Nigel P Smart

List of Publications by Citations

Source: https://exaly.com/author-pdf/8888685/nigel-p-smart-publications-by-citations.pdf
Version: 2024-04-28

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

47 papers	1,929 citations	16 h-index	43 g-index
47 ext. papers	2,208 ext. citations	1.1 avg, IF	5.22 L-index

#	Paper	IF	Citations
47	Multiparty Computation from Somewhat Homomorphic Encryption. *Lecture Notes in Computer Science*, **2012**, 643-662	0.9	477
46	Homomorphic Evaluation of the AES Circuit. *Lecture Notes in Computer Science*, **2012**, 850-867	0.9	291
45	Secure Two-Party Computation Is Practical. *Lecture Notes in Computer Science*, **2009**, 250-267	0.9	220
44	Practical Covertly Secure MPC for Dishonest Majority Or: Breaking the SPDZ Limits. *Lecture Notes in Computer Science*, **2013**, 1-18	0.9	185
43	Fully Homomorphic Encryption with Polylog Overhead. *Lecture Notes in Computer Science*, **2012**, 465-482	0.9	183
42	Better Bootstrapping in Fully Homomorphic Encryption. *Lecture Notes in Computer Science*, **2012**, 1-16	0.9	79
41	Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries. *Lecture Notes in Computer Science*, **2008**, 2-20	0.9	63
40	Efficient Constant Round Multi-party Computation Combining BMR and SPDZ. *Lecture Notes in Computer Science*, **2015**, 319-338	0.9	55
39	Implementing AES via an Actively/Covertly Secure Dishonest-Majority MPC Protocol. *Lecture Notes in Computer Science*, **2012**, 241-263	0.9	33
38	Dishonest Majority Multi-Party Computation for Binary Circuits. *Lecture Notes in Computer Science*, **2014**, 495-512	0.9	33
37	From Keys to Databases Real-World Applications of Secure Multi-Party Computation. *Computer Journal*, **2018**,	1.3	28
36	Cryptography Made Simple. *Information Security and Cryptography*, **2016**,	3.6	27
35	Hash function requirements for Schnorr signatures. *Journal of Mathematical Cryptology*, **2009**, 3,	0.6	25
34	MPC-Friendly Symmetric Key Primitives **2016**,		24
33	Wildcarded Identity-Based Encryption. *Journal of Cryptology*, **2011**, 24, 42-82	2.1	19
32	More Efficient Constant-Round Multi-party Computation from BMR and SHE. *Lecture Notes in Computer Science*, **2016**, 554-581	0.9	18
31	Overdrive2k: Efficient Secure MPC over (mathbb {Z}_{2^k}) from Somewhat Homomorphic Encryption. *Lecture Notes in Computer Science*, **2020**, 254-283	0.9	16

30	Error Detection in Monotone Span Programs with Application to Communication-Efficient Multi-party Computation. *Lecture Notes in Computer Science*, **2019**, 210-229	0.9	14
29	Using TopGear in Overdrive: A More Efficient ZKPoK for SPDZ. *Lecture Notes in Computer Science*, **2020**, 274-302	0.9	14
28	Anonymity guarantees of the UMTS/LTE authentication and connection protocol. *International Journal of Information Security*, **2014**, 13, 513-527	2.8	11
27	Distributing Any Elliptic Curve Based Protocol. *Lecture Notes in Computer Science*, **2019**, 342-366	0.9	10
26	Between a Rock and a Hard Place: Interpolating between MPC and FHE. *Lecture Notes in Computer Science*, **2013**, 221-240	0.9	10
25	MPC Joins The Dark Side **2019**,		9
24	Physical side-channel attacks on cryptographic systems. *Software Focus*, **2000**, 1, 6-13		9
23	Zaphod **2019**,		9
22	Modes of Operation Suitable for Computing on Encrypted Data. *IACR Transactions on Symmetric Cryptology*,294-324		8
21	Reducing Communication Channels in MPC. *Lecture Notes in Computer Science*, **2018**, 181-199	0.9	8
20	Benchmarking Privacy Preserving Scientific Operations. *Lecture Notes in Computer Science*, **2019**, 509-529	0.9	7
19	Sharing the LUOV: Threshold Post-quantum Signatures. *Lecture Notes in Computer Science*, **2019**, 128-153	0.9	7
18	Efficient Constant-Round Multi-party Computation Combining BMR and SPDZ. *Journal of Cryptology*, **2019**, 32, 1026-1069	2.1	6
17	Adding Distributed Decryption and Key Generation to a Ring-LWE Based CCA Encryption Scheme. *Lecture Notes in Computer Science*, **2019**, 192-210	0.9	6
16	BBQ: Using AES in Picnic Signatures. *Lecture Notes in Computer Science*, **2020**, 669-692	0.9	6
15	Sashimi: Cutting up CSI-FiSh Secret Keys to Produce an Actively Secure Distributed Signing Protocol. *Lecture Notes in Computer Science*, **2020**, 169-186	0.9	6
14	Private Liquidity Matching Using MPC. *Lecture Notes in Computer Science*, **2022**, 96-119	0.9	2
13	Optimizing Registration Based Encryption. *Lecture Notes in Computer Science*, **2021**, 129-157	0.9	2

12	Multi-party computation mechanism for anonymous equity block trading: A secure implementation of turquoise plato uncross. *Intelligent Systems in Accounting, Finance and Management*,	2.5	2
11	High-Performance Multi-party Computation for Binary Circuits Based on Oblivious Transfer. *Journal of Cryptology*, **2021**, 34, 1	2.1	2
10	Thresholdizing HashEdDSA: MPC to the Rescue. *International Journal of Information Security*, **2021**, 20, 879	2.8	2
9	Semi-commutative Masking: A Framework for Isogeny-Based Protocols, with an Application to Fully Secure Two-Round Isogeny-Based OT. *Lecture Notes in Computer Science*, **2020**, 235-258	0.9	1
8	Secure Fast Evaluation of Iterative Methods: With an Application to Secure PageRank. *Lecture Notes in Computer Science*, **2021**, 1-25	0.9	1
7	Actively Secure Setup for SPDZ. *Journal of Cryptology*, **2022**, 35, 1	2.1	1
6	Large Scale, Actively Secure Computation from LPN and Free-XOR Garbled Circuits. *Lecture Notes in Computer Science*, **2021**, 33-63	0.9	0
5	The Cost of IEEE Arithmetic in Secure Computation. *Lecture Notes in Computer Science*, **2021**, 431-452	0.9	0
4	Gladius: LWR Based Efficient Hybrid Public Key Encryption with Distributed Decryption. *Lecture Notes in Computer Science*, **2021**, 125-155	0.9	
3	Bootstrapping BGV ciphertexts with a wider choice of p and q. *IET Information Security*, **2016**, 10, 348-357	1.4	
2	Compilation of Function Representations for Secure Computing Paradigms. *Lecture Notes in Computer Science*, **2021**, 26-50	0.9	
1	MPC for $$mathcal {Q}_2$$ Access Structures over Rings and Fields. *Lecture Notes in Computer Science*, **2022**, 131-151	0.9	