Andy Rupp

List of Publications by Year
in descending order

27	436	933447 10	839539 18
papers	citations	h-index	g-index

27	27	27	270
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Cryptanalysis with COPACOBANA. IEEE Transactions on Computers, 2008, 57, 1498-1513.	3.4	98
2	A Parallel Hardware Architecture for fast Gaussian Elimination over GF(2). , 2006, , .		35
3	(R)CCA Secure Updatable Encryption with Integrity Protection. Lecture Notes in Computer Science, 2019, , 68-99.	1.3	29
4	Fault-Tolerant Aggregate Signatures. Lecture Notes in Computer Science, 2016, , 331-356.	1.3	29
5	A Real-World Attack Breaking A5/1 within Hours. Lecture Notes in Computer Science, 2008, , 266-282.	1.3	25
6	Fast multivariate signature generation in hardware: The case of rainbow. , 2008, , .		22
7	Polynomial Spaces: A New Framework for Composite-to-Prime-Order Transformations. Lecture Notes in Computer Science, 2014, , 261-279.	1.3	21
8	Efficient Zero-Knowledge Arguments in the Discrete Log Setting, Revisited. , 2019, , .		18
9	BBA+. , 2017, , .		16
10	Cryptographic Theory Meets Practice. ACM Transactions on Information and System Security, 2015, 17, 1-31.	4.5	15
11	Public-Key Encryption with Simulation-Based Selective-Opening Security and Compact Ciphertexts. Lecture Notes in Computer Science, 2016, , 146-168.	1.3	14
12	Black-Box Accumulation: Collecting Incentives in a Privacy-Preserving Way. Proceedings on Privacy Enhancing Technologies, 2016, 2016, 62-82.	2.8	14
13	The Semi-Generic Group Model and Applications to Pairing-Based Cryptography. Lecture Notes in Computer Science, 2010, , 539-556.	1.3	13
14	Fast Multivariate Signature Generation in Hardware: The Case of Rainbow. , 2008, , .		10
15	A Hardware-Assisted Realtime Attack on A5/2 Without Precomputations. Lecture Notes in Computer Science, 2007, , 394-412.	1.3	10
16	Faster Multi-exponentiation through Caching: Accelerating (EC)DSA Signature Verification. Lecture Notes in Computer Science, 2008, , 39-56.	1.3	9
17	P4R: Privacy-Preserving Pre-Payments with Refunds for Transportation Systems. Lecture Notes in Computer Science, 2013, , 205-212.	1.3	9
18	Packet trace manipulation rramework for test labs. , 2004, , .		8

#	Article	IF	Citations
19	New Techniques for Structural Batch Verification in Bilinear Groups with Applications to Groth-Sahai Proofs. , 2017, , .		7
20	P4TCâ€”Provably-Secure yet Practical Privacy-Preserving Toll Collection. Proceedings on Privacy Enhancing Technologies, 2020, 2020, 62-152.	2.8	7
21	Black-Box Wallets: Fast Anonymous Two-Way Payments for Constrained Devices. Proceedings on Privacy Enhancing Technologies, 2020, 2020, 165-194.	2.8	6
22	Non-malleability vs. CCA-Security: The Case of Commitments. Lecture Notes in Computer Science, 2018, , 312-337.	1.3	5
23	Efficient Threshold Zero-Knowledge with Applications to User-Centric Protocols. Lecture Notes in Computer Science, 2012, , 147-166.	1.3	5
24	Hardware SLE solvers: Efficient building blocks for cryptographic and cryptanalyticapplications. The Integration VLSI Journal, 2011, 44, 290-304.	2.1	4
25	Reconfigurable Cryptography: A Flexible Approach to Long-Term Security. Lecture Notes in Computer Science, 2016, , 416-445.	1.3	4
26	P6V2G: a privacy-preserving V2G scheme for two-way payments and reputation. Energy Informatics, 2019, 2, .	2.3	2
27	PUBA: Privacy-Preserving User-Data Bookkeeping and Analytics. Proceedings on Privacy Enhancing Technologies, 2022, 2022, 447-516.	2.8	1