Anupam Chattopadhyay

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/6615481/publications.pdf

Version: 2024-02-01

124 papers	1,832 citations	623188 14 h-index	454577 30 g-index
127 all docs	127 docs citations	127 times ranked	1865 citing authors

#	Article	IF	Citations
1	Lattice-based Key-sharing Schemes. ACM Computing Surveys, 2022, 54, 1-39.	16.1	11
2	On Exploiting Message Leakage in (Few) NIST PQC Candidates for Practical Message Recovery Attacks. IEEE Transactions on Information Forensics and Security, 2022, 17, 684-699.	4.5	10
3	On Threat ofÂHardware Trojan toÂPost-Quantum Lattice-Based Schemes: A Key Recovery Attack onÂSABER andÂBeyond. Lecture Notes in Computer Science, 2022, , 81-103.	1.0	2
4	The Bitlet Model: A Parameterized Analytical Model to Compare PIM and CPU Systems. ACM Journal on Emerging Technologies in Computing Systems, 2022, 18, 1-29.	1.8	10
5	Autonomous Vehicle: Security by Design. IEEE Transactions on Intelligent Transportation Systems, 2021, 22, 7015-7029.	4.7	61
6	PQC Acceleration Using GPUs: FrodoKEM, NewHope, and Kyber. IEEE Transactions on Parallel and Distributed Systems, 2021, 32, 575-586.	4.0	28
7	In-memory realization of SHA-2 using ReVAMP architecture. , 2021, , .		0
8	Perspectives on Emerging Computation-in-Memory Paradigms. , 2021, , .		9
9	A survey on adversarial attacks and defences. CAAI Transactions on Intelligence Technology, 2021, 6, 25-45.	3.4	115
10	MemEnc: A Lightweight, Low-Power, and Transparent Memory Encryption Engine for IoT. IEEE Internet of Things Journal, 2021, 8, 7182-7191.	5.5	3
11	Cycle PUF: A Cycle operator based PUF in Carbon Nanotube FET Technology. , 2021, , .		5
12	Application of Resistive Random Access Memory in Hardware Security: A Review. Advanced Electronic Materials, 2021, 7, 2100536.	2.6	20
13	Comprehensive Study of Side-Channel Attack on Emerging Non-Volatile Memories. Journal of Low Power Electronics and Applications, 2021, 11, 38.	1.3	6
14	Analysis of Aneuploidy Spectrum From Whole-Genome Sequencing Provides Rapid Assessment of Clonal Variation Within Established Cancer Cell Lines. Cancer Informatics, 2021, 20, 117693512110492.	0.9	0
15	ROWBACK: RObust Watermarking for neural networks using BACKdoors. , 2021, , .		3
16	Crossbar-Constrained Technology Mapping for ReRAM Based In-Memory Computing. IEEE Transactions on Computers, 2020, 69, 734-748.	2.4	11
17	Threshold Implementations of $mathtt{GIFT}$: A Trade-Off Analysis. IEEE Transactions on Information Forensics and Security, 2020, 15, 2110-2120.	4.5	16
18	Towards Designing a Secure RISC-V System-on-Chip: ITUS. Journal of Hardware and Systems Security, 2020, 4, 329-342.	0.8	9

#	Article	IF	Citations
19	Analysis of Area-Efficiency vs. Unrolling for eSTREAM Hardware Portfolio Stream Ciphers. Electronics (Switzerland), 2020, 9, 1935.	1.8	1
20	Post-Quantum Secure Boot. , 2020, , .		17
21	Towards Secure Composition of Integrated Circuits and Electronic Systems: On the Role of EDA. , 2020, , .		17
22	Identification and utilization of copy number information for correcting Hi-C contact map of cancer cell lines. BMC Bioinformatics, 2020, 21, 506.	1.2	4
23	Efficient Quantum Circuits for Square-Root and Inverse Square-Root. , 2020, , .		4
24	Hierarchical discovery of large-scale and focal copy number alterations in low-coverage cancer genomes. BMC Bioinformatics, 2020, 21, 147.	1.2	8
25	CONTRA. , 2020, , .		7
26	On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT. Lecture Notes in Computer Science, 2020, , 123-146.	1.0	14
27	Secure Your SoC: Building System-an-Chip Designs for Security. , 2020, , .		2
28	A Systematic Approach for Acceleration of Matrix-Vector Operations in CGRA through Algorithm-Architecture Co-Design. , 2019, , .		3
29	Sklansky tree adder realization in 1S1R resistive switching memory architecture. European Physical Journal: Special Topics, 2019, 228, 2269-2285.	1.2	15
30	Reversible Pebble Games for Reducing Qubits in Hierarchical Quantum Circuit Synthesis. , 2019, , .		3
31	SAID: A Supergate-Aided Logic Synthesis Flow for Memristive Crossbars. , 2019, , .		8
32	Design and synthesis of improved reversible circuits using AIGâ€•and MIGâ€•based graph data structures. IET Computers and Digital Techniques, 2019, 13, 38-48.	0.9	5
33	Spintronic Device-Structure for Low-Energy XOR Logic using Domain Wall Motion. , 2019, , .		8
34	Lightweight Secure-Boot Architecture for RISC-V System-on-Chip. , 2019, , .		20
35	High Level Synthesis for Symmetric Key Cryptography. Computer Architecture and Design Methodologies, 2019, , 51-90.	0.5	1
36	Security is an architectural design constraint. Microprocessors and Microsystems, 2019, 68, 17-27.	1.8	8

#	Article	IF	Citations
37	Accelerating Binary-Matrix Multiplication on FPGA. , 2019, , .		2
38	MUQUT: Multi-Constraint Quantum Circuit Mapping on NISQ Computers: Invited Paper. , 2019, , .		20
39	La Petite Fee Cosmo: Learning Data Structures Through Game-Based Learning. , 2019, , .		6
40	ITUS: A Secure RISC-V System-on-Chip. , 2019, , .		13
41	Techniques for fault-tolerant decomposition of a multicontrolled Toffoli gate. Physical Review A, 2019, 100, .	1.0	16
42	Curse of Dimensionality in Adversarial Examples. , 2019, , .		6
43	Guest Editorial Special Section on Security Challenges and Solutions With Emerging Computing Technologies. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 2469-2472.	2.1	0
44	An iterative method for linear decomposition of index generating functions. Cryptography and Communications, 2019, 11, 1079-1102.	0.9	3
45	Multi-valued and Fuzzy Logic Realization using TaOx Memristive Devices. Scientific Reports, 2018, 8, 8.	1.6	135
46	Wireless Communication and Security Issues for Cyberâ€“Physical Systems and the Internet-of-Things. Proceedings of the IEEE, 2018, 106, 38-60.	16.4	184
47	Technology-aware logic synthesis for ReRAM based in-memory computing. , 2018, , .		9
48	Toward Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation. IEEE Transactions on Industrial Informatics, 2018, 14, 2442-2451.	7.2	54
49	Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study. , 2018, , .		47
50	Floating Point Multiplication Mapping on ReRAM Based In-memory Computing Architecture. , 2018, , .		6
51	A Blockchain Framework for Insurance Processes. , 2018, , .		97
52	Accelerating Hash Computations Through Efficient Instruction-Set Customisation. , 2018, , .		3
53	TriviA and uTriviA: two fast and secure authenticated encryption schemes. Journal of Cryptographic Engineering, 2018, 8, 29-48.	1.5	3
54	Secure and Lightweight Compressive Sensing Using Stream Cipher. IEEE Transactions on Circuits and Systems II: Express Briefs, 2018, 65, 371-375.	2.2	20

#	Article	IF	Citations
55	BLIC: A Blockchain Protocol for Manufacturing and Supply Chain Management of ICS. , 2018, , .		8
56	CoLPUF : A Novel Configurable LFSR-based PUF. , 2018, , .		12
57	ReRAM-based In-Memory Computation of Galois Field arithmetic. , 2018, , .		1
58	Logic-In-Memory Architecture For Min/Max Search. , 2018, , .		3
59	Secure and Tamper-resilient Distributed Ledger for Data Aggregation in Autonomous Vehicles. , 2018, , .		7
60	MAMI: Majority and Multi-Input Logic on Memristive Crossbar Array. , 2018, , .		2
61	A template-based technique for efficient Clifford+T-based quantum circuit implementation. Microelectronics Journal, 2018, 81, 58-68.	1.1	21
62	Synthesis of Multi-valued Literal Using Lukasiewicz Logic. , 2018, , .		3
63	Domain Wall Motion-based XOR-like Activation Unit With A Programmable Threshold. , 2018, , .		1
64	Domain Wall Motion-Based Dual-Threshold Activation Unit for Low-Power Classification of Non-Linearly Separable Functions. IEEE Transactions on Biomedical Circuits and Systems, 2018, 12, 1410-1421.	2.7	1
65	Kogge-Stone Adder Realization using 1S1R Resistive Switching Crossbar Arrays. ACM Journal on Emerging Technologies in Computing Systems, 2018, 14, 1-14.	1.8	6
66	Efficient Realization of Householder Transform Through Algorithm-Architecture Co-Design for Acceleration of QR Factorization. IEEE Transactions on Parallel and Distributed Systems, 2018, 29, 1707-1720.	4.0	9
67	Quantum circuits for Toom-Cook multiplication. Physical Review A, 2018, 98, .	1.0	15
68	A New High Throughput and Area Efficient SHA-3 Implementation. , 2018, , .		28
69	Efficient and Lightweight Quantized Compressive Sensing using Î¼-Law. , 2018, , .		1
70	PPAP and iPPAP: PLL-Based Protection Against Physical Attacks. , 2018, , .		14
71	Lightweight ASIC Implementation of AEGIS-128. , 2018, , .		1
72	A Hardware-Efficient Implementation of CLOC for On-chip Authenticated Encryption. , 2018, , .		0

#	ARTICLE	IF	CITATIONS
73	Synthesis, Technology Mapping and Optimization for Emerging Technologies. , 2018, , .		0
74	Efficient Hardware Accelerator for NORX Authenticated Encryption. , 2018, , .		2
75	SMARTS. , 2018, , .		8
76	Achieving Efficient Realization of Kalman Filter on CGRA Through Algorithm-Architecture Co-design. Lecture Notes in Computer Science, 2018, , 119-131.	1.0	2
77	On Hardware Implementation of Tang-Maitra Boolean Functions. Lecture Notes in Computer Science, 2018, , 111-127.	1.0	0
78	A systematic security analysis of real-time cyber-physical systems. , 2017, , .		5
79	Area-constrained technology mapping for in-memory computing using ReRAM devices. , 2017, , .		10
80	SHA-3 implementation using ReRAM based in-memory computing architecture. , 2017, , .		10
81	Efficient complementary resistive switch-based crossbar array Booth multiplier. Microelectronics Journal, 2017, 64, 78-85.	1.1	15
82	An analysis of root functionsâ€”A subclass of the Impossible Class of Faulty Functions (ICFF). Discrete Applied Mathematics, 2017, 222, 1-13.	0.5	1
83	Efficient Binary Basic Linear Algebra Operations on ReRAM Crossbar Arrays. , 2017, , .		8
84	A Flexible Divide-and-Conquer MPSoC Architecture for MIMO Interference Cancellation. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 2789-2802.	2.1	0
85	Storages Are Not Forever. Cognitive Computation, 2017, 9, 646-658.	3.6	4
86	Accelerating BLAS and LAPACK via Efficient Floating Point Architecture Design. Parallel Processing Letters, 2017, 27, 1750006.	0.4	8
87	ReVAMP: ReRAM based VLIW architecture for in-memory computing. , 2017, , .		47
88	RC4-AccSuite: A Hardware Acceleration Suite for RC4-Like Stream Ciphers. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 1072-1084.	2.1	12
89	Efficient implementation of generalized Maioranaâ€“McFarland class of cryptographic functions. Journal of Cryptographic Engineering, 2017, 7, 287-295.	1.5	3
90	Side-Channel Attack on STTRAM Based Cache for Cryptographic Application. , 2017, , .		20

#	Article	IF	Citations
91	A Practical Fault Attack on ARX-Like Ciphers with a Case Study on ChaCha20. , 2017, , .		15
92	Attacks in Reality: the Limits of Concurrent Error Detection Codes Against Laser Fault Injection. Journal of Hardware and Systems Security, 2017, 1, 298-310.	0.8	7
93	Survey of secure processors. , 2017, , .		9
94	In-Memory Data Compression Using ReRAMs. , 2017, , 275-291.		3
95	Looting the LUTs: FPGA Optimization of AES and AES-like Ciphers for Authenticated Encryption. Lecture Notes in Computer Science, 2017, , 282-301.	1.0	11
96	Racetrack memory-based encoder/decoder for low-power interconnect architectures. , 2016, , .		0
97	Modified projected Landweber method for Compressive-Sensing reconstruction of images with non-orthogonal matrices. , 2016, , .		1
98	Integrated Synthesis of Linear Nearest Neighbor Ancilla-Free MCT Circuits. , 2016, , .		17
99	Notes on Majority Boolean Algebra. , 2016, , .		13
100	Low-quantum cost circuit constructions for adder and symmetric Boolean functions. , 2016, , .		2
101	Enabling in-memory computation of binary BLAS using ReRAM crossbar arrays. , 2016, , .		11
102	FPGA Based Cyber Security Protocol for Automated Traffic Monitoring Systems: Proposal and Implementation. , 2016, , .		3
103	Multistate Memristive Tantalum Oxide Devices for Ternary Arithmetic. Scientific Reports, 2016, 6, 36652.	1.6	58
104	Energy Optimization of Racetrack Memory-Based SIMON Block Cipher. , 2016, , .		2
105	Achieving Efficient QR Factorization by Algorithm-Architecture Co-design of Householder Transformation. , 2016, , .		7
106	RunFein: a rapid prototyping framework for Feistel and SPN-based block ciphers. Journal of Cryptographic Engineering, 2016, 6, 299-323.	1.5	4
107	The<i>Programmable Logic-in-Memory</i>(PLiM) Computer. , 2016, , .		59
108	A Low Overhead Error Confinement Method based on Application Statistical Characteristics. , 2016, , .		2

#	Article	IF	Citations
109	Exploiting Dynamic Timing Margins in Microprocessors for Frequency-Over-Scaling with Instruction-Based Clock Adjustment. , 2015, , .		25
110	Design and synthesis of reconfigurable control-flow structures for CGRA. , 2015, , .		3
111	EvoDeb: Debugging Evolving Hardware Designs. , 2015, , .		4
112	Architectural reliability estimation using design diversity. , 2015, , .		5
113	TriviA: A Fast and Secure Authenticated Encryption Scheme. Lecture Notes in Computer Science, 2015, , 330-353.	1.0	18
114	Reversible Logic Synthesis via Biconditional Binary Decision Diagrams. , 2015, , .		11
115	Efficient Hardware Accelerator for AEGIS-128 Authenticated Encryption. Lecture Notes in Computer Science, 2015, , 385-402.	1.0	5
116	Force-directed scheduling for Data Flow Graph mapping on Coarse-Grained Reconfigurable Architectures. , 2014, , .		16
117	Scalable and energy-efficient reconfigurable accelerator for column-wise givens rotation. , 2014, , .		10
118	Efficient QR Decomposition Using Low Complexity Column-wise Givens Rotation (CGR). , 2014, , .		8
119	Efficient and scalable CGRA-based implementation of Column-wise Givens Rotation. , 2014, , .		8
120	CoARX. , 2013, , .		21
121	RAPID-FeinSPN: A Rapid Prototyping Framework for Feistel and SPN-Based Block Ciphers. Lecture Notes in Computer Science, 2013, , 169-190.	1.0	6
122	Exploring security-performance trade-offs during hardware accelerator design of stream cipher RC4. , 2012, , .		4
123	LISA. , 2008, , 95-132.		25
124	Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 307-335.	0.0	63