Nuttapong Attrapadung

List of Publications by Year
in descending order

44 papers	1,758 citations	361045 20 h-index	276539 41 g-index
44 all docs	44 docs citations	44 times ranked	699 citing authors

#	Article	IF	Citations
1	Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts. Lecture Notes in Computer Science, 2011, , 90-108.	1.0	239
2	Conjunctive Broadcast and Attribute-Based Encryption. Lecture Notes in Computer Science, 2009, , 248-265.	1.0	154
3	Dual System Encryption via Doubly Selective Security: Framework, Fully Secure Functional Encryption for Regular Languages, and More. Lecture Notes in Computer Science, 2014, , 557-577.	1.0	150
4	Attribute-based encryption schemes with constant-size ciphertexts. Theoretical Computer Science, 2012, 422, 15-38.	0.5	143
5	Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes. Lecture Notes in Computer Science, 2009, , 278-300.	1.0	129
6	Functional Encryption for Inner Product: Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation. Lecture Notes in Computer Science, 2010, , 384-402.	1.0	95
7	Computing on Authenticated Data: New Privacy Definitions and Constructions. Lecture Notes in Computer Science, 2012, , 367-385.	1.0	79
8	Homomorphic Network Coding Signatures in the Standard Model. Lecture Notes in Computer Science, 2011, , 17-34.	1.0	68
9	Dual System Encryption Framework in Prime-Order Groups via Computational Pair Encodings. Lecture Notes in Computer Science, 2016, , 591-623.	1.0	66
10	Dual-Policy Attribute Based Encryption. Lecture Notes in Computer Science, 2009, , 168-185.	1.0	65
11	Efficient Completely Context-Hiding Quotable and Linearly Homomorphic Signatures. Lecture Notes in Computer Science, 2013, , 386-404.	1.0	64
12	Generic Constructions for Chosen-Ciphertext Secure Attribute Based Encryption. Lecture Notes in Computer Science, 2011, , 71-89.	1.0	55
13	A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption. Lecture Notes in Computer Science, 2014, , 275-292.	1.0	50
14	A Framework for Identity-Based Encryption with Almost Tight Security. Lecture Notes in Computer Science, 2015, , 521-549.	1.0	44
15	Duality in ABE: Converting Attribute Based Encryption for Dual Predicate and Dual Policy via Computational Encodings. Lecture Notes in Computer Science, 2015, , 87-105.	1.0	39
16	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
17	Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication. Lecture Notes in Computer Science, 2012, , 243-261.	1.0	24
18	Unbounded Dynamic Predicate Compositions in Attribute-Based Encryption. Lecture Notes in Computer Science, 2019, , 34-67.	1.0	21

#	Article	IF	Citations
19	Time-Specific Encryption from Forward-Secure Encryption. Lecture Notes in Computer Science, 2012, , 184-204.	1.0	20
20	Efficient Identity-Based Encryption with Tight Security Reduction. Lecture Notes in Computer Science, 2006, , 19-36.	1.0	20
21	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
22	Attribute-Based Encryption for Range Attributes. Lecture Notes in Computer Science, 2016, , 42-61.	1.0	18
23	Forward-Secure and Searchable Broadcast Encryption with Short Ciphertexts and Private Keys. Lecture Notes in Computer Science, 2006, , 161-177.	1.0	18
24	Revocable Group Signature with Constant-Size Revocation List. Computer Journal, 2015, 58, 2698-2715.	1.5	16
25	Graph-Decomposition-Based Frameworks for Subset-Cover Broadcast Encryption and Efficient Instantiations. Lecture Notes in Computer Science, 2005, , 100-120.	1.0	16
26	Unbounded Dynamic Predicate Compositions in ABE from Standard Assumptions. Lecture Notes in Computer Science, 2020, , 405-436.	1.0	16
27	Functional encryption for public-attribute inner products: Achieving constant-size ciphertexts with adaptive security or support for negation. Journal of Mathematical Cryptology, 2012, 5, .	0.4	14
28	Time-specific encryption from forward-secure encryption: generic and direct constructions. International Journal of Information Security, 2016, 15, 549-571.	2.3	11
29	Generic Constructions for Fully Secure Revocable Attribute-Based Encryption. Lecture Notes in Computer Science, 2017, , 532-551.	1.0	11
30	Privacy-preserving search for chemical compound databases. BMC Bioinformatics, 2015, 16, S6.	1.2	10
31	Attribute Based Encryption with Direct Efficiency Tradeoff. Lecture Notes in Computer Science, 2016, , 249-266.	1.0	9
32	Efficient and Fully Secure Forward Secure Ciphertext-Policy Attribute-Based Encryption. Lecture Notes in Computer Science, 2015, , 87-99.	1.0	7
33	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
34	Dual-Policy Attribute Based Encryption: Simultaneous Access Control with Ciphertext and Key Policies. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 116-125.	0.2	6
35	Practical attributeâ€based signature schemes for circuits from bilinear map. IET Information Security, 2018, 12, 184-193.	1.1	5
36	A CDH-Based Strongly Unforgeable Signature Without Collision Resistant Hash Function. , 2007, , 68-84.		4

#	Article	IF	Citations
37	Attribute-Based Encryption for Range Attributes. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 1440-1455.	0.2	3
38	Dual System Framework in Multilinear Settings and Applications to Fully Secure (Compact) ABE for Unbounded-Size Circuits. Lecture Notes in Computer Science, 2017, , 3-35.	1.0	3
39	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
40	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
41	Private Similarity Searchable Encryption for Euclidean Distance. IEICE Transactions on Information and Systems, 2017, E100.D, 2319-2326.	0.4	1
42	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
43	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
44	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