-24 77

1620 Formal language for security services base modelling and analysis. **1995**, 18, 921-928 2

1619 Fibonacci linear forms and parallel arithmetic algorithms for large numbers. **1995**, 31, 401-408 2

1618 Can Montgomery parasites be avoided? A design methodology based on key and cryptosystem modifications. **1995**, 5, 73-80 3

1617 Efficient network authentication protocols: Lower bounds and optimal implementations. **1995**, 9, 131-145 26

1616 On the oracle complexity of factoring integers. **1995**, 5, 237-247 8

1615 Communication intercentres d'images et de signaux multimodalit par r eau RNIS. **1995**, 17, 46-51

1614 Short RSA keys and their generation. **1995**, 8, 101-114 35

1613 Fast generation of prime numbers and secure public-key cryptographic parameters. **1995**, 8, 123-155 54

1612 A dual basis bit-serial systolic multiplier for GF(2). **1995**, 18, 139-149 9

1611 A cardinalised binary representation for exponentiation. **1995**, 30, 33-39 12

1610	Password authentications using triangles and straight lines. **1995**, 30, 63-71	12
1609	A two-phase encryption scheme for enhancing database security. **1995**, 31, 257-265	10
1608	Traffic control at terminal equipment in ATM networks using cryptographic techniques. **1995**, 18, 486-492	1
1607	ID-based non-interactive zero-knowledge proof system based on one-out-of-two non-interactive oblivious transfer. **1995**, 18, 993-996	3
1606	Smartcard standardization: Inter-industry commands and application selection. **1995**, 17, 81-87	
1605	Information Technology - Security techniques and standardization. **1995**, 17, 63-67	1
1604	Non-repudiation: Constituting evidence and proof in digital cooperation. **1995**, 17, 69-79	5
1603	Multicast security and its extension to a mobile environment. **1995**, 1, 281-295	34
1602	The design and implementation of a private message service for mobile computers. **1995**, 1, 297-309	12
1601	Demonstration of a fundamental quantum logic gate. **1995**, 75, 4714-4717	1129
1600	Higher radix nonrestoring modular multiplication algorithm and public-key LSI architecture with limited hardware resources. **1995**, 365-375	
1599	Still faster modular multiplication. **1995**, 31, 263-264	19
1598	Algorithmic number theory and its relationship to computational complexity. **1995**, 159-171	0
1597	The blinding of weak signatures. **1995**, 67-76	3
1596	Security services for telecommunications users. **1995**, 26-39	1
1595	References. **1995**, 447-466	
1594	Towards High Performance Cryptographic Software.	14
1593	Towards a classification of key agreement protocols.	3

1592 PARALLEL COMPUTATION OF THE MODULAR CASCADE EXPONENTIATION. **1995**, 7, 29-42 2

1591 . 24

1590 Secure acceleration of DSS signatures using insecure server. **1995**, 249-259 4

1589 Archiving Electronic Journals. **1995**, 21, 13-21 6

1588 The magic words are squeamish ossifrage. **1995**, 261-277 19

1587 Securing data transfer in asynchronous transfer mode networks. 6

1586 Cryptanalysis of secure addition chain for SASC applications. **1995**, 31, 175-176 4

1585 Extending the Wiener attack to RSA-type cryptosystems. **1995**, 31, 1736-1738 11

1584 Focused fault injection testing of software implemented fault tolerance mechanisms of Voltan TMR nodes. **1995**, 2, 39-49 3

1583 Improved generalisation common-multiplicand multiplications algorithm of Yen and Laih. **1995**, 31, 1738-1739 18

1582 Multiplicative non-abelian sharing schemes and their application to threshold cryptography. **1995**, 19-32 17

1581 Use of RSA moduli with prespecified bits. **1995**, 31, 785-786

1580 Dynamic fault-tolerant clock synchronization. **1995**, 42, 143-185 31

1579 Secure communications in ATM networks. *Communications of the ACM*, **1995**, 38, 45-52 2.5 26

1578 Uniform Random Numbers. **1995**, 141

1577 Advances in Cryptology □EUROCRYPT ⍰5. **1995**,

1576 An encryption/signature scheme with low message expansion. **1995**, 18, 591-595 8

1575 . **1995**, 3, 31-41 42

1574	Integrity concepts. **1995**, 9-22	0
1573	A secure and efficient conference key distribution system. **1995**, 275-286	300
1572	. **1995**, 13, 416-420	42
1571	. **1995**, 13, 1523-1531	10
1570	. **1995**, 83, 944-957	201
1569	. **1995**, 44, 729-730	2
1568	. **1995**, 44, 957-959	36
1567	. **1995**, 44, 1064-1065	104
1566	Fair Blind Signatures. **1995**, 209-219	112
1565	Blind signatures based on the discrete logarithm problem. **1995**, 428-432	70
1564	.	90
1563	Quantum cryptography. **1995**, 36, 149-163	93
1562	TMR processing without explicit clock synchronisation.	2
1561	Implementation of a hybrid encryption scheme for Ethernet.	4
1560	Efficient protocols secure against guessing and replay attacks.	9
1559	.	4
1558	.	
1557	.	27

1556	A personal view of average-case complexity.	58
1555	Security estimates for 512-bit RSA.	0
1554	.	
1553	ATOMIC BROADCAST: FROM SIMPLE MESSAGE DIFFUSION TO BYZANTINE AGREEMENT.	35
1552	.	
1551	.	17
1550	. **1995**, 2, 34-49	155
1549	.	
1548	Synthesizers and their application to the parallel construction of pseudo-random functions.	12
1547	.	18
1546	. **1995**, 43, 3-6	131
1545	A secure anonymous voting by employing Diffie-Hellman PKD concept.	1
1544	Certifying Permutations: Noninteractive zero-knowledge based on any trapdoor permutation. **1996**, 9, 149-166	36
1543	On-line/off-line digital signatures. **1996**, 9, 35-67	202
1542	Security Proofs for Signature Schemes. **1996**, 387-398	445
1541	A Non-interactive Public-Key Distribution System. **1996**, 9, 305-316	
1540	Achieving Rights Untransferability with Client-Independent Servers. **1996**, 8, 263-271	0
1539	New hybrid fault models for asynchronous approximate agreement. **1996**, 45, 439-449	18

1538	Implementing fail-silent nodes for distributed systems. **1996**, 45, 1226-1238	21
1537	Blind decoding, blind undeniable signatures, and their applications to privacy protection. **1996**, 257-264	16
1536	An empirical study of secure MPEG video transmissions.	91
1535	25 years of quantum cryptography. **1996**, 27, 13-24	37
1534	Distributed communication services in the Masix system.	
1533	Limitations on design principles for public key protocols.	7
1532	Implementing the Rivest, Shamir, Adleman cryptographic algorithm on the Motorola 56300 family of digital signal processors.	
1531	. **1996**, 4, 56-69	190
1530	Redundant integer representations and fast exponentiation. **1996**, 7, 135-151	11
1529	A non-interactive public-key distribution system. **1996**, 9, 305-316	37
1528	Achieving rights untransferability with client-independent servers. **1996**, 8, 263	1
1527	. **1996**, 22, 6-15	234
1526	A secure group membership protocol. **1996**, 22, 31-42	48
1525	. **1996**, 22, 302-312	143
1524	. **1996**, 34, 56-61	6
1523	Cryptographic smart cards. **1996**, 16, 14, 16-24	58
1522	Analyzing and comparing Montgomery multiplication algorithms. **1996**, 16, 26-33	296
1521	SCALPS: Smart card for limited payment systems. **1996**, 16, 42-51	7

1520	Quantum-inspired genetic algorithms.	252
1519	GF(2/sup m/) multiplication and division over the dual basis. **1996**, 45, 319-327	85
1518	Public key security systems [Guest Editor's Introduction]. **1996**, 16, 10	3
1517	Modelling a public-key infrastructure. **1996**, 325-350	99
1516	Digital watermarks for audio signals. **1996**,	205
1515	A systolic RSA public key cryptosystem.	4
1514	Designated Verifier Proofs and Their Applications. **1996**, 143-154	314
1513	Provably secure blind signature schemes. **1996**, 252-265	90
1512	Security enhanced MPEG player.	2
1511	Services and architectures for electronic publishing.	1
1510	A new paradigm for public key identification. **1996**, 42, 1757-1768	102
1509	An authenticated camera.	7
1508	Preserving integrity in remote file location and retrieval.	1
1507	A high-throughput secure reliable multicast protocol.	11
1506	Parallelized network security protocols.	4
1505	Cryptographic postage indicia. **1996**, 378-391	4
1504	A private architecture for public networks.	1
1503	Advances in Cryptology □CRYPTO □6. **1996**,	9

1502	The IC design of a high speed RSA processor.	2
1501	Pipeline algorithms of RSA data encryption and data compression.	4
1500	Security issues in an EDI environment.	1
1499	Groups, Factoring, and Cryptography. **1996**, 69, 103-109	4
1498	Computing in Abstract Algebra. **1996**, 27, 136-142	1
1497	Secure communication in distributed Ada. **1996**, 198-210	
1496	Games servers play: A procedural approach. **1996**, 127-142	
1495	A cryptologic based trust center for medical images. **1996**, 3, 410-21	13
1494	A multi-recastable ticket scheme for electronic elections. **1996**, 116-124	5
1493	On the efficiency of one-time digital signatures. **1996**, 145-158	25
1492	Security issues on the Internet. **1996**, 14, 37-42	1
1491	Cryptosystems for hierarchical groups. **1996**, 275-286	2
1490	Cryptovirology: extortion-based security threats and countermeasures.	59
1489	Some active attacks on fast server-aided secret computation protocols for modular exponentiation. **1996**, 215-227	1
1488	Access with pseudonyms. **1996**, 232-243	41
1487	Public-key cryptography on smart cards. **1996**, 250-269	
1486	Integrating smart cards into authentication systems. **1996**, 270-281	5
1485	Foiling active network impersonation attacks made in collusion with an insider. **1996**, 301-312	

1484 The CASS shell. **1996**, 313-325 0

1483 Cost-effective payment schemes with privacy regulation. **1996**, 266-275 13

1482 RSA decryption using the one-hot residue number system.

1481 The validation of cryptographic algorithms. **1996**, 301-310 4

1480 How to utilize the transformability of digital signatures for solving the oracle problem. **1996**, 322-333 7

1479 A message recovery signature scheme equivalent to DSA over elliptic curves. **1996**, 1-14 8

1478 Quantum cryptographic network based on quantum memories. **1996**, 54, 2651-2658 131

1477 A redundant binary algorithm for RSA. **1996**, 11, 416-420 0

1476 Security in computer networks and distributed systems. **1996**, 19, 379-388 3

1475 Carryless addition. **1996**, 32, 153-163 0

1474 A practical parallel algorithm for computinga b modc *. **1996**, 1, 446-449

1473 From quantum cellular automata to quantum lattice gases. **1996**, 85, 551-574 436

1472 Modified Harn signature scheme based on factorising and discrete logarithms. **1996**, 143, 196 18

1471 Cryptographic Key Agreement for Mobile Radio. **1996**, 6, 207-212 101

1470 A highly safe self-stabilizing mutual exclusion algorithm. **1996**, 57, 301-305 13

1469 Smart card based secure password authentication scheme. **1996**, 15, 231-237 63

1468 A tool for support of key distribution and validity certificate check in global Directory service. **1996**, 28, 709-717

1467 Cryptanalysis and repair of the multi-verifier signature with verifier specification. **1996**, 15, 537-544 1

1466	GOST 34.10A brief overview of Russia's DSA. **1996**, 15, 725-732	7
1465	Design and implementation of a multimedia CSCW platform. **1996**, 2, 85-109	
1464	Two ID-based multisignature protocols for sequential and broadcasting architectures. **1996**, 19, 851-856	11
1463	Security platforms in the telecommunication market: technologies, developments and regulations. **1996**, 19, 824-829	
1462	Pretty good encryption. **1996**, 22, 133-146	0
1461	Mathematical Mysteries. **1996**,	6
1460	Verifiable transaction atomicity for electronic payment protocols.	2
1459	.	
1458	Breaking and fixing the Needham-Schroeder Public-Key Protocol using FDR. **1996**, 147-166	405
1457	A systolic linear array for modular multiplication.	
1456	BSA: a framework for efficient accounting on wide-area networks.	
1455	Mixing E-mail with Babel.	91
1454	Tamper resistant software: an implementation. **1996**, 317-333	112
1453	Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. **1996**, 104-113	1535
1452	Irreversible encryption method by generation of polynomials. **1996**, 21, 113-21	6
1451	On design of efficient square generator.	
1450	KOMMUNIKATION. **1996**, 19,	
1449	Systems Support for the Information Age. **1996**, 38, 12-17	

1448 The Yaksha security system. *Communications of the ACM*, **1996**, 39, 55-60 2.5 120

1447 .

1446 Finite automation cryptosystem.

1445 On the security of Park et al.'s key distribution protocol for digital mobile communications.

1444 An improvement of the digital cash protocol of Okamoto and Ohta. **1996**, 436-445

1443 Fast exponentiation method by folding exponent in half. **1996**, 32, 984 20

1442 Strategic directions in research in theory of computing. **1996**, 28, 575-590 3

1441 Towards a world-wide civilization of objects. **1996**, 5

1440 Protecting the integrity of a sequence of images. **1997**, 33, 1617

1439 New VLSI architectures of RSA public-key cryptosystem. 6

1438 Byzantine quorum systems. **1997**, 68

1437 Enhancing workflows by web technology. **1997**, 7

1436 Fast modular multiplications based on precomputations with less memory. **1997**, 33, 1370

1435 Secure distributed storage and retrieval. **1997**, 275-289 10

1434 A bit-serial systolic algorithm and VLSI implementation for RSA. 1

1433 Network and data security design for telemedicine applications. **1997**, 22, 133-42 13

1432 Network access and data security design for telemedicine applications. 3

1431 Secure official document mail systems for office automation. 0

1430	Algorithms for multi-exponentiation based on complex arithmetic.	1
1429	Hierarchical organization of certification authorities for secure environments.	2
1428	An embedded cryptosystem for digital broadcasting.	
1427	Optimized authenticated self-synchronizing Byzantine agreement protocols.	0
1426	Parallel computation of the multi-exponentiation for cryptosystems. **1997**, 63, 9-26	13
1425	Efficient and secure conference-key distribution. **1997**, 119-129	34
1424	Augmented encrypted key exchange using RSA encryption.	1
1423	Music on the Internet and the intellectual property protection problem.	10
1422	An intelligent mobile agent framework for distributed network management.	2
1421	Intranet security: an increasing concern in industrial environments.	
1420	The prevalence of kleptographic attacks on discrete-log based cryptosystems. **1997**, 264-276	45
1419	Identity-based and self-certified key-exchange protocols. **1997**, 303-313	18
1418	Consumer devices for networked audio.	1
1417	Secure rewarding schemes.	1
1416	Sliding encryption: A cryptographic tool for mobile agents. **1997**, 230-241	15
1415	Implementing block ciphering algorithms in hardware. **1997**, 83, 581-598	1
1414	Data Structures and Algorithms. **1997**,	2
1413	On using Carmichael numbers for public key encryption systems. **1997**, 265-269	

1412	.	2
1411	High assurance engineering: the good, the bad, and the ugly.	
1410	Improvement to Nyang-Song fast digital signature scheme. **1997**, 33, 1861	2
1409	A joint authorisation scheme. **1997**, 31, 88-96	
1408	Protection of data and delegated keys in digital distribution. **1997**, 271-282	
1407	Design of CSCW applications for medical teleconsultation and remote diagnosis support. **1997**, 22, 121-32	11
1406	On the foundations of modern cryptography. **1997**, 46-74	17
1405	Fast encryption of image data using chaotic Kolmogorov flows. **1997**,	4
1404	A one way function based on ideal arithmetic in number fields. **1997**, 385-394	4
1403	Proactive RSA. **1997**, 440-454	73
1402	Efficient elliptic curve exponentiation. **1997**, 282-290	40
1401	A new and optimal chosen-message attack on RSA-type cryptosystems. **1997**, 302-313	3
1400	On weak RSA-keys produced from pretty good privacy. **1997**, 314-324	
1399	Hiding the hidden: A software system for concealing ciphertext as innocuous text. **1997**, 335-345	47
1398	RSA-type signatures in the presence of transient faults. **1997**, 155-160	18
1397	On the security of the KMOV public key cryptosystem. **1997**, 235-248	13
1396	Efficient scalable fair cash with off-line extortion prevention. **1997**, 463-477	11
1395	Cryptographic permutations based on BOOT decompositions of walsh matrices. **1997**, 580-590	

1394	Design and implementation of a coprocessor for cryptography applications.	8
1393	A multiplicative attack using LLL algorithm on RSA signatures with redundancy. **1997**, 221-234	10
1392	Security of blind digital signatures. **1997**, 150-164	118
1391	Fast RSA-type cryptosystems using n-adic expansion. **1997**, 372-384	12
1390	An efficient message authentication scheme for link state routing.	37
1389	Provable security for cryptographic protocols-exact analysis and engineering applications.	3
1388	Trapdoor one-way permutations and multivariate polynomials. **1997**, 356-368	36
1387	Control of Information Distribution and Access. **1997**, 44, 219-283	
1386	New directions in cryptography: twenty some years later (or cryptograpy and complexity theory: a match made in heaven).	5
1385	Digital signatures. Whom do you trust?.	1
1384	On certificate-based security protocols for wireless mobile communication systems. **1997**, 11, 50-55	14
1383	Optimal-resilience proactive public-key cryptosystems.	71
1382	VLSI implementation of modulo multiplication using carry free addition.	
1381	Normalisation in diminished-radix modulus transformation. **1997**, 33, 1931	6
1380	An encryption scheme for high speed passive optical networks.	
1379	Remote electronic gambling.	9
1378	. **1997**, 11, 30-33	2
1377	.	40

1376 Access control in wide-area networks.

1375 An improved e-mail security protocol. 7

1374 A flexible security model for using Internet content. 1

1373 An RNS Montgomery modular multiplication algorithm. 8

1372 Public watermarks and resistance to tampering. 61

1371 Digital signal processing techniques and architectures in secure facsimile communications.

1370 Secure reliable multicast protocols in a WAN. 9

1369 Cryptographic key recovery. 0

1368 Building trust for distributed commerce transactions. 3

1367 A fast modular exponentiation for rsa on systolic arrays. **1997**, 63, 215-226

1366 On-line error detection for finite field multipliers. 1

1365 Reducing the cost of security in link-state routing. 23

1364 Reliable processing on the Seljuk-Amoeba operating environment.

1363 Selective Forgery of RSA Signatures Using Redundancy. **1997**, 495-507 14

1362 Space/time trade-offs for higher radix modular multiplication using repeated addition. **1997**, 46, 139-141 20

1361 O(n)-depth modular exponentiation circuit algorithm. **1997**, 46, 701-704 2

1360 Security issues in networks with Internet access. **1997**, 85, 2034-2051 19

1359 A flexible security system for using Internet content. **1997**, 14, 52-59 13

1358	Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. **1997**, 26, 1484-1509	3588
1357	IEEE P1363: A standard for RSA, Diffie-Hellman, and Elliptic-Curve cryptography (abstract). **1997**, 117-118	1
1356	Quantum information processing: The good, the bad and the ugly. **1997**, 337-341	1
1355	Public-key cryptosystems from lattice reduction problems. **1997**, 112-131	206
1354	Applying anti-trust policies to increase trust in a versatile e-money system. **1997**, 217-238	10
1353	VLSI array algorithms and architectures for RSA modular multiplication. **1997**, 5, 211-217	29
1352	.	122
1351	Seamless integration of online services in the Oberon document system. **1997**, 366-379	
1350	Plug and play encryption. **1997**, 75-89	41
1349	Fail-Stop Signatures. **1997**, 26, 291-330	39
1348	Efficient group signature schemes for large groups. **1997**, 410-424	502
1347	Explicit communication revisited: two new attacks on authentication protocols. **1997**, 23, 185-186	15
1346	Using CSP to detect errors in the TMN protocol. **1997**, 23, 659-669	90
1345	An Implementable scheme for secure delegation of computing and data. **1997**, 445-451	1
1344	A high-throughput secure reliable multicast protocol. **1997**, 5, 113-127	24
1343	Digital signature and public key cryptosystem in a prime order subgroup of Zn*. **1997**, 346-355	2
1342	How to sign digital streams. **1997**, 180-197	134
1341	Two efficient RSA multisignature schemes. **1997**, 217-222	10

1340 Dual basis systolic multipliers for GF(2m). **1997**, 144, 43 28

1339 Efficient cheater identification method for threshold schemes. **1997**, 144, 23 22

1338 Elliptic curve cryptosystems using curves of smooth order over the ring Z/sub n/. **1997**, 43, 1231-1237 19

1337 ATM cell encryption and key update synchronization. **1997**, 7, 391-408 1

1336 Von der empirischen zur abstrakten Kryptographie. **1997**, 114, 729-741

1335 FAPKC3: A new finite automaton public key cryptosystem. **1997**, 12, 289-305 9

1334 A chosen message attack on Demytko elliptic curve cryptosystem. **1997**, 10, 71-72 8

1333 Batch RSA. **1997**, 10, 75-88 47

1332 Batch Diffie-Hellman key agreement systems. **1997**, 10, 89-96 3

1331 The security of the birational permutation signature schemes. **1997**, 10, 207-221 33

1330 Elliptic curve cryptosystem The answer to strong, fast public-key cryptography for securing constrained environments. **1997**, 2, 78-87 39

1329 Speeding up the computations of elliptic curves cryptoschemes. **1997**, 33, 29-36 3

1328 A generalized secret sharing scheme. **1997**, 36, 267-272 3

1327 The code makers. **1997**, 16, 1-9 1

1326 Remote auditing of software outputs using a trusted coprocessor. **1997**, 13, 9-18 12

1325 Protection of software algorithms executed on secure modules. **1997**, 13, 55-63 1

1324 Multi-application smart cards and encrypted data, processing. **1997**, 13, 65-74 9

1323 Image compression and encryption using tree structures. **1997**, 18, 1253-1259 48

1322	Multilevel secure database encryption with subkeys. **1997**, 22, 117-131	9
1321	ID-based group-oriented cryptosystem and its digital signature scheme. **1997**, 20, 1019-1026	1
1320	Artificial intelligence approaches to network management: recent advances and a survey. **1997**, 20, 1313-1322	22
1319	Three ID-based information security functions. **1997**, 20, 1301-1307	1
1318	Authenticated key-exchange in a mobile radio network. **1997**, 8, 265-269	10
1317	An integrated co-processor architecture for a smartcard. **1997**, 20, 323-337	
1316	Evidence and non-repudiation. **1997**, 20, 267-281	43
1315	A variant of the public key cryptosystem FAPKC3. **1997**, 20, 283-303	7
1314	On the Clark-Jacob version of SPLICE/AS. **1997**, 62, 251-254	3
1313	A simple approach for generating RSA keys. **1997**, 63, 19-21	2
1312	Authenticated encryption schemes with linkage between message blocks. **1997**, 63, 247-250	23
1311	An active attack on protocols for server-aided RSA signature computation. **1998**, 65, 71-73	2
1310	A common-multiplicand method to the montgomery algorithm for speeding up exponentiation. **1998**, 66, 105-107	28
1309	Reducing the Elliptic Curve Cryptosystem of Meyer-Müller to the Cryptosystem of Rabin-Williams. **1998**, 14, 53-56	
1308	Unconditionally Secure Group Authentication. **1998**, 14, 281-296	7
1307	A comparative overview ofcryptographic voting protocols. **1998**, 84, 29-43	
1306	Some Consequences of Cryptographical Conjectures forS12and EF. **1998**, 140, 82-94	88
1305	Digital signatures. **1998**, 2, 12-22	2

1304 Comparison of MPEG encryption algorithms. **1998**, 22, 437-448 118

1303 Anonymous mechanisms in group decision support systems communication. **1998**, 23, 297-328 23

1302 Teleworks: a CSCW application for remote medical diagnosis support and teleconsultation. **1998**, 2, 62-73 23

1301 Minimising the risk of electronic document forgery. **1998**, 19, 161-167

1300 How to ensure data security of an epidemiological follow-up: quality assessment of an anonymous record linkage procedure. **1998**, 49, 117-22 67

1299 Signature schemes based on factoring and discrete logarithms. **1998**, 145, 33 18

1298 Cryptanalysis and improvement of signcryption schemes. **1998**, 145, 149 37

1297 Fast algorithm for modular reduction. **1998**, 145, 265 22

1296 Two integrated schemes of user authentication and access control in a distributed computer network. **1998**, 145, 419 7

1295 A Survey of Fast Exponentiation Methods. **1998**, 27, 129-146 334

1294 A high-speed public key encryption processor. **1998**, 29, 20-32

1293 Byzantine quorum systems. **1998**, 11, 203-213 225

1292 □ +□: four different views. **1998**, 20, 55-60 2

1291 Security for the digital information age of medicine: issues, applications, and implementation. **1998**, 11, 33-44 15

1290 Optical detection of random features for high security applications. **1998**, 147, 173-179 25

1289 Using RSA with low exponent in a public network. **1998**, 21, 284-286 2

1288 Authenticity of public keys in asymmetric cryptosystems. **1998**, 21, 195-198

1287 Secure broadcasting in large networks. **1998**, 21, 279-283 3

1286	Threshold signature schemes with traceable signers in group communications. **1998**, 21, 771-776	32
1285	An on-line secret sharing scheme for multi-secrets. **1998**, 21, 1170-1176	40
1284	Implementation and timing analysis of Clock Synchronization on a transputer-based replicated system. **1998**, 40, 291-309	3
1283	Univariate polynomial factorization over finite fields. **1998**, 191, 1-36	5
1282	Paramita wisdom password authentication scheme without verification tables. **1998**, 42, 45-57	36
1281	An adaptive exponentiation method. **1998**, 42, 59-69	3
1280	RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography. **1998**, 17, 637-650	9
1279	A framework for the management of information security. **1998**, 232-245	2
1278	Copyright labeling of digitized image data. **1998**, 36, 94-100	18
1277	A pipelined architecture of fast modular multiplication for RSA cryptography.	2
1276	New Chinese remainder theorems.	21
1275	Protecting Java code via code obfuscation. **1998**, 4, 21-23	28
1274	Vicarious certification and billing agent for Web information service.	
1273	The security of individual RSA bits.	5
1272	The Solar Trust Model: authentication without limitation.	6
1271	ID-based cryptographic schemes using a non-interactive public-key distribution system.	3
1270	A share assignment method to maximize the probability of secret sharing reconstruction under the Internet.	
1269	A public key watermark for image verification and authentication.	11

1268 Electronic exchange check system on the Internet.

1267 A certified e-mail protocol. 11

1266 Implementation of RSA cryptoprocessor based on Montgomery algorithm. 3

1265 A pseudonymous joint signature scheme.

1264 A new public-key cryptosystem as secure as factoring. **1998**, 308-318 314

1263 A smartcard-based framework for secure document exchange. 0

1262 Breaking RSA may not be equivalent to factoring. **1998**, 59-71 117

1261 Provable security for block ciphers by decorrelation. **1998**, 249-275 49

1260 Securing threshold cryptosystems against chosen ciphertext attack. **1998**, 1-16 116

1259 Group blind digital signatures: A scalable solution to electronic cash. **1998**, 184-197 84

1258 Surf NCSign: Client signatures on Web documents. **1998**, 37, 61-71 3

1257 An RNS Montgomery modular multiplication algorithm. **1998**, 47, 766-776 84

1256 Design of a high-speed square generator. **1998**, 47, 1021-1026 7

1255 An energy/security scalable encryption processor using an embedded variable voltage DC/DC converter. **1998**, 33, 1799-1809 34

1254 Real-time mixes: a bandwidth-efficient anonymity protocol. **1998**, 16, 495-509 53

1253 Some general methods for tampering with watermarks. **1998**, 16, 587-593 124

1252 Stop- and- Go-MIXes Providing Probabilistic Anonymity in an Open System. **1998**, 83-98 130

1251 A new RSA cryptosystem hardware design based on Montgomery's algorithm. **1998**, 45, 908-913 42

1250	A new public key cryptosystem based on higher residues. **1998**,	162
1249	Cryptographic Primitives for Information Authentication State of the Art. **1998**, 49-104	13
1248	State of the Art in Applied Cryptography. **1998**,	
1247	Digital patient assistants: privacy vs cost in compulsory health insurance. **1998**, 4, 138-156	1
1246	Fast digital identity revocation. **1998**, 137-152	53
1245	Remarks on blind decryption. **1998**, 109-115	
1244	An Attack on RSA Given a Small Fraction of the Private Key Bits. **1998**, 25-34	97
1243	Signature scheme based on discrete logarithm without using one-way hash function. **1998**, 34, 1079	5
1242	Batch verifying multiple RSA digital signatures. **1998**, 34, 1219	42
1241	A secure electronic market for anonymous transferable emission permits.	
1240	Fast RSA-type cryptosystem modulo pkq. **1998**, 318-326	81
1239	Applied Abstract Algebra. **1998**,	28
1238	Cryptography, quantum computation and trapped ions. **1998**, 356, 1853-1868	10
1237	Key establishment protocols for secure mobile communications: A selective survey. **1998**, 344-355	25
1236	Security of ID-based key exchange scheme. **1998**, 34, 653	
1235	Batch verifying multiple DSA-type digital signatures. **1998**, 34, 870	32
1234	Optimal efficiency of optimistic contract signing. **1998**,	33
1233	Extended analogy. **1998**,	8

1232	Key management for encrypted broadcast. **1998**,	7
1231	An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products. **1998**,	34
1230	Optimisation of Montgomery modular multiplication algorithm for systolic arrays. **1998**, 34, 1830	4
1229	BACK MATTER. **1998**, 381-400	
1228	Two facets of authentication.	4
1227	Identity-based non-interactive key sharing equivalent to RSA public-key cryptosystem.	0
1226	SG logic a formal analysis technique for authentication protocols. **1998**, 159-176	1
1225	A protocol for billing mobile network access devices operating in foreign networks.	
1224	.	
1223	Survivable consensus objects.	1
1222	Literatur. 311-319	
1221	NTRU: A ring-based public key cryptosystem. **1998**, 267-288	663
1220	Making benchmarks uncheatable.	2
1219	A SAFE AND SCALABLE PAYMENT INFRASTRUCTURE FOR TRADE OF ELECTRONIC CONTENT. **1998**, 07, 331-354	2
1218	Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults. **1998**, 115-124	55
1217	Digital signatures for flows and multicasts.	13
1216	Advances in Cryptology ASIACRYPT 98. **1998**,	7
1215	Efficient Elliptic Curve Exponentiation Using Mixed Coordinates. **1998**, 51-65	197

1214	Divertible protocols and atomic proxy cryptography. **1998**, 127-144	585
1213	Key schedules of iterative block ciphers. **1998**, 80-89	4
1212	Secure Information Gathering Agent for Internet Trading. **1998**, 183-193	3
1211	Key Distribution and Authentication Protocol for Secure Wireless Conferencing. **1998**, 15, 471-476	
1210	Hippocrates: an integrated platform for telemedicine applications. **1998**, 23, 265-76	3
1209	A novel digit-serial systolic array for modular multiplication.	2
1208	Key recovery and confidentiality oops, where did I put that key?.	
1207	The SecureRing protocols for securing group communication.	64
1206	A Web-based secure system for the distributed printing of documents and images.	
1205	Inline network encryption for multimedia wireless LANs.	
1204	Optimised bit serial modular multiplier for implementation on field programmable gate arrays. **1998**, 34, 738	5
1203	Cryptanalysis of message authentication codes. **1998**, 55-65	4
1202	ID-based secret-key cryptography. **1998**, 32, 33-39	5
1201	Securing confidentiality in PON and HFC networks. **1998**,	
1200	Fast algorithm for finding a small root of a quadratic modular equation. **1998**, 75-81	
1199	A high-speed small RSA encryption LSI with low power dissipation. **1998**, 174-187	3
1198	On private-key cryptosystems based on product codes. **1998**, 68-79	6
1197	The inductive approach to verifying cryptographic protocols. **1998**, 6, 85-128	524

1196 Strength of two Data Encryption Standard implementations under timing attacks. **1998**, 192-205 3

1195 Flexible internet secure transactions based on collaborative domains. **1998**, 37-51

1194 On finding small solutions of modular multivariate polynomial equations. **1998**, 158-170 20

1193 An address resolution and key exchange protocol for conferencing applications on the Internet. **1998**, 47-58

1192 Batch verification with applications to cryptography and checking. **1998**, 170-191 16

1191 Long operand arithmetic on instruction systolic computer architectures and its application in RSA cryptography. **1998**, 916-922 6

1190 Optimistic fair exchange of digital signatures. **1998**, 591-606 167

1189 Group signatures for hierarchical multigroups. **1998**, 273-281 11

1188 Protocol failures related to order of encryption and signature computation of discrete logarithms in RSA groups. **1998**, 238-249 2

1187 Distributed Trustees and revocability: A framework for internet payment. **1998**, 28-42 3

1186 The security of public key cryptosystems based on integer factorization. **1998**, 9-23 2

1185 Strengthened security for blind signatures. **1998**, 391-405 32

1184 Generic constructions for secure and efficient confirmer signature schemes. **1998**, 406-421 27

1183 Distributed public key cryptosystems. **1998**, 1-13 15

1182 Guaranteed correct sharing of integer factorization with off-line shareholders. **1998**, 60-71 23

1181 On concrete security treatment of signatures derived from identification. **1998**, 354-369 55

1180 A secure intelligent trade agent system. **1998**, 218-228 2

1179 LITESET: A light-weight secure electronic transaction protocol. **1998**, 215-226 5

1178	On the security of some variants of the RSA signature scheme. **1998**, 85-96	2
1177	Barter: A backbone architecture for trade of electronic content. **1998**, 65-79	2
1176	A key escrow system with protecting user's privacy by blind decoding. **1998**, 147-157	4
1175	Kolmogorov systems: Internal time, irreversibility and cryptographic applications. **1998**,	1
1174	Provable security for cryptographic protocols exact analysis and engineering applications. **1998**, 6, 23-52	
1173	A payment scheme using vouchers. **1998**, 103-121	3
1172	On the Cryptographic Value of the qth Root Problem. **1999**, 135-142	
1171	On the fly signatures based on factoring. **1999**,	15
1170	Efficient verifiable encryption (and fair exchange) of digital signatures. **1999**,	71
1169	Handbook of Applied Cryptography. By Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet. By Shawn James Rosenheim. **1999**, 106, 85-88	
1168	On the Design of RSA with Short Secret Exponent. **1999**, 150-164	20
1167	Scalable multicast security in dynamic groups. **1999**,	23
1166	Facsimile Equipment. **1999**,	
1165	Number Theory. **1999**,	
1164	Data Security. **1999**,	5
1163	Parallel modular multiplication with application to VLSI RSA implementation.	3
1162	A public key system with signature and master key functions. **1999**, 27, 2207-2222	60
1161	Cryptography: A Survey. **1999**, 16, 287-296	

1160	Tactical network security.	1
1159	An efficient VLSI architecture for RSA public-key cryptosystem.	0
1158	An infrastructure for distributed and dynamic network management based on mobile agent technology.	18
1157	A unified method for iterative computation of modular multiplication and reduction operations.	5
1156	Factorization of RSA-140 Using the Number Field Sieve. **1999**, 195-207	12
1155	The design space layer. **1999**,	3
1154	Confined types. **1999**,	40
1153	A Signature Scheme with Message Recovery as Secure as Discrete Logarithm. **1999**, 378-389	16
1152	Handbook of Applied Crytography.. **1999**, 106, 85	1
1151	Emperor. **1999**,	0
1150	Identification scheme based on Shamir's RSA for paranoids. **1999**, 35, 1941	1
1149	Strength of two data encryption standard implementations under timing attacks. **1999**, 2, 416-437	15
1148	Design and implementation of a distributed virtual machine for networked computers. **1999**,	33
1147	Confined types. **1999**, 34, 82-96	9
1146	The State of Cryptographic Hash Functions. **1999**, 158-182	25
1145	Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries. **1999**, 165-179	69
1144	Cryptanalysis of RSA with Private Key d Less than N0.292. **1999**, 1-11	50
1143	Moduli for testing implementations of the RSA cryptosystem.	1

1142	Simulating the Effect of Decoherence and Inaccuracies on a Quantum Computer. **1999**, 447-459	6
1141	A Self-Certified Group-Oriented Cryptosystem without a Combiner. **1999**, 192-201	3
1140	A dual encryption protocol for scalable secure multicasting.	16
1139	Certified exchange of electronic mail (CEEM).	
1138	A new public-key cryptosystem family based on feedback shift registers.	
1137	A real-time protocol for stock market transactions.	
1136	Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. **1999**, 223-238	2580
1135	.	
1134	Unconditional Security in Cryptography. **1999**, 217-250	6
1133	Web-Based Chronobiological Analysis. **1999**, 30, 477-496	1
1132	Key-Dependent S-Box Manipulations. **1999**, 15-26	1
1131	Factorization of the tenth Fermat number. **1999**, 68, 429-452	13
1130	Secure audit logs to support computer forensics. **1999**, 2, 159-176	218
1129	Public Key Cryptography. **1999**,	1
1128	Encrypted Message Authentication by Firewalls. **1999**, 69-81	43
1127	Efficient certificate status handling within PKIs: an application to public administration services.	3
1126	Signature management in workflow systems.	3
1125	Security and authentication in PCS. **1999**, 25, 225-248	14

1124 The Korean certificate-based digital signature algorithm. **1999**, 25, 249-265 4

1123 Boolean permutation-based key escrow. **1999**, 25, 291-304 1

1122 On private-key encryption using product codes. **1999**, 25, 439-450

1121 Partially blind threshold signatures based on discrete logarithm. **1999**, 22, 73-86 13

1120 A secure and practical electronic voting scheme. **1999**, 22, 279-286 13

1119 A fast modular multiplication method based on the Lempel□iv binary tree. **1999**, 22, 871-874 2

1118 Anonymous channel and authentication in wireless communications. **1999**, 22, 1502-1511 34

1117 Decentralized group key management for secure multicast communications. **1999**, 22, 1183-1187 9

1116 Padding attacks on RSA. **1999**, 4, 28-33

1115 Secure and lightweight advertising on the Web. **1999**, 31, 1101-1109 15

1114 On finite automaton public-key cryptosystem. **1999**, 226, 143-172 3

1113 A concept of designing cheater identification methods for secret sharing. **1999**, 46, 7-11 10

1112 Achieving non-repudiation of Web based transactions. **1999**, 48, 165-175 2

1111 Analytical performance evaluation of nested certificates. **1999**, 36-37, 213-232 4

1110 Hash-based encryption system. **1999**, 18, 345-350 10

1109 Enforcing network security: a real cease study in a research organization. **1999**, 18, 533-543 1

1108 Password authentication schemes with smart cards. **1999**, 18, 727-733 180

1107 Analysis of the variable length nonzero window method for exponentiation. **1999**, 37, 21-29 6

1106	Fast group operations on elliptic curves in Maple. **1999**, 37, 129-138	
1105	A method for computing Lucas sequences. **1999**, 38, 187-196	3
1104	A new model of security for metasystems. **1999**, 15, 713-722	8
1103	Broadcasting cryptosystem in computer networks. **1999**, 37, 85-87	8
1102	A fast modular multiplication algorithm for calculating the product AB modulo N. **1999**, 72, 77-81	2
1101	A probability model for reconstructing secret sharing under the internet environment. **1999**, 116, 109-127	8
1100	A novel ID-based group signature. **1999**, 120, 131-141	10
1099	A Calculus for Cryptographic Protocols: The Spi Calculus. **1999**, 148, 1-70	484
1098	Function Field Sieve Method for Discrete Logarithms over Finite Fields. **1999**, 151, 5-16	49
1097	Experimental measurements and design guidelines for real-time software encryption in multimedia wireless LANs. **1999**, 2, 35-43	1
1096	Efficient Rabin-type Digital Signature Scheme. **1999**, 16, 53-64	10
1095	Chinese Remaindering Based Cryptosystems in the Presence of Faults. **1999**, 12, 241-245	104
1094	Fast direct computation of modular reduction. **1999**, 35, 507-515	0
1093	Public-key cryptosystems based on cubic finite field extensions. **1999**, 45, 2601-2605	64
1092	Dynamic participation in a secure conference scheme for mobile communications. **1999**, 48, 1469-1474	30
1091	Security of Shao's signature schemes based on factoring and discrete logarithms. **1999**, 146, 119	11
1090	Integrated approach for fault tolerance and digital signature in RSA. **1999**, 146, 151	9
1089	(t, n) threshold verifiable multisecret sharing scheme based on the factorisation intractability and discrete logarithm modulo a composite problems. **1999**, 146, 264	17

1088 A Web-Based Secure System for the Distributed Printing of Documents and Images. **1999**, 10, 1-11 52

1087 Synthesizers and Their Application to the Parallel Construction of Pseudo-Random Functions. **1999**, 58, 336-375 64

1086 An Improvement on a Practical Secret Voting Scheme. **1999**, 225-234 30

1085 Lectures on Data Security. **1999**, 4

1084 Transport layer security: how much does it really cost?. **1999**, 56

1083 Secure Integration of Asymmetric and Symmetric Encryption Schemes. **1999**, 537-554 444

1082 How to Enhance the Security of Public-Key Encryption at Minimum Cost. **1999**, 53-68 129

1081 Verification of classical certificates via nested certificates and nested certificate paths. 2

1080 A remote password authentication scheme based on the digital signature method. **1999**, 70, 657-666 27

1079 Improving fairness and privacy of Zhou-Gollmann's fair non-repudiation protocol. 1

1078 Towards a scalable PKI for electronic commerce systems.

1077 Controlling the dissemination of electronic documents. **1999**, 1

1076 Montgomery modular exponentiation on reconfigurable hardware. 75

1075 . 2

1074 TrustedBox: a kernel-level integrity checker. 3

1073 Safe areas of computation for secure computing with insecure applications. 1

1072 Montgomery modular multiplication and exponentiation in the residue number system. 2

1071 Proving security protocols correct. 5

1070	Design of LAN-Lock, a system for securing wireless networks.	
1069	COPS: a model and infrastructure for secure and fair electronic markets.	4
1068	Quantum computing for beginners.	23
1067	Real-time aware protocols for general e-commerce and electronic auction transactions.	2
1066	Distributing mobility agents hierarchically under frequent location updates.	16
1065	Certificate revocation the responsible way.	4
1064	The design space layer: supporting early design space exploration for core-based designs.	1
1063	Providing support for survivable CORBA applications with the Immune system.	10
1062	Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. **1999**, 41, 303-332	934
1061	A Pseudorandom Generator from any One-way Function. **1999**, 28, 1364-1396	876
1060	The Relationship Between Breaking the Diffie--Hellman Protocol and Computing Discrete Logarithms. **1999**, 28, 1689-1721	93
1059	An improved Montgomery's algorithm for high-speed RSA public-key cryptosystem. **1999**, 7, 280-284	22
1058	Modern Cryptography, Probabilistic Proofs and Pseudorandomness. **1999**,	90
1057	.	
1056	On the Security Properties of OAEP as an All-or-Nothing Transform. **1999**, 503-518	38
1055	Differential Power Analysis. **1999**, 388-397	2834
1054	Cryptanalysis of an authentication and key distribution protocol. **1999**, 3, 7-8	3
1053	Authentication protocols with nonrepudiation services in personal communication systems. **1999**, 3, 236-238	20

1052 The VersaKey framework: versatile group key management. **1999**, 17, 1614-1631 155

1051 The use of watermarks in the protection of digital multimedia products. **1999**, 87, 1197-1207 112

1050 . **1999**, 7, 502-513 113

1049 Safe primes density and cryptographic applications.

1048 Understanding Contemporary Cryptography and its Wider Impact upon the General Law. **1999**, 13, 95-126 6

1047 Results of an elliptic-curve-approach for use in cryptosystems. **1999**,

1046 Design and implementation of an RSA public-key cryptosystem.

1045 Toward an FPGA architecture optimized for public-key algorithms. **1999**, 7

1044 High-confidence design for security. *Communications of the ACM*, **1999**, 42, 33-37 2.5 76

1043 A VLSI architecture of fast high-radix modular multiplication for RSA cryptosystem.

1042 Modular exponential accelerator chip based on precomputations for RSA cryptography application. **1999**,

1041 Design and implementation of a distributed virtual machine for networked computers. **1999**, 33, 202-216 3

1040 Securing the anonymity of content providers in the World Wide Web. **1999**, 6

1039 Digital signature management. **1999**, 9, 262-271 2

1038 Context-agile encryption for high speed communication networks. **1999**, 29, 35-49 8

1037 Security of broadcasting cryptosystem in computer networks. **1999**, 35, 2108 4

1036 Mathematical Models in Public-Key Cryptology. **1999**,

1035 Software agent-mediated confidential information gathering system.

1034	Internet-based operations for the Mars Polar Lander mission.	19
1033	Secret and public key authentication watermarking schemes that resist vector quantization attack. **2000**, 3971, 417	26
1032	On the validity of digital signatures. **2000**, 30, 29-34	8
1031	Group communication security on regional PC communication networks. **2000**, 83, 10-19	0
1030	A new fast modular multiplication method and its application to modular exponentiation-based cryptography. **2000**, 83, 88-93	5
1029	Public key watermarking for authentication of CSG models. **2000**, 32, 727-735	33
1028	Efficient construction of vote-tags to allow open objection to the tally in electronic elections. **2000**, 75, 211-215	8
1027	Partitioned systolic architecture for modular multiplication in. **2000**, 76, 135-139	1
1026	Linear systolic multiplier/squarer for fast exponentiation. **2000**, 76, 105-111	16
1025	On the construction of a powerful distributed authentication server without additional key management. **2000**, 23, 1638-1644	
1024	Randomization enhanced Chaum's blind signature scheme. **2000**, 23, 1677-1680	23
1023	MNPA: a mobile network privacy architecture. **2000**, 23, 1777-1788	5
1022	Key establishment protocols for secure mobile communications: a critical survey. **2000**, 23, 575-587	10
1021	MicroISPs: providing convenient and low-cost high-bandwidth Internet access. **2000**, 33, 789-802	6
1020	The Italian academic community's electronic voting system. **2000**, 34, 851-860	3
1019	Scaling issues in large PKI communities. **2000**, 16, 361-372	
1018	Secure distributed storage and retrieval. **2000**, 243, 363-389	44
1017	A traceable group signature scheme. **2000**, 31, 147-160	2

1016 ElGamal-like digital signature and multisignature schemes using self-certified public keys. **2000**, 50, 99-105 18

1015 A Generic Electronic Payment Model Supporting Multiple Merchant Transactions. **2000**, 19, 453-465 2

1014 Generation of RSA Keys That Are Guaranteed to be Unique for Each User. **2000**, 19, 282-288 1

1013 Fast BBS-sequence generation using Montgomery multiplication. **2000**, 147, 252 4

1012 Improved linear systolic array for fast modular exponentiation. **2000**, 147, 323 12

1011 Security of the Jan-Tseng integrated schemes for user authentication and access control. **2000**, 147, 365 2

1010 Cryptanalysis of RSA with private key d less than N/sup 0.292/. **2000**, 46, 1339-1349 189

1009 Authentication theory and hypothesis testing. **2000**, 46, 1350-1356 99

1008 Digital multisignature schemes for authenticating delegates in mobile code systems. **2000**, 49, 1464-1473 23

1007 COPS: a model and infrastructure for secure and fair electronic markets. **2000**, 29, 343-355 11

1006 The DiffieHellman Protocol. **2000**, 19, 147-171 48

1005 Information Security, Mathematics, and Public-Key Cryptography. **2000**, 19, 77-99 5

1004 Supporting the Distributed German Government with POLITeam. **2000**, 12, 39-58 2

1003 Chain authentication in mobile communication systems. **2000**, 13, 213-240 1

1002 A new forgery attack on message recovery signatures. **2000**, 17, 234-237 0

1001 Security Arguments for Digital Signatures and Blind Signatures. **2000**, 13, 361-396 1245

1000 A New Public-Key Cryptosystem over a Quadratic Order with Quadratic Decryption Time. **2000**, 13, 263-272 19

999 The multi-dimension RSA and its low exponent security. **2000**, 43, 349-354 6

998	Input-trees of finite automata and application to cryptanalysis. **2000**, 15, 305-325	3
997	Secure reliable multicast protocols in a WAN. **2000**, 13, 19-28	5
996	Algebraic Aspects of Cryptography. By Neal Koblitz. **2000**, 107, 384-386	
995	Advances in Cryptology EUROCRYPT 2000. **2000**,	5
994	Lattice Reduction in Cryptology: An Update. **2000**, 85-112	40
993	Practical Threshold Signatures. **2000**, 207-220	273
992	Adaptability in CORBA: the mobile proxy approach.	2
991	Recent Progress and Prospects for Integer Factorisation Algorithms. **2000**, 3-22	19
990	Secure Transactions with Mobile Agents in Hostile Environments. **2000**, 289-297	29
989	Information Security and Privacy. **2000**,	2
988	Advances in Cryptology ASIACRYPT 2000. **2000**,	7
987	Web-Age Information Management. **2000**,	12
986	Smart Card Crypto-Coprocessors for Public-Key Cryptography. **2000**, 372-379	17
985	Key management for encrypted broadcast. **2000**, 3, 107-134	13
984	Optimized squaring with sliding windows.	3
983	An expandable Montgomery modular multiplication processor. **2000**,	3
982	Bilateral anonymity and prevention of abusing logged Web addresses.	1
981	Public key cryptography. **2000**, 7, 14-22	5

980 Efficient Design of ENCA Based Cipher System. **2000**, 46, 163-173 1

979 Privacy-preserving global customization. **2000**, 15

978 Scalable multicast security with dynamic recipient groups. **2000**, 3, 136-160 19

977 Radix-4 modular multiplication and exponentiation algorithms for the RSA public-key cryptosystem. **2000**, 12

976 Secure and linear cryptosystems using error-correcting codes. **2000**, 51, 244-244 4

975 Construction and Categories of Codes. **2000**, 266-277

974 Public key cryptosystems based on boolean permutations and their applications. **2000**, 74, 167-184 5

973 Multiparty authenticative mechanisms for network-mediated document-object conferencing and collaborative processing.

972 Advances in Cryptology CRYPTO 2000. **2000**, 44

971 Image authentication and integrity verification via content-based watermarks and a public key cryptosystem.

970 Number Theory. **2000**, 1

969 An architecture for survivable coordination in large distributed systems. **2000**, 12, 187-202 47

968 Quantum entanglement using trapped atomic spins. **2000**, 62, 43

967 Residue-to-binary converters based on new Chinese remainder theorems. **2000**, 47, 197-205 86

966 An asymmetric cryptographuic key assignment scheme for access control in totally-ordered hierarchies *. **2000**, 73, 463-468 8

965 Information Security and Cryptology - ICISC 99. **2000**, 6

964 Selected Areas in Cryptography. **2000**, 4

963 State of the art in electronic payment systems. **2000**, 53, 425-449 12

962	Smart Card Research and Applications. **2000**,	2
961	REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. **2000**, 159-174	106
960	A New and Efficient Fail-stop Signature Scheme. **2000**, 43, 430-437	12
959	Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99. **2000**, 14-29	33
958	Fairness and privacy on pay-per view system for Web-based video service. **2000**, 46, 980-985	2
957	Further cryptanalysis of the McEliece public-key cryptosystem. **2000**, 4, 18-19	5
956	Secure cookies on the Web. **2000**, 4, 36-44	60
955	A Group Signature Scheme with Improved Efficiency (Extended Abstract). **2000**, 160-174	67
954	Some guidelines for non-repudiation protocols. **2000**, 30, 29-38	19
953	Nonmalleable Cryptography. **2000**, 30, 391-437	526
952	Partial encryption of compressed images and videos. **2000**, 48, 2439-2451	306
951	Efficient Generation of Prime Numbers. **2000**, 340-354	24
950	The RSA Public Key Cryptosystem. **2000**, 101-123	8
949	A Survey of Number Theory and Cryptography. **2000**, 217-239	6
948	Trapdooring Discrete Logarithms on Elliptic Curves over Rings. **2000**, 573-584	21
947	IEEE Standard Specifications for Public-Key Cryptography.	14
946	Modular multiplication in the residue number system with application to massively-parallel public-key cryptography systems.	3
945	A heuristic search based factoring tool.	

944	Multiple signature handling in workflow systems.	3
943	From crash fault-tolerance to arbitrary-fault tolerance: towards a modular approach.	12
942	Abstractions for devising Byzantine-resilient state machine replication.	5
941	Radix-4 modular multiplication and exponentiation algorithms for the RSA public-key cryptosystem.	
940	Utilization of multiple block cipher hashing in authentication and digital signatures.	
939	Modular exponentiation on fine-grained FPGA.	
938	A wearable public key infrastructure (WPKI).	0
937	Certified electronic mail protocol resistant to a minority of malicious third parties.	6
936	The Chinese Remainder Theorem and its application in a high-speed RSA crypto chip.	9
935	Ring-planarized cylindrical arrays with application to modular multiplication.	4
934	Performance-scalable array architectures for modular multiplication.	9
933	A scalable approach for subscription-based information commerce.	2
932	FPGA implementation of RSA public-key cryptographic coprocessor.	5
931	Methods and protocols for secure key negotiation using IKE. **2000**, 14, 18-29	2
930	.	
929	Security against compelled disclosure.	2
928	Securing electronic commerce: reducing the SSL overhead. **2000**, 14, 8-16	26
927	Design methodology for Booth-encoded Montgomery module design for RSA cryptosystem.	0

926	Itinerant Agents for Mobile Computing. **2000**, 3, 34-49	9
925	On multiple precision based Montgomery multiplication without precomputation of N'/sub 0/=-N/sub 0//sup -1/ mod W.	
924	Two systolic architectures for modular multiplication. **2000**, 8, 103-107	29
923	An efficient, dynamic and trust preserving public key infrastructure.	3
922	A systolic architecture for elliptic curve cryptosystems.	
921	Implementing 1,024-bit RSA exponentiation on a 32-bit processor core.	9
920	Network security (security in large networks).	1
919	Efficient authentication and signing of multicast streams over lossy channels.	311
918	Asynchronous implementation of 1024-bit modular processor for RSA cryptosystem.	
917	Cox-Rower Architecture for Fast Parallel Montgomery Multiplication. **2000**, 523-538	70
916	Asynchronous implementation of modular exponentiation for RSA cryptography.	
915	Applications in health care using public-key certificates and attribute certificates.	3
914	Complexity and fast algorithms for multiexponentiations. **2000**, 49, 141-147	34
913	Optimal left-to-right binary signed-digit recoding. **2000**, 49, 740-748	78
912	Checking before output may not be enough against fault-based cryptanalysis. **2000**, 49, 967-970	195
911	. **2000**, 4, 52-55	83
910	. **2000**, 18, 593-610	232
909	High-radix Montgomery modular exponentiation on reconfigurable hardware. **2001**, 50, 759-764	118

908	Techniques for the creation of digital watermarks in sequential circuit designs. **2001**, 20, 1101-1117	84
907	Two implementation methods of a 1024-bit RSA cryptoprocessor based on modified Montgomery algorithm.	9
906	An architecture for the Internet Key Exchange Protocol. **2001**, 40, 721-746	10
905	How to Leak a Secret. **2001**, 552-565	625
904	Trusted Information. **2001**,	0
903	Backoff protocols for distributed mutual exclusion and ordering.	16
902	PKI and digital certification infrastructure.	13
901	A 1024-bit RSA crypto-coprocessor for smart cards.	2
900	Trust and Deception in Virtual Societies. **2001**,	94
899	Technological infrastructure for PKI and digital certification. **2001**, 24, 1460-1471	10
898	Fast encryption for multimedia. **2001**, 47, 101-107	34
897	Fast VLSI arithmetic algorithms for high-security elliptic curve cryptographic applications. **2001**, 47, 700-708	12
896	DOCSIS/sup TM/ cable modem technology. **2001**, 39, 202-209	19
895	Hardware and software symbiosis helps smart card evolution. **2001**, 21, 14-25	25
894	Secret and public key image watermarking schemes for image authentication and ownership verification. **2001**, 10, 1593-601	334
893	A new RSA cryptosystem hardware implementation based on high-radix Montgomery's algorithm.	1
892	Multi-application smart card with elliptic curve cryptosystem certificate.	4
891	Improved ZDN-arithmetic for fast modulo multiplication.	

890	One-time installation with traitors tracing for copyright programs.	
889	Persistent objects in the Fleet system.	17
888	Design of portable mobile devices based e-payment system and e-ticketing system with digital signature.	2
887	Computer Aided Systems Theory EUROCAST 2001. **2001**,	2
886	Information Security. **2001**,	4
885	Untraceable off-line electronic cash flow in e-commerce.	6
884	Jini-enabled high performance computing.	1
883	A secure image coding scheme using residue number system.	9
882	Embedded core testing using broadcast test architecture.	
881	RSA cryptosystem design based on the Chinese remainder theorem.	1
880	Cryptography and relational database management systems.	11
879	.	4
878	Performance of finite field arithmetic in an elliptic curve cryptosystem.	
877	A buyer-seller watermarking protocol. **2001**, 10, 643-9	187
876	Modular multiplication and base extensions in residue number systems.	42
875	Securing distributed adaptation.	1
874	Cryptography in C and C++. **2001**,	2
873	Literaturverzeichnis. **2001**, 325-332	

872 Bibliography. **2001**, 271-274

871 Putting the Pieces Together: Using Off-The-Shelf Software to Safely Transfer Medical Data. **2001**, 40, 236-240

870 Reviews. **2001**, 108, 983-992

869 An Efficient Blind Signature Scheme for Information Hiding. **2001**, 6, 93-100 15

868 A Two-level Time-Stamping System. **2001**, 139-149 1

867 A Fair and Privacy-preserved Protocol for Sealed-bid Auctions. **2001**, 11, 163-170 0

866 Novel biometric digital signatures for Internet-based applications. **2001**, 9, 205-212 39

865 Defense and security of a wireless tactical network. **2001**,

864 A trustworthy Internet auction model with verifiable fairness. **2001**, 11, 159-166 6

863 Mathematics Unlimited 2001 and Beyond. **2001**, 23

862 Model calculations to estimate the probability of secret reconstruction in computer environments. **2001**, 9, 13-20

861 An Efficient Software Protection Scheme. **2001**, 385-401 10

860 One-time installation with traitors tracing for copyright programs. **2001**,

859 The Elliptic Curve Digital Signature Algorithm (ECDSA). **2001**, 1, 36-63 807

858 A course in number theory and cryptology. **2001**, 6, 91-94

857 Handling signature purposes in workflow systems. **2001**, 55, 245-259 4

856 Delegated multisignature scheme with document decomposition. **2001**, 55, 321-328 6

855 Hiding Digital Information Using a Novel System Scheme. **2001**, 20, 533-538 5

854	Analogies and differences between quantum and stochastic automata. **2001**, 262, 69-81	24
853	Similarity in the statistics of prime numbers. **2001**, 296, 523-528	7
852	Computing the order of points on an elliptic curve modulo N is as difficult as factoring N. **2001**, 14, 341-346	4
851	Cryptanalysis of Liaw's broadcasting Cryptosystem. **2001**, 41, 1575-1578	6
850	Cryptographic authentication protocols for smart cards. **2001**, 36, 437-451	8
849	E-commerce applications of smart cards. **2001**, 36, 453-472	11
848	Batch verifying multiple DSA-type digital signatures. **2001**, 37, 383-389	3
847	Confined types in Java. **2001**, 31, 507-532	47
846	Communications security on the internet. **2001**, 2, 104-111	1
845	Quantum wave processing. **2001**, 30, 81-94	11
844	A secure multicast protocol for the internet's multicast backbone. **2001**, 11, 129-136	2
843	Secure key agreement for group communications. **2001**, 11, 365-374	6
842	Electronic voting in a large-scale distributed system. **2001**, 38, 22-32	7
841	Permutation Polynomials Modulo 2w. **2001**, 7, 287-292	50
840	Authenticity and integrity of digital mammography images. **2001**, 20, 784-91	106
839	Approaching Secure Communications in a Message-Oriented Mobile Computing Environment. **2001**, 13, 147-163	2
838	On String Replacement Exponentiation. **2001**, 23, 173-184	1
837	How to Choose Secret Parameters for RSA-Type Cryptosystems over Elliptic Curves. **2001**, 23, 297-316	3

836	A bit-interleaved systolic architecture for a high-speed RSA system. **2001**, 30, 169-175	0
835	A simple micro-payment scheme. **2001**, 55, 221-229	30
834	Threshold signature scheme with multiple signing policies. **2001**, 148, 95-99	13
833	PayFair: a prepaid internet micropayment scheme ensuring customer fairness. **2001**, 148, 207-213	16
832	Integrating SET and EDI for secure healthcare commerce. **2001**, 23, 367-381	3
831	Scholarly publishing in the Internet age: a citation analysis of computer science literature. **2001**, 37, 661-675	118
830	New iterative algorithms and architectures of modular multiplication for cryptography.	2
829	Computer supported collaborative environment for virtual simulation of radiation treatment planning.	1
828	Bit-level architectures for Montgomery's multiplication.	
827	Digit-serial modular multiplication using skew-tolerant domino CMOS.	1
826	Agent Mediated Electronic Commerce. **2001**,	5
825	RSA cryptosystem design based on the Chinese remainder theorem. **2001**,	21
824	Signature Schemes Based on 3rd Order Shift Registers. **2001**, 445-459	2
823	Progress in Cryptology INDOCRYPT 2001. **2001**,	3
822	Cryptographic Hardware and Embedded Systems CHES 2001. **2001**,	4
821	AN OPTIMISTIC THIRD PARTY PROTOCOL TO PROTECT A MOBILE AGENT'S BINARY CODE. **2001**, 11, 607-619	1
820	Role-based access control on the web. **2001**, 4, 37-71	121
819	E-Commerce Agents. **2001**,	6

818	Off-the-record email system.	
817	Advances in Cryptology ASIACRYPT 2001. **2001**,	5
816	A Discipline of Multiprogramming. **2001**,	41
815	The Two Faces of Lattices in Cryptology. **2001**, 146-180	99
814	Improved Online/Offline Signature Schemes. **2001**, 355-367	175
813	[Record linkage with cryptographic identification data in a population-based cancer registry. Development, implementation and error rates]. **2001**, 63, 376-82	15
812	The BiBa one-time signature and broadcast authentication protocol. **2001**,	125
811	DSP application in e-commerce security.	
810	High-speed modular multiplication algorithm for RSA cryptosystem.	
809	A scalable approach for broadcasting data in a wireless network. **2001**,	0
808	SPINS. **2001**,	701
807	Delegation of cryptographic servers for capture-resilient devices. **2001**,	6
806	Twin signatures. **2001**,	19
805	Events in security protocols. **2001**,	17
804	The SecureRing group communication system. **2001**, 4, 371-406	29
803	Digital signature scheme based on factoring and discrete logarithms. **2001**, 37, 220	18
802	Petri nets in cryptographic protocols.	4
801	Optimization of RSA algorithm implementation on TI TMS320C54x signal processors.	

800	The Internet public key infrastructure. **2001**, 40, 648-665	10
799	.	55
798	.	
797	.	16
796	High-Radix Design of a Scalable Modular Multiplier. **2001**, 185-201	25
795	Ethernet Wrapper: extension of the TCP Wrapper.	
794	The Tangram framework: asynchronous circuits for low power.	12
793	Stability-guaranteed dynamic ElGamal cryptosystem for encrypted control systems. **2020**, 14, 2242-2252	2
792	Performance Optimization of DPSK and QPSK for Super Dense Wavelength Division Multiplexing System. **2021**, 20, 2150005	0
791	Implications of Quantum Superposition in Cryptography: A True Random Number Generation Algorithm. **2021**, 419-431	
790	Loki: A Lightweight LWE Method with Rogue Bits for Quantum Security in IoT Devices. **2021**, 543-553	
789	Information security issues in an APL application. **1984**, 14, 185-191	
788	Discourse and Religion in Educational Practice. **2020**, 571-592	
787	A Zero-Knowledge Identification Scheme Based on the Discrete Logarithm Problem and Elliptic Curves. **2021**, 27-35	0
786	Decryption speed up of ElGamal with composite modulus. **2020**, 15, e0240248	
785	Real-time Digital Signatures for Named Data Networking. **2020**,	0
784	Data encryption protocols for electronic mail. **1985**, 3, 43-47	
783	Exploring Architectures for Cryptographic Access Control Enforcement in the Cloud for Fun and Optimization. **2020**,	1

782	Towards model-based development of decentralised peer-to-peer data vaults. **2020**,	
781	Complexity bounds on Semaev's naive index calculus method for ECDLP. **2020**, 14, 460-485	
780	The Join Algorithm: Ordering Messages in Replicated Systems. **1986**, 19, 51-55	2
779	Public key encryption scheme for internet of things based on seminearrings. **2020**,	
778	Homomorphic Encryption. **2021**, 281-307	
777	Trillion Sensors Security. **2021**, 61-93	
776	On the Efficiency of the Lamport Signature Scheme. **2020**, 25, 275-280	
775	Encyclopedia of Cryptography, Security and Privacy. **2021**, 1-1	
774	An Extended Type-1 Generalized Feistel Networks: Lightweight Block Cipher for IoT. **2021**, 1-1	0
773	End-to-End Secure IoT Node Provisioning. **2021**, 341-346	0
772	Efficient ordering policy for secret key assignment in quantum key distribution-secured optical networks. **2022**, 68, 102755	1
771	Formal Modelling and Automated Trade-off Analysis of Enforcement Architectures for Cryptographic Access Control in the Cloud. **2022**, 25, 1-37	1
770	Bibliographie. **2021**, 195-198	
769	A Lightweight Smart Meter Framework using a Scalable Blockchain for Smart Cities. **2021**,	1
768	Timing Attacks in Single-Chip Microcomputer through Workflow Verification. **2021**,	1
767	An Efficient Batch Verification Scheme for SM2 Signatures. **2021**,	0
766	HARDROID: Transparent Integration of Crypto Accelerators in Android. **2021**,	
765	Secure Sharing of Text Based Data Using Hybrid Encryption Algorithms in a Client-Server Model. **2021**,	0

764 Area-Time Scalable High Radix Montgomery Modular Multiplier for Large Modulus. **2021**, 1

763 On Disabling Prefetcher to Amplify Cache Side Channels. **2021**,

762 A Randomized Montgomery Powering Ladder Exponentiation for Side-Channel Attack Resilient RSA and Leakage Assessment. **2021**,

761 . **2021**, 0

760 Generating Prime Numbers Using Genetic Algorithms. **2021**,

759 Fuzzy AHP based Ranking of Cryptography Indicators. **2021**,

758 A Cloud Data Integrity Verification Scheme Based on Blockchain. **2021**,

757 New Code-Based Cryptosystem Based on Binary Image of Generalized Reed-Solomon Code. **2021**, 1

756 Knowledge-Based Approach for the Perception Enhancement of a Vehicle. **2021**, 10, 66 0

755 Video encryption/compression using compressive coded rotating mirror camera. **2021**, 11, 23191 1

754 Digital signatures over HMAC entangled chains. **2021**, 32, 101076

753 Threshold ECDSA with an Offline Recovery Party. **2022**, 19, 1 3

752 The power of the snake: number theory with Python. 1-7

751 Factoring the Modulus of Type N = p2q by Finding Small Solutions of the Equation er □(Ns + t) = p□2 + q□2. **2021**, 9, 2931

750 Homodyne Detection Quadrature Phase Shift Keying Continuous-Variable Quantum key Distribution with High Excess Noise Tolerance. **2021**, 2, 10

749 Increasing security to public key cryptography for point-to-point communication. 1-15

748 Secure space□time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks. **2021**, 4, 827-836 6

747 Profiling Attack against RSA Key Generation Based on a Euclidean Algorithm. **2021**, 12, 462 1

746	Artificial Intelligence-Powered Blockchains for Cardiovascular Medicine. **2021**,	3
745	New Semi-Prime Factorization and Application in Large RSA Key Attacks. **2021**, 1, 660-674	1
744	The Return of Eratosthenes: Secure Generation of RSA Moduli using Distributed Sieving. **2021**,	
743	An image encryption scheme based on finite-time cluster synchronization of two-layer complex dynamic networks. 1	6
742	A Certificateless Authentication and Key Agreement Scheme for Secure Cloud-assisted Wireless Body Area Network. 1	1
741	A Novel Key Distribution Scheme Based on Transmission Delays. **2021**, 2021, 1-13	1
740	Appendices. **2021**, 469-470	
739	You Are Known by Your Mood: A Text-Based Sentiment Analysis for Cloud Security. **2021**, 129-147	
738	Cybersecurity. **2021**, 89-111	
737	Vulnerability - Information Leakage of Reused Secret Key in NewHope. **2021**,	
736	Side-Channel Analysis of ´CRYSTALS-Kyber and A Novel Low-Cost Countermeasure. **2021**, 30-46	
735	Efficient Construction of a Control Modular Adder on a Carry-Lookahead Adder Using Relative-phase Toffoli Gates. **2021**, 1-1	2
734	Limiting Exposure by Hiding the Identity. **2021**, 39-68	
733	Layering Quantum-Resistance into Classical Digital Signature Algorithms. **2021**, 26-41	2
732	THC: Practical and Cost-Effective Verification of Delegated Computation. **2021**, 513-530	
731	Network Thinking. **2021**, 253-297	
730	An ACP-Based Parallel Approach for Color Image Encryption Using Redundant Blocks. **2021**, PP,	1
729	Improvement over Montgomery Modular Multiplication. **2021**, 212-217	

728	Lightweight EdDSA Signature Verification for the Ultra-Low-Power Internet of Things. **2021**, 263-282	1
727	ZERMIA - A Fault Injector Framework for Testing Byzantine Fault Tolerant Protocols. **2021**, 38-60	1
726	Information Encryption and Decryption Analysis, Vulnerabilities and Reliability Implementing the RSA Algorithm in Python. **2021**, 391-404	1
725	Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status. **2021**, 9, 155949-155976	4
724	Adaptive Security via ́Deletion in ́Attribute-Based Encryption: Solutions from ́Search Assumptions in ́Bilinear Groups. **2021**, 311-341	1
723	Fundamentals of Cryptography. **2021**, 45-68	
722	Cryptanalysis of RSA Variants with Primes Sharing Most Significant Bits. **2021**, 42-53	1
721	Blind Signature Protocol Based on Hidden Discrete Logarithm Problem Set in a Commutative Algebra. 1	
720	Routing and Secret Key Assignment for Secure Multicast Services in Quantum Satellite Networks.	2
719	A Survey of Oblivious Transfer Protocol.	0
718	High-speed parallel reconfigurable Fp multipliers for elliptic curve cryptography applications.	
717	Id-PC: An Identification Scheme based on Polar Codes. 1-14	0
716	A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues. **2022**, 26, 100312	5
715	Multi-node data exchange traffic analysis for a communication framework embedded on smart meters. **2022**, 205, 107734	
714	Recent Topics on EM information Security: EM display image stealing threats and its countermeasures. **2018**, 72, 862-866	
713	Bibliographie. **2019**, 275-278	
712	A Benchmarking of the Effectiveness of Modular Exponentiation Algorithms using the library GMP in C language. **2020**,	
711	An Efficient Sieve Algorithm with Evolutionary Technique. **2020**,	

710	aCIOSm4: An Asynchronous CIOS Algorithm. **2020**,	
709	Quantum Public Key Distribution using Randomized Glauber States. **2020**,	0
708	Decoy-state quantum key distribution with direct modulated commercial off-the-shelf VCSEL lasers. **2020**,	
707	Efficient BIKE Hardware Design with Constant-Time Decoder. **2020**,	1
706	Fast Coding of Irregular Binary Binomial Numbers with a Set Number of Units Series. **2020**,	1
705	Efficient Parallel GCD Algorithms for Multicore Shared Memory Architectures. **2020**,	
704	Demystifying Cryptography behind Blockchains and a Vision for Post-Quantum Blockchains. **2020**,	1
703	Method of Indirect Steganographic Coding of Information without Visual Distortion of the Video Container series. **2020**,	1
702	Hardware Trojan Design and Detection in Asynchronous NCL Circuits. **2020**,	1
701	Decoding Method of Information-Psychological Destructions in the Phonetic Space of Information Resources. **2020**,	1
700	Privacy-Preserving Public Verification of Ethical Cobalt Sourcing. **2020**,	0
699	Hierarchical Services of Convolutional Neural Networks via Probabilistic Selective Encryption. **2021**, 1-1	
698	Generating Residue Number System Bases. **2021**,	0
697	Digital Signature Scheme over Lattices. **2021**,	0
696	Multi-Prime RSA Verilog Implementation Using 4-Primes. **2021**,	0
695	Method of Hierarchical Protection of Biometric Information. **2021**,	
694	Method of Masking Information in the Contours of Video Images. **2021**,	
693	Method of coding dynamic sequence of frame-spline structures of provided frames in info-communications. **2021**,	0

692 Possible Ways of Video Processing at the Quantization Stage.

691 ChaDRaL: RGB Image Encryption based on 3D Chaotic Map, DNA, RSA and LSB. **2021**,

690 New direction in Cryptography: Homomorphic Encryption. **2021**, 1

689 A Channel Magnitude Based Key Generation Scheme for Static and Dynamic Environments. **2021**,

688 A hybrid architecture for resolving Cryptographic issues in internet of things (IoT), Employing Quantum computing supremacy. **2021**, 0

687 A Secret Sharing Scheme to Reduce the Total Data Size. **2021**,

686 A privacy-friendly aggregation algorithm for demand side management of residential loads. **2021**, 0

685 JointCloud Cross-chain Verification Model of Decentralized Identifiers. **2021**, 1

684 An Efficient Non-Profiled Side-Channel Attack on the CRYSTALS-Dilithium Post-Quantum Signature. **2021**, 2

683 New McEliece Cryptosystem Based on Polar-LDPC Concatenated Codes as a Post-quantum Cryptography. **2021**,

682 Multi-Qubit Size-Hopping Deutsch-Jozsa Algorithm with Qubit Reordering for Secure Quantum Key Distribution. **2021**, 0

681 Blind Decryption for Preserving Privacy in the DRM System. **2021**,

680 A Random Number Generator Based on Metastability of Oscillators. **2021**, 0

679 Post-Quantum Security for Ultra-Reliable Low-Latency Heterogeneous Networks. **2021**, 0

678 An SD-WAN Approach for EUt+Network. **2021**, 0

677 A survey on Attribute-Based Signatures. **2022**, 124, 102396 0

676 Quantum Computing and Simulations for Energy Applications: Review and Perspective. 4

675 An Algorithmic Reduction Theory for Binary Codes: LLL and more. **2022**, 1-1

674	Efficient and Scalable Hardware Implementation of Montgomery Modular Multiplication.	1
673	Network-Compatible Unconditionally Secured Classical Key Distribution via Quantum Superposition-Induced Deterministic Randomness. **2022**, 6, 4	1
672	Introduction to Cryptography in Blockchain. **2022**, 1-34	
671	A variant RSA acceleration with parallelisation. 1-15	
670	A bibliometric review of research on digital identity: Research streams, influential works and future research paths. **2022**, 62, 523-538	1
669	Cryptanalysis and improvement of a (t,´n) threshold group signature scheme. **2022**, 21, 1	2
668	The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. **2022**, 1-1	11
667	A comprehensive survey of image and video forgery techniques: variants, challenges, and future directions. 1	1
666	A Pairing-Free Signature Scheme from Correlation Intractable Hash Function and Strong Diffie-Hellman Assumption. **2022**, 26-48	
665	Encrypted SQL Arithmetic Functions Processing for´Secure Cloud Database. **2022**, 207-225	
664	A quantum hash function with grouped coarse-grained boson sampling. **2022**, 21, 1	1
663	Algorithm-Level Confidentiality for Average Consensus on Time-Varying Directed Graphs. **2022**, 1-1	3
662	Efficient Homomorphic Encryption Accelerator With Integrated PRNG Using Low-Cost FPGA. **2022**, 10, 7753-7771	2
661	Anonymous Privacy-Preserving Consensus via Mixed Encryption Communication. **2022**, 1-1	
660	A review of the tropical approach in cryptography. 1-25	0
659	Preliminaries. **2022**, 27-42	
658	Secure E-Commerce Scheme. **2022**, 10, 10359-10370	0
657	Qubits based mutual authentication protocol.	

656 Fuzzy MP - A Fuzzy Digital Signature Scheme with Biometrics. **2022**, 299-315

655 Physical publicly verifiable randomness from pulsars. **2022**, 38, 100549 0

654 An Analysis on the Variants of the RSA Cryptography. **2022**,

653 Combined two-dimensional word-based serial-in/serial-out systolic processor for multiplication and squaring over GF(2m). **2022**,

652 Lattice Points on the Fermat Factorization Method. **2022**, 2022, 1-18

651 Robust encryption method based on AES-CBC using elliptic curves DiffieHellman to secure data in wireless sensor networks. **2022**, 28, 991 3

650 Safety Architecture Proposal for Low-Latency Sensor/Actuator Networks using IO-Link Wireless. **2022**, 10, 3030-3044 1

649 Current Trends in Blockchain Implementations on the Paradigm of Public Key Infrastructure: A Survey. **2022**, 1-1 0

648 Using Genetic Algorithm in Inner Product to Resist Modular Exponentiation From Higher Order DPA Attacks. **2022**, 10, 3238-3251 1

647 Light and Secure Encryption Technique Based on Artificially Induced Chaos and Nature-Inspired Triggering Method. **2022**, 14, 218

646 Randomised Key Selection and Encryption of Plaintext Using Large Primes. **2022**, 39-46

645 Semi-automatic ladderisation: improving code security through rewriting and dependent types. **2022**,

644 New (k,l,m)-verifiable multi-secret sharing schemes based on XTR public key system. **2022**, 0

643 High-Radix Design of a Scalable Montgomery Modular Multiplier With Low Latency. **2022**, 71, 436-449 2

642 GENDA: A Graph Embedded Network Based Detection Approach on encryption algorithm of binary program. **2022**, 65, 103088 0

641 PARFAIT: Privacy-preserving, secure, and low-delay service access in fog-enabled IoT ecosystems. **2022**, 206, 108799 0

640 Efficient FPGA implementation of RNS Montgomery multiplication using balanced RNS bases. **2022**, 84, 72-83 0

639 HybridPKE: A forward-secure non-interactive quantum-safe hybrid key exchange scheme. **2022**, 34, 101094 1

638	Quantum Computing: The Future of Big Data and Artificial Intelligence in Spine.. **2022**, 6, 93-98	2
637	Die ganzen Zahlen. **2022**, 47-97	
636	Efficient and scalable FPGA design of GF(2m) inversion for post-quantum cryptosystems. **2022**, 1-1	1
635	Advanced digital signatures for preserving privacy and trust management in hierarchical heterogeneous IoT: Taxonomy, capabilities, and objectives. **2022**, 100492	2
634	An Efficient Variant of Pollard□s p □1 for the Case That All Prime Factors of the p □1 in B-Smooth. **2022**, 14, 312	0
633	Nanomaterials for Quantum Information Science and Engineering.. **2022**, e2109621	6
632	Connectivity invariant lightweight resiliency improvement strategies for CRT-subset scheme. **2022**, 102803	
631	A quantum circuit design of AES requiring fewer quantum qubits and gate operations. **2022**, 17, 1	1
630	Quantum Signature without Classical Private Key. **2022**, 61, 1	0
629	A privacy preserving homomorphic computing toolkit for predictive computation. **2022**, 59, 102880	0
628	On the Universal Encoding Optimality of Primes. **2021**, 9, 3155	
627	Work-in-Progress: Enabling Secure Boot for Real-Time Restart-Based Cyber-Physical Systems. **2021**,	
626	A 3d Visual Security (3dvs) Score to Measure the Visual Security Level of Selectively Encrypted 3d Objects.	
625	A brief and understandable guide to pseudo-random number generators and specific models for security. **2022**, 16,	0
624	On Polynomial Modular Number Systems over $ mathbb{Z}/{p}mathbb{Z} $. **2022**,	0
623	A Novel Three-Factor Authentication Protocol for Multiple Service Providers in 6G-Aided Intelligent Healthcare Systems. **2022**, 10, 28975-28990	5
622	Bayesian Neural Networks for Reversible Steganography. **2022**, 1-1	0
621	High-Speed Post-Quantum Cryptoprocessor Based on RISC-V Architecture for IoT. **2022**, 1-1	2

620 Traditional Machine Learning Methods for Side-Channel Analysis. **2022**, 25-47 0

619 An Iterative Montgomery Modular Multiplication Algorithm With Low Area-Time Product. **2022**, 1-1

618 Low Complexity and High Speed Montgomery Multiplication Based on FFT. **2022**, 693-703

617 Shift-Sub Modular Multiplication Algorithm and Hardware Implementation for RSA Cryptography. **2022**, 541-552

616 Privacy-Preserving Multi-class Support Vector Machine Model on Medical Diagnosis.. **2022**, PP, 0

615 Multi-Use Trust in Crowdsourced IoT Services. **2022**, 1-1 1

614 Ferproof: A Constant Cost Range Proof Suitable for Floating-Point Numbers. **2022**, 648-667

613 Privacy Preserving via Secure Summation in Distributed Kalman Filtering. **2022**, 1-1 1

612 Private AI: Machine Learning on Encrypted Data. **2022**, 97-113 0

611 Deep Learning on Side-Channel Analysis. **2022**, 48-71

610 A Quantum Architecture Based Decoherence Model. **2022**, 442-458

609 Comparing Quantum Computing Platforms. **2022**, 423-441

608 Enhancing Security with In-Depth Analysis of Brute-Force Attack on Secure Hashing Algorithms. **2022**, 513-522 0

607 Prediction of Heart Disease using LDL in Edge Computing Systems. **2022**, 583-599

606 Privacy-Preserving Machine Learning Using Cryptography. **2022**, 109-129

605 Reversible Linguistic Steganography With Bayesian Masked Language Modeling. **2022**, 1-10 1

604 A Provably Secure User Authentication Scheme Over Unreliable Networks. **2022**, 602-613

603 Privacy-Preserving Cluster Validity. **2022**, 159-170 1

602	SPoTKD: A Protocol for Symmetric Key Distribution Over Public Channels Using Self-Powered Timekeeping Devices. **2022**, 17, 1159-1171	0
601	Developing a framework of beta cryptosystem based on Santilli's isofields second-kind. **2022**,	0
600	A Secure Secret Key-Sharing System for Resource-Constrained IoT Devices using MQTT. **2022**,	
599	Varibox encryption algorithm : The new generation of hybrid security measure for the era of quantum computation. 1-27	
598	Towards a fully homomorphic symmetric cipher scheme resistant to plain-text/cipher-text attacks. 1	1
597	A Searchable Encryption Scheme with Biometric Authentication and Authorization for Cloud Environments. **2022**, 6, 8	3
596	Lightweight encryption for short-range wireless biometric authentication systems in Industry 4.0. **2022**, 29, 153-173	2
595	Synchronously scrambled diffuse image encryption method based on a new cosine chaotic map.	0
594	Rethinking modular multi-exponentiation in real-world applications. 1	
593	Histogram Shifting-Based Quick Response Steganography Method for Secure Communication. **2022** , 2022, 1-11	2
592	A Secure and Anonymous Communicate Scheme over the Internet of Things.	9
591	Quantum public key encryption scheme with four states key. **2022**, 97, 045102	
590	New Signature Scheme Based on Elliptic Curve and Factoring Problems Using Chaotic Map. 1-9	
589	A variant of RSA using continued fractions. 1-8	
588	Implementation of three efficient 4-digit fault-tolerant quantum carry lookahead adders. 1	0
587	Multiparty Generation of an RSA Modulus. **2022**, 35, 1	0
586	Efficient high-precision integer multiplication on the GPU. 109434202210779	
585	Variations of QKD Protocols Based on Conventional System Measurements: A Literature Review. **2022**, 6, 12	3

584 Quantum Algorithm Implementations for Beginners. 4

583 A WSN Framework for Privacy Aware Indoor Location. **2022**, 12, 3204 2

582 Privacy Preservation in Social Network Data using Evolutionary Model. **2022**, 1

581 The alternative method to speed up RSA decryption process. 1-22

580 Privacy-Preserving Minority Oversampling Protocols with Fully Homomorphic Encryption. **2022**, 2022, 1-9

579 Challenges of post-quantum digital signing in real-world applications: a survey. 1 1

578 A Quantum Public-Key Cryptosystem without Quantum Channels between any Two Users Based on Quantum Teleportation. **2022**, 61, 1

577 An Optical Image Encryption Method Using Hopfield Neural Network.. **2022**, 24, 2

576 Bibliography. **2022**, 327-337

575 Speeding Up Fermat Factoring Method using Precomputation. **2022**, 6, 50-60 0

574 An Efficient Crypto Processor Architecture for Side-Channel Resistant Binary Huff Curves on FPGA. **2022**, 11, 1131

573 Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states.. **2022**, 11, 83 7

572 Towards Secure Big Data Analysis via Fully Homomorphic Encryption Algorithms.. **2022**, 24, 1

571 Verifiable varying sized (m,n,n) multi-image secret sharing with combiner verification and cheater identification. **2022**, 84, 103466

570 TPPSUPPLY : A traceable and privacy-preserving blockchain system architecture for the supply chain. **2022**, 66, 103116 1

569 Improved Sine-Tangent chaotic map with application in medical images encryption. **2022**, 66, 103131 3

568 Comment on An enhanced and secured RSA public cryptosystem algorithm using Chinese remainder theorem (ESRPKC) **2022**, 177, 106263

567 Privacy-Preserving Biometric Matching Using Homomorphic Encryption. **2021**, 3

566	Knowledge art. **2021**,	
565	A K-nearest neighbor classifier based on homomorphic encryption scheme. **2021**,	
564	Comparative Study of Cryptographic and Biometric Signatures. **2021**,	
563	Rando: A General-purpose True Random Number Generator for Conventional Computers. **2021**,	2
562	Strengthening Security of Images Using Dynamic S-Boxes for Cryptographic Applications. **2021**,	
561	On one method for using quantum polarization filters in encryption. **2021**,	
560	Data Security and Privacy using DNA Cryptography and AES Method in Cloud Computing. **2021**,	0
559	A Multi-Key Based Lightweight Additive Homomorphic Encryption Scheme. **2021**,	1
558	Single-Trace Side-Channel Attacks on □Small Polynomial Sampling: With Applications to NTRU, NTRU Prime, and CRYSTALS-DILITHIUM. **2021**,	2
557	A Practical and Efficient Node Blind SignCryption Scheme for the IoT Device Network. **2022**, 12, 278	0
556	INDIRECT INFORMATION HIDING TECHNOLOGY ON A MULTIADIC BASIS. **2021**, 11, 14-17	
555	Design and Specification of a Blockchain-based P2P Energy Trading Platform. **2021**,	
554	Small Prime Divisors Attack and Countermeasure against the RSA-OTP Algorithm. **2022**, 11, 95	0
553	SimAnMo□A parallelized runtime model generator.	0
552	Post-Quantum and Code-Based Cryptography□Some Prospective Research Directions. **2021**, 5, 38	1
551	Managing Cyber Security with Quantum Techniques. **2021**,	
550	A quantum encryption design featuring confusion, diffusion, and mode of operation. **2021**, 11, 23774	2
549	SABER-GPU: A Response-Based Cryptography Algorithm for SABER on the GPU. **2021**,	1

548 Quantum Hoare Logic with Classical Variables. **2021**, 2, 1-43 3

547 Image Encryption Using Lorenz's Attractor and Fractional Fourier Transform. **2021**,

546 Stellar calibration of the single-photon receiver for satellite-to-ground quantum key distribution. **2021**, 2086, 012137 1

545 Synchronization of a Memristor Chaotic System and Image Encryption. **2021**, 31, 0

544 Fault-Tolerant Computation Meets Network Coding: Optimal Scheduling in Parallel Computing. **2021**, 0

543 BSI: Blockchain to secure routing protocol in Internet of Things. **2022**, 34, 0

542 Perspectives of Blockchain in Digital Health in Brazil. **2022**, 1-18

541 Homomorphic Encryption Reference Model for Mobile Cyber Physical Systems. **2021**,

540 Advanced Encryption Schemes. **2022**, 195-204

539 Power Pell Sequences, Some Periodic Relations of These Sequences, and a Cryptographic Application With Power Pell Sequences. **2022**, 21-43

538 Protected Fair Secret Sharing Based Bivariate Asymmetric Polynomials in Satellite Network. **2022**, 72, 4789-4802

537 Cryptosystem and Authentication System. **2022**, 153-196

536 Asymmetric Encryption Schemes. **2022**, 131-146

535 Lattice Cryptalization and Cybersecurity: New Findings in Analyzing Cryptovalues Dynamics. **2022**, 353-358

534 An Enhanced Cloud-Based Healthcare System for Patient Data Privacy and Security Using Hybrid Encryption. **2022**,

533 FPGA Implementation of High-Performance Montgomery Modular Multiplication with Adaptive Hold Logic. **2022**,

532 Dickson basis multiplier with concurrent error detection against fault attacks for lightweight cryptosystems.

531 Atomicity and Regularity Principles Do Not Ensure Full Resistance of ECC Designs against Single-Trace Attacks.. **2022**, 22, 0

530	A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. **2022**,	2
529	Multi-party interactive cryptographic key distribution protocol over a public network based on computational ghost imaging. **2022**, 155, 107067	1
528	Ransomware Attack as Hardware Trojan: A Feasibility and Demonstration Study. **2022**, 10, 44827-44839	
527	The "Cyber Security via Determinism" Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT). **2022**, 10, 45893-45930	1
526	SPMAC: Scalable Prefix Verifiable Message Authentication Code for Internet of Things. **2022**, 1-1	
525	Trusted Execution Environment Hardware by Isolated Heterogeneous Architecture for Key Scheduling. **2022**, 10, 46014-46027	1
524	The Philosophy of Quantum Computing. **2022**, 107-152	
523	Designing Optimal Key Lengths and Control Laws for Encrypted Control Systems based on Sample Identifying Complexity and Deciphering Time. **2022**, 1-1	0
522	Steganography Method Using Effective Combination of RSA Cryptography and Data Compression. **2022**,	
521	Performance Evaluation of RSA, ElGamal, and Paillier Partial Homomorphic Encryption Algorithms. **2022**,	0
520	Byte Frequency Based Indicators for Crypto-Ransomware Detection from Empirical Analysis. **2022**, 37, 423-442	0
519	Generalized Goldwasser and Micali's Type Cryptosystem. **2022**, 37, 459-467	
518	Distance Enhancement of Quantum Cryptography through MANET. **2022**, 86-93	
517	A Scalable Digit-Parallel Polynomial Multiplier Architecture for NIST-Standardized Binary Elliptic Curves. **2022**, 12, 4312	0
516	Versatile Hardware Framework for Elliptic Curve Cryptography. **2022**,	
515	Secure cloud model for intellectual privacy protection of arithmetic expressions in source codes using data obfuscation techniques. **2022**,	1
514	An efficient mutual authentication scheme for IoT systems. 1	1
513	A Review of Cryptographic Electronic Voting. **2022**, 14, 858	2

512	Medical Cooperative Authenticated Key Agreement Schemes with Involvement of Personal Care Assistant in Telemedicine. **2022**, 106809	
511	Cypherpunk. **2022**, 11,	
510	Malicious Finding and Validation Scheme Using New Enhanced Adaptive Ack. **2022**,	0
509	Speeding up wheel factoring method. 1	1
508	Ibn Sina: A Patient Privacy-preserving Authentication Protocol in Medical Internet of Things. **2022**, 102753	0
507	Patient-centered cross-enterprise document sharing and dynamic consent framework using consortium blockchain and ciphertext-policy attribute-based encryption. **2022**,	1
506	Crytographical primitive for blockchain: a secure random DNA encoded key generation technique. 1	
505	Post-Quantum Cipher Power Analysis in Lightweight Devices. **2022**,	
504	Transitioning organizations to post-quantum cryptography.. **2022**, 605, 237-243	4
503	Implementation of Shor's Algorithm and Reliability of Quantum Computing Devices. **2021**,	
502	xRSA: Construct Larger Bits RSA on Low-Cost Devices. **2021**,	
501	An Empirical Study of Secure and Complex Variants of RSA Scheme. **2022**, 185-196	
500	A Channel State Information-Based Key Generation Scheme for Internet of Things. **2022**, 2022, 1-15	2
499	Quantum mean-value approximator for hard integer-value problems. **2022**, 105,	0
498	Factoring semi-primes with (quantum) SAT-solvers.. **2022**, 12, 7982	0
497	DIGITAL RADIOGRAPHIC IMAGE ARCHIVAL, RETRIEVAL, AND MANAGEMENT. **2000**, 44, 339-358	6
496	Security Issues of Novel RSA Variant. **2022**, 1-1	1
495	Improving small private exponent attack on the Murru-Saettone cryptosystem. **2022**,	1

494	IETD: a novel image encryption technique using Tinkerbell map and Duffing map for IoT applications.	1
493	Quantum Digital Signature with Continuous-Variable. **2022**, 61,	
492	RPVC: A Revocable Publicly Verifiable Computation Solution for Edge Computing. **2022**, 22, 4012	
491	Frequency Domain Horizontal Cross Correlation Analysis of RSA. **2022**, 22, 3-10	
490	Analyzing the Security of Three-State Protocols Using Information-Theoretic.	
489	Multi-key Encryption Based on RSA and Block Segmentation. **2022**, 687-695	
488	Bibliographie. **2022**, 299-302	
487	Review of Chosen Isogeny-Based Cryptographic Schemes. **2022**, 6, 27	
486	Secure cloud-based data storage scheme using postquantum integer lattices-based signcryption for IoT applications.	
485	Low-Rate Denial-of-Service Attack Detection: Defense Strategy Based on Spectral Estimation for CV-QKD. **2022**, 9, 365	0
484	An Improvement of a Key Exchange Protocol Relying on Polynomial Maps.	
483	Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. **2022**, 12,	1
482	A cluster-based networking approach for large-scale and wide-area quantum key agreement. **2022**, 21,	
481	Blockchain Based Electronic Voting Protocol. **2022**, 5, 56-115	
480	Jamming a terahertz wireless link. **2022**, 13,	4
479	A Probabilistic Chaotic Image Encryption Scheme. **2022**, 10, 1910	0
478	Data security: a cryptographic approach. **1982**, 5, 65-83	1
477	Cryptographic algorithms in IoT - a detailed analysis. **2021**,	

476 Asymmetric Cryptography Among Different 5G Core Networks. **2022**, 325-333 4

475 ESSD: Energy Saving and Securing Data Algorithm for WSNs Security. **2022**, 73, 3969-3981

474 Quantum Computing With Trapped Ions: An Overview.. **2022**, 2-8

473 PSI-Stats: Private Set Intersection Protocols Supporting Secure Statistical Functions. **2022**, 585-604

472 RSA Key Recovery from´Digit Equivalence Information. **2022**, 193-211 1

471 A High Performance SIKE Accelerator with High Frequency and Low Area-Time Product. **2022**, 1-1

470 Secured and Quantum Resistant Key Exchange Cryptography Methods A Comparison. **2022**,

469 An High Speed Area Efficient Implementation of Prime Field based Twisted Edwards Curve Point Multiplication using FPGA Architecture. **2022**,

468 Cybersecurity of Industrial Cyber-Physical Systems. **2022**, 97-116

467 Caching-based Multicast Message Authentication in Time-critical Industrial Control Systems. **2022**, 0

466 Fusion-based advanced encryption algorithm for enhancing the security of Big Data in Cloud. 1063293X2210890 0

465 An Effective and enhanced RSA based Public Key Encryption Scheme (XRSA).

464 Automation of reversible steganographic coding with nonlinear discrete optimisation. **2022**, 34, 1719-1735 1

463 Event-Triggered Privacy-Preserving Bipartite Consensus for Multi-agent Systems based on Encryption. **2022**,

462 Modified SHARK Cipher and Duffing Map-Based Cryptosystem. **2022**, 10, 2034

461 The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges A Systematic Literature Review (SLR). **2022**, 2022, 1-26 1

460 LedgerView: Access-Control Views on Hyperledger Fabric. **2022**, 0

459 BlindFL: Vertical Federated Machine Learning without Peeking into Your Data. **2022**, 1

458	Quantum permutation pad for universal quantum-safe cryptography. **2022**, 21,	1
457	Triboelectric biometric signature. **2022**, 100, 107496	
456	PriFoB: A Privacy-aware Fog-enhanced Blockchain-based system for Global Accreditation and Credential Verification. **2022**, 205, 103440	0
455	Self-Renewal Consortium Blockchain Based on Proof of Rest and Strong Smart Contracts. **2022**, 27, 964-972	
454	Cryptographic Tools for Blockchains. **2021**, 1-25	
453	Electronic Health Records Sharing Model based on Blockchain with Checkable State PBFT Consensus Algorithm. **2022**, 1-1	1
452	Integrating and Evaluating Quantum-safe TLS in Database Applications. **2022**, 259-278	
451	A Modified Key Sifting Scheme With Artificial Neural Network Based Key Reconciliation Analysis in Quantum Cryptography. **2022**, 10, 72743-72757	0
450	EV-PUF: Lightweight Security Protocol for Dynamic Charging System of Electric Vehicles Using Physical Unclonable Functions. **2022**, 1-17	1
449	Protocols for symmetric secret key establishment: Modern approach. **2022**, 70, 604-635	
448	Two-Party E-Commerce Protocols. **2022**, 15-42	
447	Compositional inverses of AGW-PPs dedicated to professor cunsheng ding for his 60th birthday. **2022**,	
446	PDDL: Proactive Distributed Detection and Localization Against Stealthy Deception Attacks in DC Microgrids. **2022**, 1-1	
445	Privacy-Preserving Distributed Economic Dispatch of Microgrids: A Dynamic Quantization Based Consensus Scheme with Homomorphic Encryption. **2022**, 1-1	1
444	PMNS for efficient arithmetic and small memory cost. **2022**, 1-14	1
443	Data Secrecy: Why Does It Matter in the Cloud Computing Paradigm?. **2022**, 549-560	
442	On New Problems in Asymmetric Cryptography Based on Error-Resistant Coding. **2022**, 58, 184-201	1
441	MEHE based Prediction of Health Condition using LBM in Edge Computing Systems. **2022**,	

440 Image Crypto-Compression. **2022**, 91-128

439 Revisiting the Polynomial-Time Equivalence of Computing the CRT-RSA Secret Key and Factoring. **2022**, 10, 2238 1

438 A Neural Network Model Secret-Sharing Scheme with Multiple Weights for Progressive Recovery. **2022**, 10, 2231 1

437 A glance at blockchain technology and cryptocurrencies as an application. **2022**, 10, 60-65

436 Security in quantum cryptography. **2022**, 94, 4

435 Privacy-Preserved Federated Learning for 3D Tooth Segmentation in Intra-Oral Mesh Scans. 3,

434 Compact modular multiplier design for strong security capabilities in resource-limited Telehealth IoT devices. **2022**,

433 Fuel Monitoring System based on IoT: Overview and Device Authentication. **2022**,

432 A Business-to-Business Collaboration System That Promotes Data Utilization While Encrypting Information on the Blockchain. **2022**, 22, 4909 0

431 Blockchain for Ecologically Embedded Coffee Supply Chains. **2022**, 6, 43 1

430 Flawed implemented cryptographic algorithm in the Microsoft ecosystem. **2022**, 73, 190-196

429 Output Feedback Stabilization of Large-Scale Networked Cyberphysical Systems Using Cryptographic Techniques. **2022**,

428 Cryptanalysis of Encryption Scheme Based on Compound Coupled Logistic Map and Anti-Codifying Technique for Secure Data Transmission. **2022**, 169628 0

427 Transfer of linewidth and frequency stability from an iodine-stabilized Nd:YAG laser to a quantum memory control laser through an optical frequency comb. 0

426 Hash-based signature revisited. **2022**, 5,

425 Advances in Near-Infrared Organic Micro/Nanolasers. 2200815 1

424 Efficient chain-encryption-based quantum signature scheme with semi-trusted arbitrator. **2022**, 21, 0

423 Using Shor algorithm on near term Quantum computers: a reduced version. **2022**, 4, 1

422	Lightweight Architecture for Elliptic Curve Scalar Multiplication over Prime Field. **2022**, 11, 2234	
421	Twin physically unclonable functions based on aligned carbon nanotube arrays.	1
420	A secure and lightweight anonymous mutual authentication scheme for wearable devices in Medical Internet of Things. **2022**, 68, 103259	0
419	Security in Digital Aeronautical Communications A Comprehensive Gap Analysis. **2022**, 38, 100549	0
418	Bibliographie. **2022**, 239-240	
417	Cryptanalysis of RSA-Variant Cryptosystem Generated by Potential Rogue CA Methodology. **2022**, 14, 1498	1
416	A two-layer networks-based audio encryption/decryption scheme via fixed-time cluster synchronization.	0
415	Quantum Randomness in Cryptography A Survey of Cryptosystems, RNG-Based Ciphers, and QRNGs. **2022**, 13, 358	
414	Variational quantum attacks threaten advanced encryption standard based symmetric cryptography. **2022**, 65,	1
413	Continuous-variable quantum key distribution in a multi-way setting. **2022**,	
412	A Multivariate-Based Provably Secure Certificateless Signature Scheme With Applications To The Internet Of Medical Things.	
411	A 3D Visual Security (3DVS) score to measure the visual security level of selectively encrypted 3D objects. **2022**, 108, 116832	
410	Privacy-preserving decentralized price coordination for EV charging stations. **2022**, 212, 108355	1
409	Experimental quantum key distribution certified by Bell's theorem. **2022**, 607, 682-686	9
408	Improved Lattice Enumeration Algorithms by Primal and Dual Reordering Methods. **2022**, 159-174	1
407	Cryptographic Algorithms for Security in Wireless Sensor Networks. **2022**,	
406	Novel Encryption Scheme Based on Continued Fraction and Permutation. **2022**,	
405	Adversarial Prefetch: New Cross-Core Cache Side Channel Attacks. **2022**,	

404 Electronic Health Record Security in Cloud. **2022**, 853-877

403 Method for Approximating RSA Prime Factors. **2022**,

402 Advancements in Data Security and Privacy Techniques Used in IoT-Based Hospital Applications. **2022**, 662-684

401 Efficient and Side-Channel Resistant Design of High-Security Ed448 on ARM Cortex-M4. **2022**, 2

400 An Authentication Mechanism for Remote Keyless Entry Systems in Cars to Prevent Replay and RollJam Attacks. **2022**, 0

399 A verifiable threshold secret image sharing (SIS) scheme with combiner verification and cheater identification.

398 Public-Key Cryptography Based on Tropical Circular Matrices. **2022**, 12, 7401

397 Post-Quantum Secure Identity-Based Encryption Scheme using Random Integer Lattices for IoT-enabled AI Applications. **2022**, 2022, 1-14

396 Quantum (t,n) Threshold Proxy Blind Signature Scheme Based on Bell States. **2022**, 61,

395 Quantum Cryptography and Security. **2022**, 63-77

394 Construction of Permutation Polynomials Using Additive and Multiplicative Characters. **2022**, 14, 1539

393 A secure finger vein verification and authentication scheme for banking network. 0

392 Creating an Open Community of Cryptographers. **2022**, 185-212

391 The Development of a Crypto Policy Community: Diffie□Hellman□s Impact on Public Policy. **2022**, 213-256

390 FogDedupe: A Fog-Centric Deduplication Approach Using Multi-Key Homomorphic Encryption Technique. **2022**, 2022, 1-16

389 A new quantum-safe multivariate polynomial public key digital signature algorithm. **2022**, 12, 0

388 An anonymous and unlinkable electronic toll collection system.

387 Classically verifiable quantum advantage from a computational Bell test. **2022**, 18, 918-924 3

386	Enhanced RSA Algorithm for Data Security in the Internet of Things.	
385	Photon-by-photon quantum light state engineering. **2022**, 100414	
384	An Improved Algorithm for Computing Logarithms over GF (p) and Its Cryptographic Significance. **2022**, 415-430	
383	NuText: A Novel Method for Music Encoding and Its Practical Application.	
382	A Novel Reversible Data Hiding Algorithm Based on Enhanced Reduced Difference Expansion. **2022** , 14, 1726	0
381	Public Key Cryptography in Computer and Network Security. **2022**, 57-76	
380	Public Key Cryptography's Impact on Society: How Diffie and Hellman Changed the World. **2022**, 19-56	
379	A Gift that Keeps on Giving: The Impact of Public-Key Cryptography on Theoretical Computer Science. **2022**, 157-184	
378	An authenticated and secure accounting system for international emissions trading. 1-10	
377	Improved lattice enumeration algorithms by primal and dual reordering methods.	
376	Fast Introduction to Quantum Computers. 1-6	
375	Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things. **2022**, 11, 2560	1
374	Design and realization of a secure multiplicative homomorphic encryption scheme for cloud services.	
373	Instruction flow-based detectors against fault injection attacks. **2022**, 104638	
372	SoK: How private is Bitcoin? Classification and Evaluation of Bitcoin Privacy Techniques. **2022**,	
371	Privacy and Authentication: An Introduction to Cryptography. **2022**, 431-514	
370	Hybrid Intelligent Security Mechanism for Data Transmission among UPFs belonging to Different 5G Networks.	
369	Quantum Information Theory in Infinite Dimensions with Application to Optical Channels.	

368	Design of digital image encryption based on elliptic curve cryptography (ECC) algorithm and Radix-64 conversion. **2022**, 1-12	0
367	Cryptanalysis of RSA with smooth prime sum. 1-21	
366	CREASE: Certificateless and REused-pseudonym based Authentication Scheme for Enabling security and privacy in VANETs. **2022**, 20, 100605	0
365	Ensuring security of artificial pancreas device system using homomorphic encryption. **2023**, 79, 104044	0
364	D-NISQ: A reference model for Distributed Noisy Intermediate-Scale Quantum computers. **2023**, 89, 16-28	0
363	Encapsulating Secrets Using Lockable Obfuscation and a RMERS-Based Public Key Encryption. **2022**, 14, 11412	0
362	SM2-based low-cost and efficient parallel modular multiplication. **2022**, 94, 104650	0
361	Efficient hardware realization and high radix implementation of modular multi exponential techniques for public key cryptography. **2022**, 128, 105548	0
360	A quantum blockchain-enabled framework for secure private electronic medical records in Internet of Medical Things. **2022**, 612, 942-958	2
359	Improvements on Non-Interactive Zero-Knowledge Proof Systems Related to Quadratic Residuosity Languages. **2022**, 613, 324-343	0
358	RMA-CPABE : A multi-authority CPABE scheme with reduced ciphertext size for IoT devices. **2023**, 138, 226-242	1
357	Introduction to the Field of Information Security.	0
356	Optimal Power Allocation and Optimal Linear Encoding for Parameter Estimation in the Presence of a Smart Eavesdropper. **2022**, 70, 4093-4108	0
355	Quantum key distribution. **2022**, 215-272	0
354	A Quantum Mechanical Proof of Insecurity of the Theoretical QKD Protocols. **2022**, 12, 53-63	0
353	Challenges and Opportunities for Next-Generation Manufacturing in Space. **2022**, 55, 963-968	0
352	Secure Hierarchical Deterministic Wallet Supporting Stealth Address. **2022**, 89-109	1
351	Higher-Order Masked Saber. **2022**, 93-116	2

350	DU-QS22: A Dataset for Analyzing QC-MDPC-Based Quantum-Safe Cryptosystems. **2022**, 3-10	0
349	A New Key Recovery Side-Channel Attack on HQC with Chosen Ciphertext. **2022**, 353-371	0
348	Cryptographic Primitives. **2022**, 1-24	0
347	On Extension of Evaluation Algorithms in Keyed-Homomorphic Encryption. **2022**, 189-207	0
346	Dilithium for Memory Constrained Devices. **2022**, 217-235	0
345	FUTURE: A Lightweight Block Cipher Using an Optimal Diffusion Matrix. **2022**, 28-52	0
344	Quantum Bitcoin: The Intersection of Bitcoin, Quantum Computing and Blockchain. **2022**, 223-234	0
343	Dependability. **2022**, 143-175	0
342	A Generalized Attack on the Multi-prime Power RSA. **2022**, 537-549	1
341	PipeFL: Hardware/Software co-Design of an FPGA Accelerator for Federated Learning. **2022**, 10, 98649-98661	1
340	Improving Fault Attacks on Rainbow with Fixing Random Vinegar Values. **2022**, 147-165	0
339	Efficient Multiplication of Somewhat Small Integers Using Number-Theoretic Transforms. **2022**, 3-23	0
338	Cosmic Coding and Transfer (COSMOCAT) for Ultra High Security Near-Field Communications.	0
337	A Privacy-Preserving Medical Data Sharing Scheme Based on Blockchain. **2022**, 1-12	0
336	A New Public Key Encryption Using Dickson Polynomials Over Finite Field with $$2^{m}$$. **2022**, 555-563	0
335	One-Time Key-Encapsulation Mechanisms: Definitions, Constructions and Cybersecurity Applications.	0
334	On the Effectiveness of True Random Number Generators Implemented on FPGAs. **2022**, 315-326	0
333	Efficient key exchange protocol for industrial internet of things. **2022**,	0

332	Efficiently Masking Polynomial Inversion at´Arbitrary Order. **2022**, 309-326	1
331	A Comparative Study of Privacy-Preserving Homomorphic Encryption Techniques in Cloud Computing. **2022**, 12, 1-11	1
330	Calculating the Sum of Multidigit Values in a Parallel Computational Model. **2022**, 58, 473-480	0
329	Analysis of Network-level Key Exchange Protocols in the Post-Quantum Era. **2022**,	1
328	A Scrutiny Review of CPS 4.0-Based Blockchain With Quantum Resistance. **2022**, 131-157	0
327	Dynamic Quantizer Synthesis for Encrypted State-Feedback Control Systems with Partially Homomorphic Encryption. **2022**,	0
326	Cryptography in the Quantum Era. **2022**,	0
325	Implementation and Analysis of Quantum Homomorphic Encryption. **2022**,	0
324	Research on Encryption Technology of CAA Software Based on RSA Algorithm and Hardware Information Extraction. **2022**,	0
323	Design of Montgomery Multiplier RSA Algorithm. **2022**, 2325, 012022	0
322	Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography.	0
321	On the Existence of Multiple RSA Private Keys. **2022**, 2022, 1-6	0
320	Research on the Used Car System Based on Blockchain and Cryptographic Technology. **2022**, 10, 105-111	0
319	On (Unknowingly) Using Near-Square RSA Primes. **2022**, 14, 1898	0
318	A Low-Storage Blockchain Framework Based on Incentive Pricing Strategies. **2022**, 1, 250-275	1
317	NN-Based 8FSK Demodulator for the Covert Channel. **2022**, 22, 7181	0
316	A Security Scheme for Distributing Analysis Codes Supporting CDM-Based Research in a Multi-Center Environment. **2022**, 107159	0
315	Lightweight noncommutative key exchange protocol for IoT environments. 10,	0

314	Coherence as a Resource for Shor's Algorithm. **2022**, 129,	1
313	Study of Enterprise Internal Control Based on Virtual Team and Cryptology Technique. **2022**, 13, 75-83	0
312	Study of COVID-19 Monitoring System Based on Block Chain and Anonymity Techniques. **2022**, 21, 635-640	0
311	Dynamic DNA coding multi-image encryption based on compound chaos. **2022**, 31,	0
310	Provably efficient machine learning for quantum many-body problems. **2022**, 377,	1
309	Security analysis on an interference-based optical image encryption scheme.	0
308	Hybrid Cryptosystem's Design with AES and SHA-1 Algorithms. **2023**, 65-75	0
307	Unconditionally secure digital signatures implemented in an eight-user quantum network*. **2022**, 24, 093038	0
306	Cloud Computing and Information Security. **2023**, 113-146	0
305	Homomorphic encryption for stochastic computing.	0
304	Illegal Trojan design and detection in asynchronous NULL Convention Logic and Sleep Convention Logic circuits.	0
303	Ergodic Secrecy Capacity Analysis Over Composite Weibull/Inverse Gamma Fading Channel. **2023**, 501-507	0
302	A Novel Personal Medicine Record Scheme Based on Block Chain and Cryptographic. **2022**, 13, 100-106	0
301	Design and Testing of a Computer Security Layer for the LIN Bus. **2022**, 22, 6901	0
300	Small Private Exponent Attacks on RSA Using Continued Fractions and Multicore Systems. **2022**, 14, 1897	2
299	A simulator of optical coherent-state evolution in quantum key distribution systems. **2022**, 54,	0
298	Efficient and HRA Secure Universal Conditional Proxy Re-Encryption for Cloud-Based Data Sharing. **2022**, 12, 9586	0
297	Secured Quantum Key Distribution Encircling Profuse Attacks and Countermeasures. **2023**, 233-241	0

296	Directional modulation techniques for secure wireless communication: a comprehensive survey. **2022**, 2022,	0
295	A probabilistic public key encryption switching scheme for secure cloud storage.	0
294	Federated and Transfer Learning: A Survey on Adversaries and Defense Mechanisms. **2023**, 29-55	0
293	Optical asymmetric JTC cryptosystem based on binary phase modulation and image superposition subtraction operation. **2022**, 61, 8711	1
292	Private key and password protection by steganographic image encryption. **2022**,	0
291	PKIs in C-ITS: Security functions, architectures and projects: A survey. **2022**, 100531	0
290	Scalable high-rate measurement-device-independent quantum key distribution network without reference-frame alignment.	0
289	An IoT Privacy-Oriented selective disclosure credential system. **2022**, 8,	0
288	Practical Statistically-Sound Proofs of Exponentiation in Any Group. **2022**, 370-399	2
287	An Optimization of Bleichenbacher Oracle Padding Attack. **2022**, 145-155	0
286	Authenticated Continuous Top-k Spatial Keyword Search on Dynamic Objects. **2022**, 32-51	0
285	A Multifunctional Modular Implementation of Grover Algorithm. **2022**, 228-247	0
284	On the Impossibility of Key Agreements from Quantum Random Oracles. **2022**, 165-194	1
283	Post-COVID-19 Neural Cryptographic Onset of Homeopathy Psychiatry Medicine Transmission in New Normal Form **2022**, 4,	0
282	Finding Points on Elliptic Curves with Coppersmith Method. **2022**, 69-80	0
281	Quantum Computing Foundations. **2022**, 1-24	0
280	Attack on the Common Prime Version of Murru and Saettone RSA Cryptosystem. **2022**, 32-45	0
279	Impact of Nonbinary Input Vectors on Security of Tree Parity Machine. **2022**, 94-103	0

278	Mutual Authentication of Devices under Multi-Cluster Environment in Industrial Internet of Things (IIoT) Networks. **2022**,	0
277	Security Analysis of One-step QSDC Protocol with Hyperentanglement. **2022**,	0
276	Performance Analysis of LEACH and LEACH-CC Protocol with Cryptographic Algorithms in Wireless Sensor Networks. **2022**,	0
275	The Systems Approach and Design Path of Electronic Bidding Systems Based on Blockchain Technology. **2022**, 11, 3501	0
274	Improved malicious node detection method for detecting a bait in an extensive network for getting the maximum throughput.	0
273	A Comprehensive Survey on the Non-Invasive Passive Side-Channel Analysis. **2022**, 22, 8096	0
272	Data Provenance for Cloud Forensic Investigations, Security, Challenges, Solutions and Future Perspectives: a survey. **2022**,	0
271	SCA-Safe Implementation of Modified SaMAL2R Algorithm in FPGA. **2022**, 13, 1872	1
270	Lightweight and Secure IoT-based Payment Protocols from an Identity-Based Signature Scheme. **2022**, 11, 3445	0
269	e-Voting: I Changed My Mind, Now What?. **2023**, 447-466	0
268	PDF Steganography Using Hybrid Crypto Encryption Technique. **2023**, 453-466	0
267	Secure multicasting in wireless sensor networks using identity based cryptography.	1
266	A Communication-Efficient Secure Routing Protocol for IoT Networks. **2022**, 22, 7503	0
265	Speeding-Up Elliptic Curve Cryptography Algorithms. **2022**, 10, 3676	0
264	A Survey on Wireless Wearable Body Area Networks: A Perspective of Technology and Economy. **2022**, 22, 7722	1
263	Quantum Misuse Attack on Frodo. **2022**, 24, 1418	0
262	A novel traceability approach in IoT paradigm for CP-ABE proxy re-encryption. **2022**, 47,	0
261	Integer Factorization: Why Two-Item Joint Replenishment Is Hard.	0

260	Privacy preserving IoT-based crowd-sensing network with comparable homomorphic encryption and its application in combating COVID19. **2022**, 20, 100625	0
259	A survey of methods for encrypted network traffic fingerprinting. **2022**, 20, 2183-2202	0
258	A Survey of Deep Learning Architectures for Privacy-Preserving Machine Learning With Fully Homomorphic Encryption. **2022**, 10, 117477-117500	0
257	Practical Public Template Attack Attacks on CRYSTALS-Dilithium with Randomness Leakages. **2022**, 1-1	0
256	SEEMQTT: Secure End-to-End MQTT-Based Communication for Mobile IoT Systems Using Secret Sharing and Trust Delegation. **2022**, 1-1	0
255	A Survey of´Ciphertext Processing Techniques. **2022**, 735-747	0
254	Cryptanalysis of´the´Multi-Power RSA Cryptosystem Variant. **2022**, 245-257	0
253	Text Cryptography via Special Polynomial Technique. **2022**, 9,	0
252	Efficient Implementation of ECDH for Sigfox Communication. **2021**,	0
251	Routing and Scheduling of Key Assignment in Optical Networks secured by Quantum Key Distribution. **2021**,	0
250	Homomorphic Encryption between Client and Cloud Server. **2022**,	0
249	Quantum and Post-Quantum Cybersecurity Challenges and Finance Organizations Readiness. **2022**, 314-337	0
248	Privacy-Preserving Computing via Homomorphic Encryption. **2022**, 288-313	0
247	Overview of Medical Data Privacy Protection based on Blockchain Technology. **2022**,	0
246	Efficient RNS Realization of High-Speed Arithmetic Multiplier with Respect to Cryptographic Computation. **2023**, 13-21	0
245	A secure data fitting scheme based on CKKS homomorphic encryption for medical IoT. **2022**, 1-16	0
244	New Constructions of Existential Unforgeable Aggregate Signature Scheme from CSP. **2022**, 2022, 1-13	0
243	New Identified Strategies to Forge Multivariate Signature Schemes. **2022**, 14, 2368	0

242	Equivalent Keys: Side-Channel Countermeasure for Post-Quantum Multivariate Quadratic Signatures. **2022**, 11, 3607	0
241	Quantum key secure communication protocol via enhanced superdense coding. **2023**, 55,	0
240	Side-Channel Analysis of Lattice-Based Post-Quantum Cryptography: Exploiting Polynomial Multiplication.	3
239	Analysis of´Secret Key Agreement Protocol for´Massive MIMO Systems. **2023**, 86-94	0
238	On Advances of Lattice-Based Cryptographic Schemes and Their Implementations. **2022**, 6, 56	0
237	A Raft Algorithm with Byzantine Fault-Tolerant Performance. **2022**,	0
236	Smart Biomedical Sensor Network for Multi-patient Cardiac Arrhythmia Monitoring. **2022**, 1-1	0
235	Further Cryptanalysis of´a´Type of´RSA Variants. **2022**, 133-152	0
234	Fully Continuous Leakage-Resilient Certificate-Based Signcryption Scheme for Mobile Communications. **2022**, 1-24	0
233	Secure Teleoperation Control Using Somewhat Homomorphic Encryption. **2022**, 55, 593-600	0
232	Cryptography: Confidentiality. **2022**, 13-41	0
231	FedDual: Pair-Wise Gossip Helps Federated Learning in Large Decentralized Networks. **2023**, 18, 335-350	0
230	TPPD: Targeted Pseudo Partitioning based Defence for cross-core covert channel attacks. **2023**, 135, 102805	0
229	Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. **2023**, 47, 100530	1
228	Secure HPC: A workflow providing a secure partition on an HPC system. **2023**, 141, 677-691	0
227	Optical asymmetric JTC cryptosystem based on multiplication-division operation and RSA algorithm. **2023**, 160, 109042	1
226	A Review of Blockchain Solutions in Supply Chain Traceability. **2023**, 28, 500-510	0
225	Continued Fractions Applied to´a´Family of´RSA-like Cryptosystems. **2022**, 589-605	0

224	Privacy-Preserving Intelligent Resource Allocation for Federated Edge Learning in Quantum Internet. **2022**, 1-15	0
223	The SPN Network for Digital Audio Data Based on Elliptic Curve Over a Finite Field. **2022**, 10, 127939-127955	1
222	EG-Four$mathbb {Q}$: An Embedded GPU Based Efficient ECC Cryptography Accelerator for Edge Computing. **2022**, 1-10	0
221	Cryptography: Integrity and Authenticity. **2022**, 43-62	0
220	A Key Recovery Protocol for Multiparty Threshold ECDSA Schemes. **2022**, 1-1	0
219	Public-Key Encryption from´Homogeneous CLWE. **2022**, 565-592	0
218	TIDE: A Novel Approach to´Constructing Timed-Release Encryption. **2022**, 244-264	1
217	Cyber Security. **2023**, 223-244	0
216	Efficient Word Size Modular Multiplication over Signed Integers. **2022**,	0
215	Benchmark Performance of a New Quantum-Safe Multivariate Polynomial Digital Signature Algorithm. **2022**,	0
214	Public Key Cryptographic Implementation Validation: A Review. **2022**,	0
213	Identity-Based Deterministic Proxy Re-Encryption Scheme on Lattice. **2022**,	0
212	Analysis of Message Authentication Solutions for IEC 61850 in Substation Automation Systems. **2022**,	1
211	A Comprehensive Survey on Quantum Machine Learning and Possible Applications. **2022**, 13, 1-17	0
210	Asymptotic Bound for RSA Variant With Three Decryption Exponents.	0
209	Biology and medicine in the landscape of quantum advantages. **2022**, 19,	0
208	Cryptanaylsis to´Sowjanya et al.s ABEs from´ECC. **2023**, 287-294	0
207	Symmetric text encryption scheme based Karhunen Loeve transform. **2022**, 25, 2773-2781	0

206	Provably secure arbitrated-quantum signature. **2022**, 21,	0
205	A Blockchain-Based Fair and Transparent Homework Grading System for Online Education. **2023**, 303-326	0
204	Using Hopfield Networks to Correct Instruction Faults. **2022**,	0
203	Secure Federated Learning. **2023**, 165-212	0
202	Integrity of virtual testing for crash protection. 3,	0
201	Efficient Sequential and Parallel Prime Sieve Algorithms. **2022**, 14, 2527	1
200	Secured V2x Communication Using Optimized Prime Field Ecc Architecture.	0
199	Groups of prime degree and the Bateman–Horn Conjecture. **2022**,	0
198	Software Tool for Parallel Generation of Cryptographic Keys Based on Elliptic Curves. **2022**,	0
197	Public-Key Encryption and Security Notions. **2022**, 1-45	0
196	Post-Quantum Digital Signatures in Transport Documents. **2022**,	0
195	Balancing Security and Privacy in Genomic Range Queries*.	0
194	Numerical simulation of quantum key distribution network based on wavelength division multiplexing technology. **2022**, 2381, 012082	0
193	SDA-RDOS: A New Secure Data Aggregation Protocol for Wireless Sensor Networks in IoT Resistant to DOS Attacks. **2022**, 11, 4194	0
192	A Simple Algorithm for Prime Factorization and Primality Testing. **2022**, 2022, 1-10	0
191	Minicrypt Primitives with Algebraic Structure and Applications. **2023**, 36,	0
190	A novel hybrid authentication protocol utilizing lattice-based cryptography for IoT devices in fog networks. **2022**,	0
189	A Review on Security Issues and Solutions for Precision Health in Internet-of-Medical-Things Systems.	0

188	Privacy-Preserved Image Protection Supporting Different Access Rights. **2022**, 12, 12335	0
187	Offline User Authentication Ensuring Non-Repudiation and Anonymity. **2022**, 22, 9673	0
186	Cryptosystem with public keys and public operations.	0
185	Improved and Provably Secure ECC-Based Two-Factor Remote Authentication Scheme with Session Key Agreement. **2023**, 11, 5	0
184	Privacy preserving or trapping?.	0
183	Differential privacy: Review of improving utility through cryptography-based technologies.	0
182	Cryptosystem with public keys and public operations.	0
181	Mathematical Tools. **2011**, 911-943	0
180	Copyright Page. **2011**, iv-iv	0
179	Figure Credits. **2011**, xii-xiv	0
178	Dedication. **2011**, v-v	0
177	Preface. **2011**, xv-xvii	0
176	Make Your Query Anonymous With Oblivious Transfer. **2015**,	1
175	A Quantum Version of Pollard Rho of Which Shor Algorithm is a Particular Case. **2022**, 212-219	0
174	Quantum reversible circuits for $${text {GF}}(2^8)$$ multiplication based on composite field arithmetic operations. **2023**, 22,	0
173	Mul-IBS: a multivariate identity-based signature scheme compatible with IoT-based NDN architecture.	0
172	HE-Booster: An Efficient Polynomial Arithmetic Acceleration on GPUs for Fully Homomorphic Encryption. **2023**, 1-17	1
171	The Satoshi laundromat: a review on the money laundering open door of Bitcoin mixers.	0

170	Revisiting lower dimension lattice attacks on NTRU. **2023**, 106353	0
169	Quantifying Dark Web Shops□llicit Revenue. **2023**, 11, 4794-4808	0
168	Cosmic Coding and Transfer (COSMOCAT) for Ultra High Security Near-Field Communications. **2023**, 105897	0
167	Overview of ́Multiple User Encryption for ́Exchange of ́Private Data via ́Blockchains. **2023**, 447-453	0
166	Polar Codes for Module-LWE Public Key Encryption: The Case of Kyber. **2023**, 7, 2	0
165	Toward Lightweight Cryptography: A Survey.	0
164	Multi-Functional Resource-Constrained Elliptic Curve Cryptographic Processor. **2023**, 11, 4879-4894	0
163	Large Field-Size Elliptic Curve Processor for Area-Constrained Applications. **2023**, 13, 1240	0
162	Secure, Verifiable Object Identities as Enablerfor Value Creation in Distributed Networks. **2023**, 209-222	0
161	Large Field-Size Throughput/Area Accelerator for Elliptic-Curve Point Multiplication on FPGA. **2023**, 13, 869	0
160	Redactable Blockchain: Comprehensive Review, Mechanisms, Challenges, Open Issues and Future Research Directions. **2023**, 15, 35	0
159	A new quantum multi-party signature protocol based on SNOP states without arbitrator. **2023**, 611, 128453	0
158	LWR-based Quantum-Safe Pseudo-Random Number Generator. **2023**, 73, 103431	0
157	FPGA implementation of BIKE for quantum-resistant TLS. **2022**,	0
156	Leveled Homomorphic Encryption Based on Finite Field Isomorphism Problem Over Matrix Algebra. **2022**,	0
155	RSA-based Encryption Algorithm for Digital Images. **2022**,	0
154	Voice Privacy in Biometrics. **2023**, 1-29	0
153	Design of Hazard Management Method Based on Blockchain. **2022**,	0

152	Fundamental Cryptographic Algorithms and Technologies. **2023**, 17-27	0
151	The Fast Paillier Decryption with Montgomery Modular Multiplication Based on OpenMP. **2022**,	0
150	Parallel Methods of Representing Multidigit Numbers in Numeral Systems for Testing Multidigit Arithmetic Operations. **2022**, 58, 991-1007	0
149	DSVN: A Flexible and Secure Data-Sharing Model for VANET Based on Blockchain. **2023**, 13, 217	0
148	Fast Modular Exponentiation Methods for Public-Key Cryptography. **2022**,	0
147	Quantum-resistant public-key encryption and signature schemes with smaller key sizes.	0
146	A Review of the Key Technology in a Blockchain Building Decentralized Trust Platform. **2023**, 11, 101	0
145	A Fully Homomorphic Encryption Scheme for Real-Time Safe Control. **2022**,	0
144	Communication-friendly threshold trapdoor function from weaker assumption for distributed cryptography.	0
143	A Smart Contract-Based Access Control Framework For Smart Healthcare Systems.	0
142	Research on Medical Data Storage and Sharing Model Based on Blockchain. **2022**,	0
141	A Survey on Big Data Technologies and Their Applications to the Metaverse: Past, Current and Future. **2023**, 11, 96	0
140	Tower Building Technique on Elliptic Curve with Embedding Degree 36. **2022**, 21, 325-335	1
139	Promoting a Hybrid Cryptosystem System Security based on Fresnel lens and RSA Algorithm. **2022** ,	0
138	DYNAMIC ENCODING OF THE TRANSFORMER VIDEO IMAGES WITH REFINEMENT OF THE BASE SYSTEM. **2022**, 2, 1-11	0
137	Frontmatter. **2022**, 1-4	0
136	6. Schluss. **2022**, 227-230	0
135	A Study on Partially Homomorphic Encryption. **2023**,	0

134	Incorrectly Generated RSA Keys: How I Learned To Stop Worrying And Recover Lost Plaintexts.	0
133	Symmetrical Disguise: Realizing Homomorphic Encryption Services from Symmetric Primitives. **2023**, 353-370	0
132	A Lattice-Based Multisignature Scheme for Blockchain-Enabled Systems. **2023**, 336-346	0
131	PP-DDP: a privacy-preserving outsourcing framework for solving the double digest problem. **2023**, 24,	0
130	Implementing Data Exfiltration Defense in Situ: A Survey of Countermeasures and Human Involvement.	0
129	Securing Optical Networks Using Quantum-Secured Blockchain: An Overview. **2023**, 23, 1228	0
128	A Multifactor Ring Signature based Authentication Scheme for Quality Assessment of IoMT Environment in COVID-19 Scenario.	1
127	An Image Encryption-Based Method for Handwritten Digit Recognition. **2023**, 18-26	0
126	Steganography algorithm based on public key cryptosystem. **2023**,	0
125	Pairing based cryptography New random point exchange key protocol. **2022**,	0
124	Accelerating Elliptic Curve Digital Signature Algorithms on GPUs. **2022**,	0
123	Tower Building Technique on Elliptic Curve with Embedding Degree 72. **2022**, 10, 126-138	0
122	2. Kryptographische Sicherheitsbestimmungen. **2022**, 23-88	0
121	Literatur und weitere Quellen. **2022**, 231-252	0
120	Quantity-Simulation-Analysis Method based Novel RSA Timing Attack Algorithm for Single-Chip Microcomputer Platform. **2022**,	0
119	Achieving a Lawfully-Secure Audio Recording Framework using Consumer Electronics. **2023**,	0
118	FPGA Based Optimized Design of Montgomery Modular Multiplier using Karatsuba Algorithm. **2023**,	0
117	Fast and Lightweight Authenticated Group Key Agreement Realizing Privacy Protection for Resource-Constrained IoMT. **2023**, 129, 2403-2417	0

116	Future of virtual education and telementoring. **2023**, 34, 255-260	0
115	On the security of multivariate-based ring signature and other related primitives. **2023**, 74, 103474	0
114	An Improved NSGA-III Algorithm Based on Deep Q-Networks for Cloud Storage Optimization of Blockchain. **2023**, 34, 1406-1419	0
113	Deterministic or probabilistic? - A survey on Byzantine fault tolerant state machine replication. **2023**, 129, 103200	0
112	Structured encryption for triangle counting on graph data. **2023**, 145, 200-210	0
111	Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. **2023**, 162, 113859	0
110	High performance HITA based Binary Edward Curve Crypto processor for FPGA platforms. **2023**, 178, 56-68	0
109	Performance Evaluation of Cryptographic Schemes for Blockchain Security of Smart Grids. **2022**,	0
108	Dematerialization of Public Procurement Approach Based on Hyperledger Fabric Blockchain using OCDS. **2022**,	0
107	Research on An Encryption Method Combining RSA and Hill Cipher. **2022**,	0
106	A reversible system based on hybrid toggle radius-4 cellular automata and its application as a block cipher.	0
105	Scalable set of reversible parity gates for integer factorization. **2023**, 6,	0
104	An effective revocable and traceable public auditing scheme for sensor-based urban cities. **2023**, 35, 152-160	0
103	Scalable Cryptography. **2022**, 169-178	0
102	Blockchain-Technologie. **2022**, 121-176	0
101	On the improvement of McEliece cryptosystem based on LDPC codes. **2022**,	0
100	5. F□einen queeren Sicherheitsbegriff. **2022**, 187-226	0
99	1. Einleitung. **2022**, 7-22	0

98	Short-lived Zero-Knowledge Proofs and Signatures. **2022**, 487-516	1
97	Die unsicheren Kanäle. **2022**,	0
96	Danksagungen. **2022**, 253-258	0
95	3. IT-Sicherheit: Digitale Grenzaushandlungen. **2022**, 89-144	0
94	Inhalt. **2022**, 5-6	0
93	4. Backdoors. **2022**, 145-186	0
92	Secure Automated Video Assistance in Vehicular Networks using Unmanned Aerial Vehicles. **2022**,	0
91	A blockchain based virtual machine detection system app market. **2023**,	0
90	Quantum Advantage in Cryptography. **2023**, 61, 1895-1910	0
89	A Novel Hybrid Multikey Cryptography Technique for Video Communication. **2023**, 11, 15693-15700	0
88	Security of underwater and air–water wireless communication: State-of-the-art, challenges and outlook. **2023**, 142, 103114	0
87	Analysis of the shortest vector problems with quantum annealing to search the excited states. **2023**, 62, SC1090	0
86	Distributed LSTM-Learning from Differentially Private Label Proportions. **2022**,	0
85	Array-Antenna Power-Pattern Analysis Through Quantum Computing. **2023**, 71, 3251-3259	0
84	A Robust Two Factor Authentication Scheme with Fine Grained Biometrics Verification. **2022**, 407-418	0
83	A Secure Order-Preserving Encryption Scheme Based on Encrypted Index. **2023**, 247-261	0
82	A Privacy-Preserving Ride Matching Scheme for Ride Sharing Services in a Hot Spot Area. **2023**, 12, 915	0
81	What are the trend and core knowledge of information security? A citation and co-citation analysis. **2023**, 60, 103774	0

80	A Polynomial Multiplication Accelerator for Faster Lattice Cipher Algorithm in Security Chip. **2023**, 12, 951	0
79	The cost of privacy on blockchain: A study on sealed-bid auctions. **2023**, 100133	0
78	Silicon-based decoder for polarization-encoding quantum key distribution. **2023**, 2, 100039	0
77	Development and Examination of Secure Quadcopter Control System with Partially Homomorphic Encryption. **2023**,	0
76	Security Verification of an Authentication Algorithm Based on Verifiable Encryption. **2023**, 14, 126	0
75	Sequential and parallel sliding window algorithms for multiplying large integers. **2023**, 35, 131-140	0
74	Porting the Paillier Algorithm for Homomorphic Encryption on Portable Devices. **2023**,	1
73	HEDA. **2022**, 16, 601-614	0
72	Free-Space Quantum Secure Direct Communication: Basics, Progress, and Outlook. **2023**, 4,	0
71	Range free localization in WSN against wormhole attack using Farkas□Lemma.	0
70	Decentralized Multi-authority ABE for $$textsf{NC}^1$$ from BDH. **2023**, 36,	0
69	An overview of blockchain efficient interaction technologies. 6,	0
68	Acceleration of Wheel Factoring Techniques. **2023**, 11, 1203	0
67	Security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective. **2023**, 100135	0
66	Tower Building Technique on Elliptic Curve with Embedding Degree 18. **2023**, 83, 103-118	0
65	Quantum asymmetric key crypto scheme using Grover iteration. **2023**, 13,	0
64	Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems.	0
63	Side-channel analysis against ANSSI□s protected AES implementation on ARM: end-to-end attacks with multi-task learning.	0

62	A Novel Technique to Compress Photoplethysmogram Signal: Improvised with Particle Swarm Optimization and Rivest-Shamir-Adleman Algorithm. **2022**,	0
61	Tree Parity Machine-Based Symmetric Encryption: A Hybrid Approach. **2022**, 61-73	0
60	Distributed Cyber-infrastructures and Artificial Intelligence in Hybrid Post-Quantum Era. **2022**,	0
59	Federated Ensemble Algorithm Based on Deep Neural Network. **2023**, 76-91	0
58	RSA Cryptosystem for Rings with Commuting Ideals. **2022**, 43, 3591-3596	0
57	Extremely Lightweight Constant-Round Membership-Authenticated Group Key Establishment for Resource-Constrained Smart Environments toward 5G.	0
56	A Stealthy False Command Injection Attack on Modbus based SCADA Systems. **2023**,	0
55	Perceval: A Software Platform for Discrete Variable Photonic Quantum Computing. 7, 931	0
54	A Method of Scrambling for the System of Cryptocompression of Codograms Service Components. **2023**, 444-459	0
53	Secure and Lightweight Authentication Protocol for Privacy Preserving Communications in Smart City Applications. **2023**, 15, 5346	0
52	A Survey on Homomorphic Encryption for Biometrics Template Security Based on Machine Learning Models. **2023**,	0
51	Robust polarization state generation for long-range quantum key distribution. **2023**, 31, 13700	0
50	LCAM: Lightweight Certificate Authority for MANET and Securing DSR Routing Protocol.	0
49	Processing Marker Arrays of Clustered Transformants for Image Segments. **2023**, 428-443	0
48	Protecting Street Art Rights Using an NFT-Based System. 1-20	0
47	Research on an Encryption Algorithm of H.265 Video File. **2022**,	0
46	Comparison of Quantum and Classical Algorithm in Searching a Number in a Database Case. 38, 370-376	0
45	State-of-the-art session key generation on priority-based adaptive neural machine (PANM) in telemedicine. **2023**, 35, 9517-9533	0

44	Administration of Digital Identities Using Blockchain. **2022**,	0
43	Cryptanalysis to Ming et al.'s Revocable Multi-Authority Attribute-Based Encryption. **2022**,	0
42	Cryptanalysis and Discussion on Two Attribute-Based Encryption Schemes. **2022**,	0
41	New Digital Signature Scheme Based on RSA Using Circulant Matrix. **2023**, 4,	0
40	A typology of secure multicast communication over 5´G/6´G networks.	0
39	A Study of Reversible Data Hiding Technology with an Authentication Function. **2022**,	0
38	Privacy Protection Method for Online Medical Diagnosis Based on Attribute and Proxy Re-encryption. **2022**,	0
37	Some Properties of the Computation of the Modular Inverse with Applications in Cryptography. **2023**, 11, 70	0
36	A Unified Point Multiplication Architecture of Weierstrass, Edward and Huff Elliptic Curves on FPGA. **2023**, 13, 4194	0
35	Elektronik Posta Sistemine □c□Taraf G□veni Gerektirmeyen Bir □□h □erisi. **2023**, 12, 393-418	0
34	High-speed SABER key encapsulation mechanism in 65nm CMOS.	0
33	A Review of Homomorphic Encryption for Privacy-Preserving Biometrics. **2023**, 23, 3566	0
32	Fully Homomorphic Encryption Accelerator Using DSP Embedded Multiplier. **2023**,	0
31	Cybersecurity Systems Modeling: An Automotive System Case Study. **2023**, 1-33	0
30	A Robust and Effective Two-Factor Authentication (2FA) Protocol Based on ECC for Mobile Computing. **2023**, 13, 4425	0
29	ShEnc: A Versatile Secure Multi-Party Data Sharing Framework. **2023**,	0
28	Public-Key Cryptography behind Blockchain Security. **2022**,	0
27	Weak-Key Analysis for BIKE Post-Quantum Key Encapsulation Mechanism. **2023**, 18, 2160-2174	0

26	Solving Generalized Bivariate Integer Equations and Its Application to Factoring With Known Bits. **2023**, 11, 34674-34684	0
25	Quantum-resistance in blockchain networks. **2023**, 13,	0
24	Privacy-preserving multi-party PCA computation on horizontally and vertically partitioned data based on outsourced QR decomposition.	0
23	Design of IsoQER Cryptosystem using IPDLP. **2022**,	0
22	Encrypted model predictive control design for security to cyberattacks.	0
21	DNA Dynamic Coding-based Encryption Algorithm for Vector Map Considering Global Objects.	0
20	Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together. 2,	0
19	A survey on implementations of homomorphic encryption schemes.	0
18	Secure Control Using Homomorphic Encryption and Efficiency Analysis. **2023**, 2023, 1-12	0
17	FPGA Implementation of High Performance Hybrid Encryption Standard. **2022**,	0
16	A Survey of Privacy Preservation for Deep Learning Applications. **2022**, 4, 69-78	0
15	Implementing Privacy on Public Digital Displays Using Smart Glasses. **2023**,	0
14	Concrete Quantum Cryptanalysis of ´Binary Elliptic Curves via´Addition Chain. **2023**, 57-83	0
13	Lightweight Lattice-Based Signature for VANET. **2022**,	0
12	Study on Modified Public Key Cryptosystem Based on ElGamal and Cramer-Shoup Cryptosystems. **2023**,	0
11	Toward a common standard for data and specimen provenance in life sciences.	0
10	Side-Channel Resistant 2048-bit RSA Implementation for Wireless Sensor Networks and Internet of Things. **2023**, 1-1	0
9	Using Single Time of Quantum Computer for Shor's Factoring Algorithm. **2023**,	0

8	Improving The Security of E-Exam Systems. **2023**,	0
7	Algorithms for Implementing Repeated Homomorphic Operations on Restricted Data Type Ranges. **2023**,	0
6	Decentralized Inverse Transparency With Blockchain.	0
5	Grote: Group Testing for Privacy-Preserving Face Identification. **2023**,	0
4	Unlocking the Potential of Fully Homomorphic Encryption. **2023**, 66, 72-81	0
3	Theoretical Analysis and Software Implementation of a Quantum Encryption Proposal. **2023**,	0
2	A quantum secure direct communication scheme based on intermediate-basis. **2023**, 18,	0
1	An efficient encoding mechanism against eavesdropper with side channel information. **2023**, 153, 111062	0