Hong-Sheng Zhou

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/8872986/publications.pdf

Version: 2024-02-01

41 papers	832 citations	686830 13 h-index	552369 26 g-index
42 all docs	42 docs citations	42 times ranked	425 citing authors

#	Article	IF	Citations
1	Scriptable and composable SNARKs in the trusted hardware model1. Journal of Computer Security, 2022, , 1-37.	0.5	0
2	Locally Decodable and Updatable Non-malleable Codes and Their Applications. Journal of Cryptology, 2020, 33, 319-355.	2.1	6
3	(Efficient) Universally Composable Oblivious Transfer Using a Minimal Number of Stateless Tokens. Journal of Cryptology, 2019, 32, 459-497.	2.1	1
4	Leakage Resilience from Program Obfuscation. Journal of Cryptology, 2019, 32, 742-824.	2.1	3
5	Let a Non-barking Watchdog Bite: Cliptographic Signatures with an Offline Watchdog. Lecture Notes in Computer Science, 2019, , 221-251.	1.0	14
6	Statement Voting. Lecture Notes in Computer Science, 2019, , 667-685.	1.0	4
7	Multi-key FHE for multi-bit messages. Science China Information Sciences, 2018, 61, 1.	2.7	10
8	A Generic Paradigm for Blockchain Design. , 2018, , .		2
9	TwinsCoin. , 2018, , .		24
10	Correcting Subverted Random Oracles. Lecture Notes in Computer Science, 2018, , 241-271.	1.0	14
11	Multi-mode Cryptocurrency Systems. , 2018, , .		5
12	Leakage-Resilient Cryptography from Puncturable Primitives and Obfuscation. Lecture Notes in Computer Science, 2018, , 575-606.	1.0	3
13	Generic Semantic Security against a Kleptographic Adversary. , 2017, , .		40
14	Cryptography for Parallel RAM from Indistinguishability Obfuscation. , 2016, , .		24
15	A Unified Approach to Idealized Model Separations via Indistinguishability Obfuscation. Lecture Notes in Computer Science, 2016, , 587-603.	1.0	2
16	Leakage-Resilient Public-Key Encryption from Obfuscation. Lecture Notes in Computer Science, 2016, , 101-128.	1.0	9
17	Fair and Robust Multi-party Computation Using a Global Transaction Ledger. Lecture Notes in Computer Science, 2016, , 705-734.	1.0	93
18	Designing Proof of Human-Work Puzzles for Cryptocurrency and Beyond. Lecture Notes in Computer Science, 2016, , 517-546.	1.0	20

#	Article	IF	Citations
19	Cliptography: Clipping the Power of Kleptographic Attacks. Lecture Notes in Computer Science, 2016, , 34-64.	1.0	41
20	Incoercible Multi-party Computation and Universally Composable Receipt-Free Voting. Lecture Notes in Computer Science, 2015, , 763-780.	1.0	13
21	Multi-Client Verifiable Computation with Stronger Security Guarantees. Lecture Notes in Computer Science, 2015, , 144-168.	1.0	40
22	Leakage-Resilient Circuits Revisited â€“ Optimal Number of Computing Components Without Leak-Free Hardware. Lecture Notes in Computer Science, 2015, , 131-158.	1.0	13
23	Distributing the setup in universally composable multi-party computation. , 2014, , .		3
24	Multi-input Functional Encryption. Lecture Notes in Computer Science, 2014, , 578-602.	1.0	202
25	(Efficient) Universally Composable Oblivious Transfer Using a Minimal Number of Stateless Tokens. Lecture Notes in Computer Science, 2014, , 638-662.	1.0	14
26	Feasibility and Infeasibility of Adaptively Secure Fully Homomorphic Encryption. Lecture Notes in Computer Science, 2013, , 14-31.	1.0	11
27	Efficient, Adaptively Secure, and Composable Oblivious Transfer with a Single, Global CRS. Lecture Notes in Computer Science, 2013, , 73-88.	1.0	22
28	Feasibility and Completeness of Cryptographic Tasks in the Quantum World. Lecture Notes in Computer Science, 2013, , 281-296.	1.0	10
29	Functional Encryption from (Small) Hardware Tokens. Lecture Notes in Computer Science, 2013, , 120-139.	1.0	5
30	On the Security of the â€œFree-XORâ€•Technique. Lecture Notes in Computer Science, 2012, , 39-53.	1.0	52
31	Adaptively secure broadcast, revisited. , 2011, , .		27
32	A Framework for the Sound Specification of Cryptographic Tasks. , 2010, , .		1
33	Hidden identity-based signatures. IET Information Security, 2009, 3, 119.	1.1	6
34	Somewhat Non-committing Encryption and Efficient Adaptively Secure Oblivious Transfer. Lecture Notes in Computer Science, 2009, , 505-523.	1.0	32
35	Zero-Knowledge Proofs with Witness Elimination. Lecture Notes in Computer Science, 2009, , 124-138.	1.0	1
36	Secure Function Collection with Sublinear Storage. Lecture Notes in Computer Science, 2009, , 534-545.	1.0	1

#	Article	IF	Citations
37	Equivocal Blind Signatures and Adaptive UC-Security. , 2008, , 340-355.		18
38	Trading Static for Adaptive Security in Universally Composable Zero-Knowledge. Lecture Notes in Computer Science, 2007, , 316-327.	1.0	1
39	Concurrent Blind Signatures Without Random Oracles. Lecture Notes in Computer Science, 2006, , 49-62.	1.0	28
40	Remarks on unknown key-share attack on authenticated multiple-key agreement protocol. Electronics Letters, 2003, 39, 1248.	0.5	11
41	Towards Quantum One-Time Memories from Stateless Hardware. Quantum - the Open Journal for Quantum Science, 0, 5, 429.	0.0	2