Goichiro Hanaoka

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/773930/publications.pdf

Version: 2024-02-01

151	1,609	361045	414034
papers	citations	20 h-index	32 g-index

157	157	157	603
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Efficient Chosen Ciphertext Secure Public Key Encryption under the Computational Diffie-Hellman Assumption. Lecture Notes in Computer Science, 2008, , 308-325.	1.0	74
2	Bounded CCA2-Secure Encryption. Lecture Notes in Computer Science, 2007, , 502-518.	1.0	62
3	Generic Constructions for Chosen-Ciphertext Secure Attribute Based Encryption. Lecture Notes in Computer Science, 2011, , 71-89.	1.0	55
4	Generic Construction of Chosen Ciphertext Secure Proxy Re-Encryption. Lecture Notes in Computer Science, 2012, , 349-364.	1.0	52
5	A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption. Lecture Notes in Computer Science, 2014, , 275-292.	1.0	50
6	Identity-Based Hierarchical Strongly Key-Insulated Encryption and Its Application. Lecture Notes in Computer Science, 2005, , 495-514.	1.0	47
7	Group Signatures with Message-Dependent Opening. Lecture Notes in Computer Science, 2013, , 270-294.	1.0	44
8	A Framework for Identity-Based Encryption with Almost Tight Security. Lecture Notes in Computer Science, 2015, , 521-549.	1.0	44
9	Unconditionally Secure Digital Signature Schemes Admitting Transferability. Lecture Notes in Computer Science, 2000, , 130-142.	1.0	39
10	On the Security of Dynamic Group Signatures: Preventing Signature Hijacking. Lecture Notes in Computer Science, 2012, , 715-732.	1.0	36
11	Conversions Among Several Classes of Predicate Encryption and Applications to ABE with Various Compactness Tradeoffs. Lecture Notes in Computer Science, 2015, , 575-601.	1.0	34
12	Security Notions for Unconditionally Secure Signature Schemes. Lecture Notes in Computer Science, 2002, , 434-449.	1.0	30
13	Card-Based Protocols Using Regular Polygon Cards. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1900-1909.	0.2	29
14	On the Security of Multiple Encryption or CCA-security+CCA-security=CCA-security?. Lecture Notes in Computer Science, 2004, , 360-374.	1.0	28
15	Information-theoretically secure oblivious polynomial evaluation in the commodity-based model. International Journal of Information Security, 2015, 14, 73-84.	2.3	26
16	Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication. Lecture Notes in Computer Science, 2012, , 243-261.	1.0	24
17	On the Security of the Schnorr Signature Scheme and DSA Against Related-Key Attacks. Lecture Notes in Computer Science, 2016, , 20-35.	1.0	23
18	Fuzzy Signatures: Relaxing Requirements and a New Construction. Lecture Notes in Computer Science, 2016, , 97-116.	1.0	22

#	Article	IF	Citations
19	On the Impossibility of Constructing Efficient Key Encapsulation and Programmable Hash Functions in Prime Order Groups. Lecture Notes in Computer Science, 2012, , 812-831.	1.0	21
20	Multi-party Computation with Small Shuffle Complexity Using Regular Polygon Cards. Lecture Notes in Computer Science, 2015, , 127-146.	1.0	21
21	Time-Specific Encryption from Forward-Secure Encryption. Lecture Notes in Computer Science, 2012, , 184-204.	1.0	20
22	A Signature Scheme with a Fuzzy Private Key. Lecture Notes in Computer Science, 2015, , 105-126.	1.0	20
23	Efficient Identity-Based Encryption with Tight Security Reduction. Lecture Notes in Computer Science, 2006, , 19-36.	1.0	20
24	Unconditionally Secure Anonymous Encryption and Group Authentication. Computer Journal, 2005, 49, 310-321.	1.5	19
25	A Revocable Group Signature Scheme from Identity-Based Revocation Techniques: Achieving Constant-Size Revocation List. Lecture Notes in Computer Science, 2014, , 419-437.	1.0	19
26	Attribute-Based Encryption for Range Attributes. Lecture Notes in Computer Science, 2016, , 42-61.	1.0	18
27	Applying Fujisaki-Okamoto to Identity-Based Encryption. Lecture Notes in Computer Science, 2006, , 183-192.	1.0	18
28	Secure Grouping Protocol Using a Deck of Cards. Lecture Notes in Computer Science, 2017, , 135-152.	1.0	18
29	On the Security of a Bidirectional Proxy Re-encryption Scheme from PKC 2010. Lecture Notes in Computer Science, 2011, , 284-295.	1.0	18
30	Invisibly Sanitizable Digital Signature Scheme. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2008, E91-A, 392-402.	0.2	18
31	Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption. Lecture Notes in Computer Science, 2013, , 32-50.	1.0	17
32	Chosen Ciphertext Security via UCE. Lecture Notes in Computer Science, 2014, , 56-76.	1.0	17
33	Fully Anonymous Group Signature with Verifier-Local Revocation. Lecture Notes in Computer Science, 2018, , 23-42.	1.0	17
34	Efficient Two-level Homomorphic Encryption in Prime-order Bilinear Groups and A Fast Implementation in WebAssembly. , 2018, , .		17
35	Revocable Group Signature with Constant-Size Revocation List. Computer Journal, 2015, 58, 2698-2715.	1.5	16
36	Chosen Ciphertext Security via Point Obfuscation. Lecture Notes in Computer Science, 2014, , 95-120.	1.0	16

#	Article	IF	Citations
37	Generic Transforms to Acquire CCA-Security for Identity Based Encryption: The Cases of FOpkc and REACT. Lecture Notes in Computer Science, 2006, , 348-359.	1.0	14
38	Group signature implies public-key encryption with non-interactive opening. International Journal of Information Security, 2014, 13, 51-62.	2.3	13
39	A Short Random Fingerprinting Code Against a Small Number of Pirates. Lecture Notes in Computer Science, 2006, , 193-202.	1.0	13
40	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
41	Self-bilinear Map on Unknown Order Groups from Indistinguishability Obfuscation and Its Applications. Lecture Notes in Computer Science, 2014, , 90-107.	1.0	13
42	Secure Grouping Protocol Using a Deck of Cards. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 1512-1524.	0.2	13
43	Universally Composable and Statistically Secure Verifiable Secret Sharing Scheme Based on Pre-Distributed Data. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 725-734.	0.2	13
44	On the Theoretical Gap between Group Signatures with and without Unlinkability. Lecture Notes in Computer Science, 2009, , 149-166.	1.0	12
45	Signature schemes with a fuzzy private key. International Journal of Information Security, 2019, 18, 581-617.	2.3	12
46	Re-Encryption Verifiability: How to Detect Malicious Activities of a Proxy in Proxy Re-Encryption. Lecture Notes in Computer Science, 2015, , 410-428.	1.0	12
47	Time-specific encryption from forward-secure encryption: generic and direct constructions. International Journal of Information Security, 2016, 15, 549-571.	2.3	11
48	Generic Constructions for Fully Secure Revocable Attribute-Based Encryption. Lecture Notes in Computer Science, 2017, , 532-551.	1.0	11
49	Formal Security Treatments for IBE-to-Signature Transformation: Relations among Security Notions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 53-66.	0.2	11
50	Privacy-preserving search for chemical compound databases. BMC Bioinformatics, 2015, 16, S6.	1.2	10
51	Secure Multi-Party Computation Using Polarizing Cards. Lecture Notes in Computer Science, 2015, , 281-297.	1.0	10
52	Relations Among Notions of Security for Identity Based Encryption Schemes. Lecture Notes in Computer Science, 2006, , 130-141.	1.0	10
53	Information Theoretically Secure Oblivious Polynomial Evaluation: Model, Bounds, and Constructions. Lecture Notes in Computer Science, 2004, , 62-73.	1.0	10
54	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

#	Article	IF	Citations
55	Attribute Based Encryption with Direct Efficiency Tradeoff. Lecture Notes in Computer Science, 2016, , 249-266.	1.0	9
56	Unconditionally Secure Anonymous Encryption and Group Authentication. Lecture Notes in Computer Science, 2002, , 81-99.	1.0	9
57	Constructing and Understanding Chosen Ciphertext Security via Puncturable Key Encapsulation Mechanisms. Lecture Notes in Computer Science, 2015, , 561-590.	1.0	9
58	Group Signatures with Message-Dependent Opening: Formal Definitions and Constructions. Security and Communication Networks, 2019, 2019, 1-36.	1.0	8
59	Anonymous Authentication Scheme for Subscription Services. , 2007, , 975-983.		8
60	Traitor Tracing Scheme Secure against Adaptive Key Exposure and its Application to Anywhere TV Service. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007, E90-A, 1000-1011.	0.2	8
61	Methods for Restricting Message Space in Public-Key Encryption. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, E96.A, 1156-1168.	0.2	8
62	Unconditionally Secure Chaffing-and-Winnowing: A Relationship Between Encryption and Authentication. Lecture Notes in Computer Science, 2006, , 154-162.	1.0	8
63	Secure Computation Protocols Using Polarizing Cards. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, E99.A, 1122-1131.	0.2	7
64	Proxy Re-Encryption That Supports Homomorphic Operations for Re-Encrypted Ciphertexts. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2019, E102.A, 81-98.	0.2	7
65	Group Signature with Deniability: How to Disavow a Signature. Lecture Notes in Computer Science, 2016, , 228-244.	1.0	7
66	Efficient Broadcast Encryption with Personalized Messages. Lecture Notes in Computer Science, 2010, , 214-228.	1.0	7
67	Secure Broadcast System with Simultaneous Individual Messaging. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 1328-1337.	0.2	7
68	Formal Security Treatments for Signatures from Identity-Based Encryption. , 2007, , 218-227.		7
69	Black-Box Separations of Hash-and-Sign Signatures in the Non-Programmable Random Oracle Model. Lecture Notes in Computer Science, 2015, , 435-454.	1.0	6
70	Generic Constructions of Parallel Key-Insulated Encryption. Lecture Notes in Computer Science, 2010, , 36-53.	1.0	6
71	An Asymptotically Optimal Method for Converting Bit Encryption to Multi-Bit Encryption. Lecture Notes in Computer Science, 2015, , 415-442.	1.0	6
72	Key Encapsulation Mechanisms from Extractable Hash Proof Systems, Revisited. Lecture Notes in Computer Science, 2013, , 332-351.	1.0	6

#	Article	IF	Citations
73	Practical attributeâ€based signature schemes for circuits from bilinear map. IET Information Security, 2018, 12, 184-193.	1.1	5
74	Completeness of Single-Bit Projection-KDM Security for Public Key Encryption. Lecture Notes in Computer Science, 2015, , 201-219.	1.0	5
75	Public Key Encryption Schemes with Bounded CCA Security and Optimal Ciphertext Length Based on the CDH Assumption. Lecture Notes in Computer Science, 2011, , 299-306.	1.0	5
76	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
77	Orthogonality between Key Privacy and Data Privacy, Revisited. Lecture Notes in Computer Science, 2008, , 313-327.	1.0	5
78	Some Information Theoretic Arguments for Encryption: Non-malleability and Chosen-Ciphertext Security (Invited Talk). Lecture Notes in Computer Science, 2008, , 223-231.	1.0	5
79	Group Signature with Deniability: How to Disavow a Signature. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1825-1837.	0.2	4
80	A Survey on Identity-Based Encryption from Lattices. Mathematics for Industry, 2018, , 349-365.	0.4	4
81	Towards User-Friendly Cryptography. Lecture Notes in Computer Science, 2017, , 481-484.	1.0	4
82	A CDH-Based Strongly Unforgeable Signature Without Collision Resistant Hash Function. , 2007, , 68-84.		4
83	Achieving Chosen Ciphertext Security from Detectable Public Key Encryption Efficiently via Hybrid Encryption. Lecture Notes in Computer Science, 2013, , 226-243.	1.0	4
84	How to Obtain Fully Structure-Preserving (Automorphic) Signatures from Structure-Preserving Ones. Lecture Notes in Computer Science, 2016, , 465-495.	1.0	4
85	Efficient Provider Authentication for Bidirectional Broadcasting Service. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 1039-1051.	0.2	4
86	Between Hashed DH and Computational DH: Compact Encryption from Weaker Assumption. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 1994-2006.	0.2	4
87	A Remark on an Identity-Based Encryption Scheme with Non-interactive Opening. , 2018, , .		4
88	A Short Fail-Stop Signature Scheme from Factoring. Lecture Notes in Computer Science, 2014, , 309-316.	1.0	4
89	A Trade-off Traitor Tracing Scheme. IEICE Transactions on Information and Systems, 2009, E92-D, 859-875.	0.4	3
90	On the Security of Pseudorandomized Information-Theoretically Secure Schemes. IEEE Transactions on Information Theory, 2013, 59, 635-652.	1.5	3

#	Article	IF	Citations
91	Constructions of dynamic and non-dynamic threshold public-key encryption schemes with decryption consistency. Theoretical Computer Science, 2016, 630, 95-116.	0.5	3
92	Attribute-Based Encryption for Range Attributes. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 1440-1455.	0.2	3
93	Achieving Pairing-Free Aggregate Signatures using Pre-Communication between Signers. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021, E104.A, 1188-1205.	0.2	3
94	All-but-One Dual Projective Hashing and Its Applications. Lecture Notes in Computer Science, 2014, , 181-198.	1.0	3
95	Reducing Public Key Sizes in Bounded CCA-Secure KEMs with Optimal Ciphertext Length. Lecture Notes in Computer Science, 2015, , 100-109.	1.0	3
96	Signatures Resilient to Uninvertible Leakage. Lecture Notes in Computer Science, 2016, , 372-390.	1.0	3
97	Improving Efficiency of an â€˜On the Flyâ€™ Identification Scheme by Perfecting Zero-Knowledgeness. Lecture Notes in Computer Science, 2010, , 284-301.	1.0	3
98	Space Efficient Signature Schemes from the RSA Assumption. Lecture Notes in Computer Science, 2012, , 102-119.	1.0	3
99	Ciphertext Policy Multi-dimensional Range Encryption. Lecture Notes in Computer Science, 2013, , 247-261.	1.0	3
100	Size-Hiding Computation for Multiple Parties. Lecture Notes in Computer Science, 2016, , 937-966.	1.0	3
101	Reducing the Spread of Damage of Key Exposures in Key-Insulated Encryption. Lecture Notes in Computer Science, 2006, , 366-384.	1.0	3
102	Chosen Ciphertext Secure Public Key Encryption with a Simple Structure. Lecture Notes in Computer Science, 2008, , 20-33.	1.0	3
103	Dynamic Threshold Public-Key Encryption with Decryption Consistency from Static Assumptions. Lecture Notes in Computer Science, 2015, , 77-92.	1.0	2
104	Constructions of Fail-Stop Signatures for Multi-signer Setting. , 2015, , .		2
105	On the Security of Schnorr Signatures, DSA, and ElGamal Signatures against Related-Key Attacks. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 73-90.	0.2	2
106	Compact Public Key Encryption with Minimum Ideal Property of Hash Functions. Lecture Notes in Computer Science, 2014, , 178-193.	1.0	2
107	Group Signature Implies PKE with Non-interactive Opening and Threshold PKE. Lecture Notes in Computer Science, 2010, , 181-198.	1.0	2
108	Disavowable Public Key Encryption with Non-Interactive Opening. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 2446-2455.	0.2	2

#	Article	IF	Citations
109	Efficient Identity-Based Encryption with Tight Security Reduction. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007, E90-A, 1803-1813.	0.2	2
110	A Generic Method for Reducing Ciphertext Length of Reproducible KEMs in the RO Model. Lecture Notes in Computer Science, 2010, , 55-69.	1.0	2
111	Weakened Anonymity of Group Signature and Its Application to Subscription Services. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, E97.A, 1240-1258.	0.2	2
112	Content and Key Management to Trace Traitors in Broadcasting Services. Lecture Notes in Computer Science, 2015, , 236-252.	1.0	2
113	New Security Proof for the Boneh-Boyen IBE: Tight Reduction in Unbounded Multi-challenge Security. Lecture Notes in Computer Science, 2015, , 176-190.	1.0	2
114	Trading Plaintext-Awareness for Simulatability to Achieve Chosen Ciphertext Security. Lecture Notes in Computer Science, 2016, , 3-34.	1.0	2
115	Achieving Pairing-Free Aggregate Signatures using Pre-Communication between Signers. Lecture Notes in Computer Science, 2020, , 65-84.	1.0	2
116	Trade-Off Traitor Tracing. , 2007, , 331-340.		2
117	Private Similarity Searchable Encryption for Euclidean Distance. IEICE Transactions on Information and Systems, 2017, E100.D, 2319-2326.	0.4	1
118	A Setup-Free Threshold Encryption Scheme for the Bitcoin Protocol and Its Applications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2020, E103.A, 150-164.	0.2	1
119	How to Break COT-Based Fingerprinting Schemes and Design New One. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2005, E88-A, 2800-2807.	0.2	1
120	Unconditionally Secure Chaffing-and-Winnowing for Multiple Use. Lecture Notes in Computer Science, 2009, , 133-145.	1.0	1
121	An Efficient Encapsulation Scheme from Near Collision Resistant Pseudorandom Generators and Its Application to IBE-to-PKE Transformations. Lecture Notes in Computer Science, 2009, , 16-31.	1.0	1
122	Applications of Signcryption. Information Security and Cryptography, 2010, , 241-256.	0.2	1
123	An Improvement of Pseudorandomization against Unbounded Attack Algorithms â€“ The Case of Fingerprint Codes. Lecture Notes in Computer Science, 2010, , 213-230.	1.0	1
124	Relations between Constrained and Bounded Chosen Ciphertext Security for Key Encapsulation Mechanisms. Lecture Notes in Computer Science, 2012, , 576-594.	1.0	1
125	Generalized Hardness Assumption for Self-bilinear Map with Auxiliary Information. Lecture Notes in Computer Science, 2016, , 269-284.	1.0	1
126	Unconditionally Secure Revocable Storage: Tight Bounds, Optimal Construction, and Robustness. Lecture Notes in Computer Science, 2016, , 213-237.	1.0	1

#	Article	IF	Citations
127	On the Security of Non-Interactive Key Exchange against Related-Key Attacks. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1910-1923.	0.2	1
128	How to Make Traitor Tracing Schemes Secure against a Content Comparison Attack in Actual Services. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 34-49.	0.2	1
129	A Taxonomy of Secure Two-Party Comparison Protocols and Efficient Constructions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2019, E102.A, 1048-1060.	0.2	1
130	Practical Public-Key Encryption Scheme Tightly Secure in the Random Oracle Model. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2020, E103.A, 165-172.	0.2	1
131	A Practical Provider Authentication System for Bidirectional Broadcast Service. , 2007, , 967-974.		1
132	CCA-Secure Public Key Encryption without Group-Dependent Hash Functions. IEICE Transactions on Information and Systems, 2009, E92-D, 967-970.	0.4	0
133	Sequential Bitwise Sanitizable Signature Schemes. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 392-404.	0.2	0
134	An Efficient Authentication for Lightweight Devices by Perfecting Zero-Knowledgeness. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 92-103.	0.2	0
135	A Privacy-Enhanced Access Log Management Mechanism in SSO Systems from Nominative Signatures. , 2014, , .		0
136	Public-Key Encryption Schemes with Bounded CCA Security and Optimal Ciphertext Length Based on the CDH and HDH Assumptions. Computer Journal, 2015, 58, 2738-2746.	1.5	0
137	On Limitations and Alternatives of Privacy-Preserving Cryptographic Protocols for Genomic Data. Lecture Notes in Computer Science, 2015, , 242-261.	1.0	0
138	Convertible Nominative Signatures from Standard Assumptions without Random Oracles. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, E99.A, 1107-1121.	0.2	0
139	A limitation on security evaluation of cryptographic primitives with fixed keys. Security and Communication Networks, 2016, 9, 1663-1675.	1.0	0
140	Efficient key encapsulation mechanisms with tight security reductions to standard assumptions in the two security models. Security and Communication Networks, 2016, 9, 1676-1697.	1.0	0
141	Compact public key encryption without full random oracles. Pervasive and Mobile Computing, 2017, 41, 286-299.	2.1	0
142	Signatures from Trapdoor Commitments with Strong Openings. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1924-1931.	0.2	0
143	Anonymous Pay-TV System with Secure Revenue Sharing. Lecture Notes in Computer Science, 2007, , 984-991.	1.0	0
144	Key-Insulated Public Key Encryption with Auxiliary Helper Key: Model, Constructions and Formal Security Proofs. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007, E90-A, 1814-1829.	0.2	0

#	Article	IF	Citations
145	Extension of Broadcasting Service by Using Electronic Tokens. IEICE Transactions on Information and Systems, 2007, E90-D, 1741-1750.	0.4	0
146	A Strongly Unforgeable Signature under the CDH Assumption without Collision Resistant Hash Functions. IEICE Transactions on Information and Systems, 2008, E91-D, 1466-1476.	0.4	0
147	Simple CCA-Secure Public Key Encryption from Any Non-Malleable Identity-Based Encryption. Lecture Notes in Computer Science, 2009, , 1-19.	1.0	0
148	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
149	How to Shorten a Ciphertext of Reproducible Key Encapsulation Mechanisms in the Random Oracle Model. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 1293-1305.	0.2	0
150	New Security Proof for the Boneh-Boyen IBE: Tight Reduction in Unbounded Multi-Challenge Security. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1882-1890.	0.2	0
151	Generic transformation from broadcast encryption to round-optimal deniable ring authentication. Designs, Codes, and Cryptography, 2022, 90, 277-316.	1.0	0