Brent Waters

List of Publications by Year
in descending order

21	14,778	687363	1058476
papers	citations	13	14
		h-index	g-index

21	21	21	3710
all docs	docs citations	times ranked	citing authors

#	ARTICLE	IF	CITATIONS
1	Collusion Resistant Traitor Tracing from Learning with Errors. SIAM Journal on Computing, 2020, 49, STOC18-94-STOC18-241.	1.0	2
2	Lockable Obfuscation. , 2017, , .		73
3	Candidate Indistinguishability Obfuscation and Functional Encryption for All Circuits. SIAM Journal on Computing, 2016, 45, 882-929.	1.0	128
4	Computing on Authenticated Data. Journal of Cryptology, 2015, 28, 351-395.	2.8	22
5	Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. Journal of Cryptology, 2013, 26, 191-224.	2.8	106
6	Sequential Aggregate Signatures, Multisignatures, and Verifiably Encrypted Signatures Without Random Oracles. Journal of Cryptology, 2013, 26, 340-373.	2.8	26
7	Reconstructing a fragmented face from a cryptographic identification protocol. , 2013, , .		4
8	Functional encryption. Communications of the ACM, 2012, 55, 56-64.	4.5	103
9	Functional Encryption: Definitions and Challenges. Lecture Notes in Computer Science, 2011, , 253-273.	1.3	558
10	Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. Lecture Notes in Computer Science, 2010, , 62-91.	1.3	795
11	Revocation Systems with Very Small Private Keys. , 2010, , .		165
12	Signing a Linear Subspace: Signature Schemes for Network Coding. Lecture Notes in Computer Science, 2009, , 68-87.	1.3	218
13	Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions. Lecture Notes in Computer Science, 2009, , 619-636.	1.3	599
14	Conjunctive, Subset, and Range Queries on Encrypted Data. , 2007, , 535-554.		894
15	Ciphertext-Policy Attribute-Based Encryption. , 2007, , .		3,071
16	Attribute-based encryption with non-monotonic access structures. , 2007, , .		613
17	Attribute-based encryption for fine-grained access control of encrypted data. , 2006, , .		3,146
18	Sequential Aggregate Signatures and Multisignatures Without Random Oracles. Lecture Notes in Computer Science, 2006, , 465-485.	1.3	228

#	Article	IF	Citations
19	Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). Lecture Notes in Computer Science, 2006, , 290-307.	1.3	305
20	Efficient Identity-Based Encryption Without Random Oracles. Lecture Notes in Computer Science, 2005, , 114-127.	1.3	1,298
21	Fuzzy Identity-Based Encryption. Lecture Notes in Computer Science, 2005, , 457-473.	1.3	2,424