Noboru Kunihiro

List of Publications by Year in descending order

Source: https://exaly.com/author-pdf/8053697/publications.pdf

Version: 2024-02-01

106

papers

733

citations

687220

13

h-index

713332

21

g-index

111

all docs

111

docs citations

111

times ranked

268

citing authors

#	Article	IF	Citations
1	Generic Constructions for Chosen-Ciphertext Secure Attribute Based Encryption. Lecture Notes in Computer Science, 2011, , 71-89.	1.0	55
2	Generic Construction of Chosen Ciphertext Secure Proxy Re-Encryption. Lecture Notes in Computer Science, 2012, , 349-364.	1.0	52
3	A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption. Lecture Notes in Computer Science, 2014, , 275-292.	1.0	50
4	New Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5. , 2008, , 237-253.		27
5	Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication. Lecture Notes in Computer Science, 2012, , 243-261.	1.0	24
6	Partial Key Exposure Attacks on RSA: Achieving the Boneh-Durfee Bound. Lecture Notes in Computer Science, 2014, , 345-362.	1.0	23
7	Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors. Lecture Notes in Computer Science, 2013, , 118-135.	1.0	18
8	Small Secret Key Attack on a Variant of RSA (Due to Takagi). Lecture Notes in Computer Science, 2008, , 387-406.	1.0	16
9	A Sanitizable Signature Scheme with Aggregation. , 2007, , 51-64.		15
10	Multi-party Key Exchange Protocols from Supersingular Isogenies. , 2018, , .		15
11	Security of MD5 Challenge and Response: Extension of APOP Password Recovery Attack. Lecture Notes in Computer Science, 2008, , 1-18.	1.0	15
12	Cryptanalysis of RSA with Multiple Small Secret Exponents. Lecture Notes in Computer Science, 2014, , 176-191.	1.0	14
13	New Definition of Density on Knapsack Cryptosystems. , 2008, , 156-173.		14
14	Sanitizable and Deletable Signature. Lecture Notes in Computer Science, 2009, , 130-144.	1.0	13
15	Two-Dimensional Representation of Cover Free Families and Its Applications: Short Signatures and More. Lecture Notes in Computer Science, 2012, , 260-277.	1.0	13
16	Symmetric Inner-Product Predicate Encryption Based on Three Groups. Lecture Notes in Computer Science, 2012, , 215-234.	1.0	13
17	Self-bilinear Map on Unknown Order Groups from Indistinguishability Obfuscation and Its Applications. Lecture Notes in Computer Science, 2014, , 90-107.	1.0	13
18	How to Generalize RSA Cryptanalyses. Lecture Notes in Computer Science, 2016, , 67-97.	1.0	13

#	Article	IF	Citations
19	Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, E97.A, 1259-1272.	0.2	12
20	Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors. Lecture Notes in Computer Science, 2013, , 180-197.	1.0	11
21	New Message Difference for MD4. Lecture Notes in Computer Science, 2007, , 329-348.	1.0	10
22	Public Key Encryption Schemes from the (B)CDH Assumption with Better Efficiency. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 1984-1993.	0.2	10
23	Equivalence of counting the number of points on elliptic curve over the ring Zn and factoring n. Lecture Notes in Computer Science, 1998, , 47-58.	1.0	9
24	A Tool Kit for Partial Key Exposure Attacks on RSA. Lecture Notes in Computer Science, 2017, , 58-73.	1.0	9
25	Optimal Bounds for Multi-Prime Î¦-Hiding Assumption. Lecture Notes in Computer Science, 2012, , 1-14.	1.0	9
26	Extended partial key exposure attacks on RSA: Improvement up to full size decryption exponents. Theoretical Computer Science, 2020, 841, 62-83.	0.5	8
27	Partial Key Exposure Attacks on CRT-RSA: Better Cryptanalysis to Full Size Encryption Exponents. Lecture Notes in Computer Science, 2015, , 518-537.	1.0	8
28	Solving Generalized Small Inverse Problems. Lecture Notes in Computer Science, 2010, , 248-263.	1.0	8
29	A Unified Framework for Small Secret Exponent Attack on RSA. Lecture Notes in Computer Science, 2012, , 260-277.	1.0	8
30	A strict evaluation method on the number of conditions for the SHA-1 collision search. , 2008, , .		7
31	Partial key exposure attacks on RSA: Achieving the Bonehâ€"Durfee bound. Theoretical Computer Science, 2019, 761, 51-77.	0.5	7
32	Improved Collision Attack on MD4 with Probability Almost 1. Lecture Notes in Computer Science, 2006, , 129-145.	1.0	7
33	On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree. Lecture Notes in Computer Science, 2012, , 55-69.	1.0	7
34	General Bounds for Small Inverse Problems and Its Applications to Multi-Prime RSA. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 50-61.	0.2	7
35	Small Secret Key Attack on a Takagi's Variant of RSA. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 33-41.	0.2	7
36	Deterministic Polynomial Time Equivalence Between Factoring and Key-Recovery Attack on Takagiâ€™s RSA. , 2007, , 412-425.		7

#	Article	IF	Citations
37	Efficient Construction of a Control Modular Adder on a Carry-Lookahead Adder Using Relative-Phase Toffoli Gates. IEEE Transactions on Quantum Engineering, 2022, 3, 1-18.	2.9	7
38	Password recovery attack on authentication protocol MD4(Password||Challenge). , 2008, , .		6
39	Self-Bilinear Map on Unknown Order Groups from Indistinguishability Obfuscation and Its Applications. Algorithmica, 2017, 79, 1286-1317.	1.0	6
40	Cryptanalysis of the RSA variant based on cubic Pell equation. Theoretical Computer Science, 2021, 889, 135-144.	0.5	6
41	General Bounds for Small Inverse Problems and Its Applications to Multi-Prime RSA. Lecture Notes in Computer Science, 2015, , 3-17.	1.0	6
42	Solving Generalized Small Inverse Problems. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 1274-1284.	0.2	6
43	A Unified Framework for Small Secret Exponent Attack on RSA. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, E97.A, 1285-1295.	0.2	6
44	Partial Key Exposure Attacks on RSA with Multiple Exponent Pairs. Lecture Notes in Computer Science, 2016, , 243-257.	1.0	5
45	Searchable symmetric encryption capable of searching for an arbitrary string. Security and Communication Networks, 2016, 9, 1726-1736.	1.0	5
46	Mis-operation Resistant Searchable Homomorphic Encryption. , 2017, , .		5
47	Cryptanalysis of RSA Variants withÂModified Euler Quotient. Lecture Notes in Computer Science, 2018, , 266-281.	1.0	5
48	Adversary-Dependent Lossy Trapdoor Function from Hardness of Factoring Semi-smooth RSA Subgroup Moduli. Lecture Notes in Computer Science, 2016, , 3-32.	1.0	5
49	Yet Another Sanitizable Signature from Bilinear Maps. , 2009, , .		4
50	Yet Another Sanitizable and Deletable Signatures. , 2011, , .		4
51	Improved Key Recovery Algorithms from Noisy RSA Secret Keys with Analog Noise. Lecture Notes in Computer Science, 2017, , 328-343.	1.0	4
52	A New Strategy for Finding a Differential Path of SHA-1. Lecture Notes in Computer Science, 2007, , 45-58.	1.0	4
53	Small Secret CRT-Exponent Attacks on Takagi's RSA. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 19-27.	0.2	4
54	An Improved Attack for Recovering Noisy RSA Secret Keys and Its Countermeasure. Lecture Notes in Computer Science, 2015, , 61-81.	1.0	3

#	Article	IF	Citations
55	Decryption of Frequent Password Hashes in Rainbow Tables. , 2016, , .		3
56	Partial Key Exposure Attacks on CRT-RSA: General Improvement for the Exposed Least Significant Bits. Lecture Notes in Computer Science, 2016, , 35-47.	1.0	3
57	Bounds in Various Generalized Settings of the Discrete Logarithm Problem. Lecture Notes in Computer Science, 2017, , 498-517.	1.0	3
58	Recent Progress on Coppersmithâ€™s Lattice-Based Method: A Survey. Mathematics for Industry, 2018, , 297-312.	0.4	3
59	Reducing Public Key Sizes in Bounded CCA-Secure KEMs with Optimal Ciphertext Length. Lecture Notes in Computer Science, 2015, , 100-109.	1.0	3
60	Password Recovery on Challenge and Response: Impossible Differential Attack on Hash Function. , 2008, , 290-307.		3
61	Space Efficient Signature Schemes from the RSA Assumption. Lecture Notes in Computer Science, 2012, , 102-119.	1.0	3
62	Multi-differential Cryptanalysis on Reduced DM-PRESENT-80: Collisions and Other Differential Properties. Lecture Notes in Computer Science, 2013, , 352-367.	1.0	3
63	Improved CRT-RSA Secret Key Recovery Method from Sliding Window Leakage. Lecture Notes in Computer Science, 2020, , 278-296.	1.0	3
64	Extension of Secret Handshake Protocols with Multiple Groups in Monotone Condition. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 1122-1131.	0.2	2
65	Private Information Retrieval with Preprocessing Based on the Approximate GCD Problem. Lecture Notes in Computer Science, 2016, , 227-240.	1.0	2
66	On the Security Proof of an Authentication Protocol from Eurocrypt 2011. Lecture Notes in Computer Science, 2014, , 187-203.	1.0	2
67	Generalized Security Analysis of the Random Key Bits Leakage Attack. Lecture Notes in Computer Science, 2012, , 13-27.	1.0	2
68	A Strict Evaluation on the Number of Conditions for SHA-1 Collision Search. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 87-95.	0.2	2
69	Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, E97.A, 1273-1284.	0.2	2
70	Inference Attacks on Encrypted Databases Based on Order Preserving Assignment Problem. Lecture Notes in Computer Science, 2018, , 35-47.	1.0	2
71	Attacking Noisy Secret CRT-RSA Exponents in Binary Method. Lecture Notes in Computer Science, 2019, , 37-54.	1.0	2
72	Cryptanalysis of Two MD5-Based Authentication Protocols: APOP and NMAC. IEICE Transactions on Information and Systems, 2010, E93-D, 1087-1095.	0.4	1

#	Article	IF	Citations
73	On the Hardness of Subset Sum Problem from Different Intervals. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95.A, 903-908.	0.2	1
74	Secret handshake scheme with request-based-revealing. Computers and Mathematics With Applications, 2013, 65, 786-798.	1.4	1
75	Decentralized Netting Protocol over Consortium Blockchain. , 2018, , .		1
76	Outsourced Private Function Evaluation with Privacy Policy Enforcement. , 2018, , .		1
77	Strong security of linear ramp secret sharing schemes with general access structures. Information Processing Letters, 2020, 164, 106018.	0.4	1
78	Generic hardness of inversion on ring and its relation to self-bilinear map. Theoretical Computer Science, 2020, 820, 60-84.	0.5	1
79	Secret Handshake Scheme with Request-Based-Revealing. Lecture Notes in Computer Science, 2012, , 1-16.	1.0	1
80	Near-Collision Attacks on MD4: Applied to MD4-Based Protocols. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 76-86.	0.2	1
81	Chosen Ciphertext Security on Hard Membership Decision Groups: The Case of Semi-smooth Subgroups of Quadratic Residues. Lecture Notes in Computer Science, 2014, , 558-577.	1.0	1
82	Generalized Hardness Assumption for Self-bilinear Map with Auxiliary Information. Lecture Notes in Computer Science, 2016, , 269-284.	1.0	1
83	Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference. Lecture Notes in Computer Science, 2017, , 324-342.	1.0	1
84	A Deterministic Algorithm for Computing Divisors in an Interval. Lecture Notes in Computer Science, 2018, , 3-12.	1.0	1
85	Recovering CRT-RSA Secret Keys from Noisy Square-and-Multiply Sequences in the Sliding Window Method. Lecture Notes in Computer Science, 2020, , 642-652.	1.0	1
86	Efficient algorithms for NMR quantum computers with small qubits. New Generation Computing, 2003, 21, 329-337.	2.5	0
87	A quantum algorithm using NMR computers to break secret-key cryptosystems. New Generation Computing, 2003, 21, 347-361.	2.5	0
88	New Conditions for Secure Knapsack Schemes against Lattice Attack. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 1058-1065.	0.2	0
89	An Evaluation of the Sieving Device YASD for 1024-Bit Integers. , 2010, , .		0
90	Recent Results on Lattice-Based Cryptanalysis. Ieice Ess Fundamentals Review, 2011, 5, 42-55.	0.1	0

#	Article	IF	Citations
91	Efficient variants of the Naor-Yung and Dolev-Dwork-Naor transforms for CCA secure key encapsulation mechanism. , 2013, , .		0
92	A limitation on security evaluation of cryptographic primitives with fixed keys. Security and Communication Networks, 2016, 9, 1663-1675.	1.0	0
93	Partial Server Side Parameter Selection in Private Information Retrieval. , 2016, , .		0
94	Mathematical Approach for Recovering Secret Key from Its Noisy Version. Mathematics for Industry, 2018, , 199-217.	0.4	0
95	Optimal Multiple Assignment Schemes Using Ideal Multipartite Secret Sharing Schemes. , 2019, , .		0
96	Strongly Secure Ramp Secret Sharing Schemes from Any Linear Secret Sharing Schemes. , 2019, , .		0
97	Worst case short lattice vector enumeration on block reduced bases of arbitrary blocksizes. Discrete Applied Mathematics, 2020, 277, 198-220.	0.5	0
98	Extended Password Recovery Attacks against APOP, SIP, and Digest Authentication. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 96-104.	0.2	0
99	Practical Password Recovery Attacks on MD4 Based Prefix and Hybrid Authentication Protocols. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 84-92.	0.2	0
100	Toward an Easy-to-Understand Structure for Achieving Chosen Ciphertext Security from the Decisional Diffie-Hellman Assumption. Lecture Notes in Computer Science, 2010, , 229-243.	1.0	0
101	Random Sampling Reduction with Precomputation. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, E96.A, 150-157.	0.2	0
102	Security Analysis on AUTH Protocol and Its Variant against the Man-in-the-Middle Attack. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 153-161.	0.2	0
103	Improved Differential Fault Analysis on Camellia-128. Lecture Notes in Computer Science, 2016, , 130-143.	1.0	0
104	Constructing Subspace Membership Encryption through Inner Product Encryption. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1804-1815.	0.2	0
105	Solving the DLP with Low Hamming Weight Product Exponents and Improved Attacks on the GPS Identification Scheme. Lecture Notes in Computer Science, 2017, , 460-467.	1.0	0
106	Certifying Variant of RSA with Generalized Moduli. Lecture Notes in Computer Science, 2018, , 598-608.	1.0	0