Helger Lipmaa

List of Publications by Year in descending order

Source: https://exaly.com/author-pdf/1625823/publications.pdf

Version: 2024-02-01

69 papers	2,091 citations	318942 23 h-index	286692 43 g-index
75 all docs	75 docs citations	75 times ranked	851 citing authors

#	Article	IF	Citations
1	A Unified Framework forÂNon-universal SNARKs. Lecture Notes in Computer Science, 2022, , 553-583.	1.0	3
2	On Subversion-Resistant SNARKs. Journal of Cryptology, 2021, 34, 1.	2.1	9
3	Verifiably-Extractable OWFs andÂTheir Applications toÂSubversion Zero-Knowledge. Lecture Notes in Computer Science, 2021, , 618-649.	1.0	0
4	Smooth Zero-Knowledge Hash Functions. Lecture Notes in Computer Science, 2021, , 510-535.	1.0	3
5	Efficient NIZKs forÂAlgebraic Sets. Lecture Notes in Computer Science, 2021, , 128-158.	1.0	3
6	On QA-NIZK in the BPK Model. Lecture Notes in Computer Science, 2020, , 590-620.	1.0	14
7	Key-and-Argument-Updatable QA-NIZKs. Lecture Notes in Computer Science, 2020, , 645-669.	1.0	4
8	Succinct Functional Commitment for a Large Class of Arithmetic Circuits. Lecture Notes in Computer Science, 2020, , 686-716.	1.0	9
9	UC-Secure CRS Generation for SNARKs. Lecture Notes in Computer Science, 2019, , 99-117.	1.0	13
10	DL-Extractable UC-Commitment Schemes. Lecture Notes in Computer Science, 2019, , 385-405.	1.0	4
11	On the Security Properties of e-Voting Bulletin Boards. Lecture Notes in Computer Science, 2018, , 505-523.	1.0	10
12	An Efficient Pairing-Based Shuffle Argument. Lecture Notes in Computer Science, 2017, , 97-127.	1.0	22
13	A Subversion-Resistant SNARK. Lecture Notes in Computer Science, 2017, , 3-33.	1.0	47
14	Optimally Sound Sigma Protocols Under DCRA. Lecture Notes in Computer Science, 2017, , 182-203.	1.0	5
15	A Simpler Rate-Optimal CPIR Protocol. Lecture Notes in Computer Science, 2017, , 621-638.	1.0	11
16	CCA-Secure Inner-Product Functional Encryption from Projective Hash Functions. Lecture Notes in Computer Science, 2017, , 36-66.	1.0	32
17	Efficient Culpably Sound NIZK Shuffle Argument Without Random Oracles. Lecture Notes in Computer Science, 2016, , 200-216.	1.0	16
18	Prover-Efficient Commit-and-Prove Zero-Knowledge SNARKs. Lecture Notes in Computer Science, 2016, , 185-206.	1.0	14

#	Article	IF	Citations
19	A Shuffle Argument Secure in the Generic Model. Lecture Notes in Computer Science, 2016, , 841-872.	1.0	15
20	Optimal Rate Private Information Retrieval from Homomorphic Encryption. Proceedings on Privacy Enhancing Technologies, 2015, 2015, 222-243.	2.3	24
21	Linear Batch Codes. CIM Series in Mathematical Sciences, 2015, , 245-253.	0.4	14
22	Analysis and Implementation of an Efficient Ring-LPN Based Commitment Scheme. Lecture Notes in Computer Science, 2015, , 160-175.	1.0	2
23	Communication Optimal Tardos-Based Asymmetric Fingerprinting. Lecture Notes in Computer Science, 2015, , 469-486.	1.0	5
24	Efficient NIZK Arguments via Parallel Verification of Benes Networks. Lecture Notes in Computer Science, 2014, , 416-434.	1.0	6
25	Efficient Non-Interactive Zero Knowledge Arguments for Set Operations. Lecture Notes in Computer Science, 2014, , 216-233.	1.0	4
26	A more efficient computationally sound non-interactive zero-knowledge shuffle argument. Journal of Computer Security, 2013, 21, 685-719.	0.5	5
27	Efficient Modular NIZK Arguments from Shift and Product. Lecture Notes in Computer Science, 2013, , 92-121.	1.0	10
28	Secure Equality and Greater-Than Tests with Sublinear Online Complexity. Lecture Notes in Computer Science, 2013, , 645-656.	1.0	33
29	Practical Fully Simulatable Oblivious Transfer with Sublinear Communication. Lecture Notes in Computer Science, 2013, , 78-95.	1.0	6
30	Succinct Non-Interactive Zero Knowledge Arguments from Span Programs and Linear Error-Correcting Codes. Lecture Notes in Computer Science, 2013, , 41-60.	1.0	59
31	Secure Accumulators from Euclidean Rings without Trusted Setup. Lecture Notes in Computer Science, 2012, , 224-240.	1.0	36
32	Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments. Lecture Notes in Computer Science, 2012, , 169-189.	1.0	144
33	A More Efficient Computationally Sound Non-Interactive Zero-Knowledge Shuffle Argument. Lecture Notes in Computer Science, 2012, , 477-502.	1.0	17
34	A Non-interactive Range Proof with Constant Communication. Lecture Notes in Computer Science, 2012, , 179-199.	1.0	28
35	On the CCA1-Security of Elgamal and DamgÃ¥rdâ€™s Elgamal. Lecture Notes in Computer Science, 2011, , 18-35.	1.0	15
36	Multi-query Computationally-Private Information Retrieval with Constant Communication Rate. Lecture Notes in Computer Science, 2010, , 107-123.	1.0	31

#	Article	IF	Citations
37	Two New Efficient PIR-Writing Protocols. Lecture Notes in Computer Science, 2010, , 438-455.	1.0	2
38	Additive Combinatorics and Discrete Logarithm Based Range Protocols. Lecture Notes in Computer Science, 2010, , 336-351.	1.0	20
39	First CPIR Protocol with Data-Dependent Computation. Lecture Notes in Computer Science, 2010, , 193-210.	1.0	37
40	On E-Vote Integrity in the Case of Malicious Voter Computers. Lecture Notes in Computer Science, 2010, , 373-388.	1.0	18
41	Efficient Generalized Selective Private Function Evaluation with Applications in Biometric Authentication. Lecture Notes in Computer Science, 2010, , 154-163.	1.0	4
42	On the Feasibility of Consistent Computations. Lecture Notes in Computer Science, 2010, , 88-106.	1.0	2
43	Security and Trust for the Norwegian E-Voting Pilot Project E-valg 2011. Lecture Notes in Computer Science, 2009, , 207-222.	1.0	9
44	A note on the error of optimized LFC Private Information Retrieval scheme. , 2008, , .		0
45	Succinct NP Proofs from an Extractability Assumption. Lecture Notes in Computer Science, 2008, , 175-185.	1.0	32
46	New Communication-Efficient Oblivious Transfer Protocols Based on Pairings. Lecture Notes in Computer Science, 2008, , 441-454.	1.0	7
47	Hybrid DamgÃ¥rd Is CCA1-Secure under the DDH Assumption. Lecture Notes in Computer Science, 2008, , 18-30.	1.0	2
48	3-Message NP Arguments in the BPK Model with Optimal Soundness and Zero-Knowledge. Lecture Notes in Computer Science, 2008, , 615-627.	1.0	1
49	A New Protocol for Conditional Disclosure of Secrets and Its Applications. Lecture Notes in Computer Science, 2007, , 207-225.	1.0	24
50	Cryptographically private support vector machines. , 2006, , .		87
51	On Private Scalar Product Computation for Privacy-Preserving Data Mining. Lecture Notes in Computer Science, 2005, , 104-120.	1.0	210
52	Small Coalitions Cannot Manipulate Voting. Lecture Notes in Computer Science, 2005, , 285-297.	1.0	13
53	Designated Verifier Signature Schemes: Attacks, New Security Notions and a New Construction. Lecture Notes in Computer Science, 2005, , 459-471.	1.0	88
54	An Oblivious Transfer Protocol with Log-Squared Communication. Lecture Notes in Computer Science, 2005, , 314-328.	1.0	162

#	Article	IF	Citations
55	Private Itemset Support Counting. Lecture Notes in Computer Science, 2005, , 97-111.	1.0	12
56	On the Additive Differential Probability of Exclusive-Or. Lecture Notes in Computer Science, 2004, , 317-331.	1.0	24
57	Cryptographic Randomized Response Techniques. Lecture Notes in Computer Science, 2004, , 425-438.	1.0	27
58	Interleaving Cryptography and Mechanism Design. Lecture Notes in Computer Science, 2004, , 117-131.	1.0	5
59	On Diophantine Complexity and Statistical Zero-Knowledge Arguments. Lecture Notes in Computer Science, 2003, , 398-415.	1.0	106
60	Secure Vickrey Auctions without Threshold Trust. Lecture Notes in Computer Science, 2003, , 87-101.	1.0	95
61	Verifiable Homomorphic Oblivious Transfer and Private Equality Test. Lecture Notes in Computer Science, 2003, , 416-433.	1.0	65
62	On Differential Properties of Pseudo-Hadamard Transform and Related Mappings (Extended Abstract). Lecture Notes in Computer Science, 2002, , 48-61.	1.0	11
63	On Optimal Hash Tree Traversal for Interval Time-Stamping. Lecture Notes in Computer Science, 2002, , 357-371.	1.0	10
64	Eliminating counterevidence with applications to accountable certificate management1. Journal of Computer Security, 2002, 10, 273-296.	0.5	35
65	Efficient Algorithms for Computing Differential Properties of Addition. Lecture Notes in Computer Science, 2002, , 336-350.	1.0	90
66	Fast Software Implementations of SC2000. Lecture Notes in Computer Science, 2002, , 63-74.	1.0	3
67	Optimally Efficient Accountable Time-Stamping. Lecture Notes in Computer Science, 2000, , 293-305.	1.0	30
68	Accountable certificate management using undeniable attestations. , 2000, , .		45
69	IDEA: A Cipher for Multimedia Architectures?. Lecture Notes in Computer Science, 1999, , 248-263.	1.0	17