Nigel P Smart

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/8888685/publications.pdf

Version: 2024-02-01

44 papers	2,716 citations	430754 18 h-index	289141 40 g-index
47 all docs	47 docs citations	47 times ranked	1056 citing authors

#	Article	IF	Citations
1	Multiparty Computation from Somewhat Homomorphic Encryption. Lecture Notes in Computer Science, 2012, , 643-662.	1.0	669
2	Homomorphic Evaluation of the AES Circuit. Lecture Notes in Computer Science, 2012, , 850-867.	1.0	389
3	Secure Two-Party Computation Is Practical. Lecture Notes in Computer Science, 2009, , 250-267.	1.0	276
4	Practical Covertly Secure MPC for Dishonest Majority â€“ Or: Breaking the SPDZ Limits. Lecture Notes in Computer Science, 2013, , 1-18.	1.0	257
5	Fully Homomorphic Encryption with Polylog Overhead. Lecture Notes in Computer Science, 2012, , 465-482.	1.0	238
6	Better Bootstrapping in Fully Homomorphic Encryption. Lecture Notes in Computer Science, 2012, , 1-16.	1.0	111
7	Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries. Lecture Notes in Computer Science, 2008, , 2-20.	1.0	82
8	Efficient Constant Round Multi-party Computation Combining BMR and SPDZ. Lecture Notes in Computer Science, 2015, , 319-338.	1.0	69
9	From Keys to Databasesâ€”Real-World Applications of Secure Multi-Party Computation. Computer Journal, 0, , .	1.5	57
10	Cryptography Made Simple. Information Security and Cryptography, 2016, , .	0.2	46
11	Implementing AES via an Actively/Covertly Secure Dishonest-Majority MPC Protocol. Lecture Notes in Computer Science, 2012, , 241-263.	1.0	40
12	MPC-Friendly Symmetric Key Primitives. , 2016, , .		38
13	Dishonest Majority Multi-Party Computation for Binary Circuits. Lecture Notes in Computer Science, 2014, , 495-512.	1.0	38
14	Hash function requirements for Schnorr signatures. Journal of Mathematical Cryptology, 2009, 3, .	0.4	35
15	More Efficient Constant-Round Multi-party Computation from BMR and SHE. Lecture Notes in Computer Science, 2016, , 554-581.	1.0	34
16	Wildcarded Identity-Based Encryption. Journal of Cryptology, 2011, 24, 42-82.	2.1	25
17	Using TopGear in Overdrive: A More Efficient ZKPoK for SPDZ. Lecture Notes in Computer Science, 2020, , 274-302.	1.0	24
18	MPC Joins The Dark Side. , 2019, , .		20

#	Article	IF	Citations
19	Sashimi: Cutting up CSI-FiSh Secret Keys to Produce an Actively Secure Distributed Signing Protocol. Lecture Notes in Computer Science, 2020, , 169-186.	1.0	20
20	Distributing Any Elliptic Curve Based Protocol. Lecture Notes in Computer Science, 2019, , 342-366.	1.0	19
21	Overdrive2k: Efficient Secure MPC over $$mathbb {Z}_{2^k}$$ from Somewhat Homomorphic Encryption. Lecture Notes in Computer Science, 2020, , 254-283.	1.0	19
22	Zaphod. , 2019, , .		18
23	Benchmarking Privacy Preserving Scientific Operations. Lecture Notes in Computer Science, 2019, , 509-529.	1.0	18
24	Sharing the LUOV: Threshold Post-quantum Signatures. Lecture Notes in Computer Science, 2019, , 128-153.	1.0	17
25	Error Detection in Monotone Span Programs with Application to Communication-Efficient Multi-party Computation. Lecture Notes in Computer Science, 2019, , 210-229.	1.0	16
26	Anonymity guarantees of the UMTS/LTE authentication and connection protocol. International Journal of Information Security, 2014, 13, 513-527.	2.3	15
27	Between a Rock and a Hard Place: Interpolating between MPC and FHE. Lecture Notes in Computer Science, 2013, , 221-240.	1.0	15
28	Efficient Constant-Round Multi-party Computation Combining BMR and SPDZ. Journal of Cryptology, 2019, 32, 1026-1069.	2.1	12
29	Physical side-channel attacks on cryptographic systems. Software Focus, 2000, 1, 6-13.	0.3	11
30	Reducing Communication Channels in MPC. Lecture Notes in Computer Science, 2018, , 181-199.	1.0	11
31	Modes of Operation Suitable for Computing on Encrypted Data. IACR Transactions on Symmetric Cryptology, 0, , 294-324.	0.0	10
32	Adding Distributed Decryption and Key Generation to a Ring-LWE Based CCA Encryption Scheme. Lecture Notes in Computer Science, 2019, , 192-210.	1.0	9
33	Thresholdizing HashEdDSA: MPC to the Rescue. International Journal of Information Security, 2021, 20, 879-894.	2.3	7
34	Actively Secure Setup for SPDZ. Journal of Cryptology, 2022, 35, 1.	2.1	7
35	Large Scale, Actively Secure Computation from LPN and Free-XOR Garbled Circuits. Lecture Notes in Computer Science, 2021, , 33-63.	1.0	6
36	Multiâ€party computation mechanism for anonymous equity block trading: A secure implementation of turquoise plato uncross. Intelligent Systems in Accounting, Finance and Management, 0, , .	2.8	3

#	Article	IF	Citations
37	Private Liquidity Matching Using MPC. Lecture Notes in Computer Science, 2022, , 96-119.	1.0	3
38	High-Performance Multi-party Computation for Binary Circuits Based on Oblivious Transfer. Journal of Cryptology, 2021, 34, 1.	2.1	2
39	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.	1.0	2
40	Gladius: LWR Based Efficient Hybrid Public Key Encryption withÂDistributed Decryption. Lecture Notes in Computer Science, 2021, , 125-155.	1.0	2
41	Secure Fast Evaluation of Iterative Methods: With an Application to Secure PageRank. Lecture Notes in Computer Science, 2021, , 1-25.	1.0	1
42	The Cost of IEEE Arithmetic in Secure Computation. Lecture Notes in Computer Science, 2021, , 431-452.	1.0	1
43	MPC for $$mathcal {Q}_2$$ Access Structures over Rings and Fields. Lecture Notes in Computer Science, 2022, , 131-151.	1.0	1
44	Bootstrapping BGV ciphertexts with a wider choice of p and q. IET Information Security, 2016, 10, 348-357.	1.1	0