Debdeep Mukhopadhyay

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/5506214/publications.pdf

Version: 2024-02-01

103 papers	2,029 citations	304602 22 h-index	276775 41 g-index
105 all docs	105 docs citations	105 times ranked	1206 citing authors

#	Article	IF	Citations
1	Building PUF Based Authentication and Key Exchange Protocol for IoT Without Explicit CRPs in Verifier Database. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 424-437.	3.7	171
2	Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault. Lecture Notes in Computer Science, 2011, , 224-233.	1.0	166
3	A PUF-Based Secure Communication Protocol for IoT. Transactions on Embedded Computing Systems, 2017, 16, 1-25.	2.1	132
4	A survey on adversarial attacks and defences. CAAI Transactions on Intelligence Technology, 2021, 6, 25-45.	3.4	115
5	A Multiplexer-Based Arbiter PUF Composition with Enhanced Reliability and Security. IEEE Transactions on Computers, 2018, 67, 403-417.	2.4	108
6	Secured Flipped Scan-Chain Model for Crypto-Architecture. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2007, 26, 2080-2084.	1.9	104
7	A Case of Lightweight PUF Constructions: Cryptanalysis and Machine Learning Attacks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 1334-1343.	1.9	64
8	Security analysis of concurrent error detection against differential fault analysis. Journal of Cryptographic Engineering, 2015, 5, 153-169.	1.5	61
9	Petrel: Power and Timing Attack Resistant Elliptic Curve Scalar Multiplier Based on Programmable ${m GF}(p)$ Arithmetic Unit. IEEE Transactions on Circuits and Systems I: Regular Papers, 2011, 58, 1798-1812.	3.5	53
10	Theoretical Modeling of Elliptic Curve Scalar Multiplier on LUT-Based FPGAs for Area and Speed. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2013, 21, 901-909.	2.1	46
11	Revisiting the Itoh-Tsujii Inversion Algorithm for FPGA Platforms. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2011, 19, 1508-1512.	2.1	41
12	Differential fault analysis of AES: towards reaching its limits. Journal of Cryptographic Engineering, 2013, 3, 73-97.	1.5	41
13	Constrained Search for a Class of Good Bijective S-Boxes With Improved DPA Resistivity. IEEE Transactions on Information Forensics and Security, 2013, 8, 2154-2163.	4.5	41
14	A Biased Fault Attack on the Time Redundancy Countermeasure for AES. Lecture Notes in Computer Science, 2015, , 189-203.	1.0	41
15	Who Watches the Watchmen?: Utilizing Performance Monitors for Compromising Keys of RSA on Intel Platforms. Lecture Notes in Computer Science, 2015, , 248-266.	1.0	38
16	Provably Secure Key-Aggregate Cryptosystems with Broadcast Aggregate Keys for Online Data Sharing on the Cloud. IEEE Transactions on Computers, 2017, 66, 891-904.	2.4	36
17	High-Speed Implementation of ECC Scalar Multiplication in GF(p) for Generic Montgomery Curves. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 1587-1600.	2.1	33
18	A Framework to Counter Statistical Ineffective Fault Analysis of Block Ciphers Using Domain Transformation and Error Correction. IEEE Transactions on Information Forensics and Security, 2020, 15, 1905-1919.	4.5	30

#	Article	IF	Citations
19	Fault Template Attacks on Block Ciphers Exploiting Fault Propagation. Lecture Notes in Computer Science, 2020, , 612-643.	1.0	29
20	Fault Space Transformation: A Generic Approach to Counter Differential Fault Analysis and Differential Fault Intensity Analysis on AES-Like Block Ciphers. IEEE Transactions on Information Forensics and Security, 2017, 12, 1092-1102.	4.5	28
21	Fault Tolerant Infective Countermeasure for AES. Journal of Hardware and Systems Security, 2017, 1, 3-17.	0.8	25
22	3PAA: A <u>P</u>rivate <u>P</u>UF <u>P</u>rotocol for <u>A</u>nonymous <u>A</u>uthentication. IEEE Transactions on Information Forensics and Security, 2021, 16, 756-769.	4.5	25
23	Multi-level attacks: An emerging security concern for cryptographic hardware. , 2011, , .		24
24	High Speed Flexible Pairing Cryptoprocessor on FPGA Platform. Lecture Notes in Computer Science, 2010, , 450-466.	1.0	20
25	Pinpointing Cache Timing Attacks on AES. , 2010, , .		19
26	Introducing Recurrence in Strong PUFs for Enhanced Machine Learning Attack Resistance. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2021, 11, 319-332.	2.7	19
27	Secure Dual-Core Cryptoprocessor for Pairings Over Barreto-Naehrig Curves on FPGA Platform. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2013, 21, 434-442.	2.1	18
28	From theory to practice of private circuit: A cautionary note. , 2015, , .		18
29	Automatic Characterization of Exploitable Faults: A Machine Learning Approach. IEEE Transactions on Information Forensics and Security, 2019, 14, 954-968.	4.5	18
30	Design and implementation of rotation symmetric S-boxes with high nonlinearity and high DPA resilience. , 2013, , .		17
31	SCADFA: Combined SCA+DFA Attacks on Block Ciphers with Practical Validations. IEEE Transactions on Computers, 2019, 68, 1498-1510.	2.4	16
32	Lightweight Design-for-Security Strategies for Combined Countermeasures Against Side Channel and Fault Analysis in IoT Applications. Journal of Hardware and Systems Security, 2019, 3, 103-131.	0.8	16
33	Improved Practical Differential Fault Analysis of Grain-128. , 2015, , .		15
34	An Evaluation of Lightweight Block Ciphers for Resource-Constrained Applications: Area, Performance, and Security. Journal of Hardware and Systems Security, 2017, 1, 203-218.	0.8	15
35	A Practical Fault Attack on ARX-Like Ciphers with a Case Study on ChaCha20. , 2017, , .		15
36	LoPher: SAT-Hardened Logic Embedding on Block Ciphers. , 2020, , .		15

#	Article	IF	Citations
37	Hardware Prefetchers Leak: A Revisit of SVF for Cache-Timing Attacks. , 2012, , .		14
38	Construction of Rotation Symmetric S-Boxes with High Nonlinearity and Improved DPA Resistivity. IEEE Transactions on Computers, 2017, 66, 59-72.	2.4	14
39	Hierarchical Verification of Galois Field Circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2007, 26, 1893-1898.	1.9	12
40	DRECON: DPA Resistant Encryption by Construction. Lecture Notes in Computer Science, 2014, , 420-439.	1.0	12
41	Lightweight and Side-channel Secure 4 Ã— 4 S-Boxes from Cellular Automata Rules. IACR Transactions on Symmetric Cryptology, 0, , 311-334.	0.0	12
42	Improved Differential Fault Analysis of CLEFIA. , 2013, , .		11
43	DFARPA: Differential fault attack resistant physical design automation. , 2018, , .		11
44	High speed F<inf>p</inf> multipliers and adders on FPGA platform. , 2010, , .		10
45	A Parallel Efficient Architecture for Large Cryptographically Robust n Ã— k (k>n/2) Mappings. IEEE Transactions on Computers, 2011, 60, 375-385.	2.4	10
46	Design for Security of Block Cipher S-Boxes to Resist Differential Power Attacks. , 2012, , .		10
47	Reaching the Limit of Nonprofiling DPA. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 915-927.	1.9	10
48	Micro-Architectural Analysis of Time-Driven Cache Attacks: Quest for the Ideal Implementation. IEEE Transactions on Computers, 2015, 64, 778-790.	2.4	10
49	Testability Based Metric for Hardware Trojan Vulnerability Assessment. , 2016, , .		10
50	A Combined Power and Fault Analysis Attack on Protected Grain Family of Stream Ciphers. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, 36, 1968-1977.	1.9	10
51	Breaking Redundancy-Based Countermeasures with Random Faults and Power Side Channel. , 2018, , .		10
52	A Parallel Architecture for Koblitz Curve Scalar Multiplications on FPGA Platforms. , 2012, , .		9
53	Formalizing the Effect of Feistel Cipher Structures on Differential Cache Attacks. IEEE Transactions on Information Forensics and Security, 2013, 8, 1274-1279.	4.5	9
54	PUFSSL: An OpenSSL Extension for PUF based Authentication. , 2018, , .		9

#	Article	IF	Citations
55	Trustworthy proofs for sensor data using FPGA based physically unclonable functions. , 2018, , .		9
56	Using Tweaks to Design Fault Resistant Ciphers. , 2016, , .		8
57	BLIC: A Blockchain Protocol for Manufacturing and Supply Chain Management of ICS. , 2018, , .		8
58	Count Your Toggles: a New Leakage Model for Pre-Silicon Power Analysis of Crypto Designs. Journal of Electronic Testing: Theory and Applications (JETTA), 2019, 35, 605-619.	0.9	8
59	Branch Prediction Attack on Blinded Scalar Multiplication. IEEE Transactions on Computers, 2020, 69, 633-648.	2.4	8
60	ORACALL: An Oracle-Based Attack on Cellular Automata Guided Logic Locking. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40, 2445-2454.	1.9	8
61	Formal fault analysis of branch predictors: attacking countermeasures of asymmetric key ciphers. Journal of Cryptographic Engineering, 2017, 7, 299-310.	1.5	7
62	Revisiting FPGA Implementation of Montgomery Multiplier in Redundant Number System for Efficient ECC Application in GF(p). , 2018, , .		7
63	Shuffling across rounds: A lightweight strategy to counter side-channel attacks. , 2016, , .		6
64	SmashClean: A hardware level mitigation to stack smashing attacks in OpenRISC. , 2016, , .		6
65	ExplFrame: Exploiting Page Frame Cache for Fault Analysis of Block Ciphers. , 2020, , .		6
66	A practical DPA on Grain v1 using LS-SVM. , 2015, , .		5
67	Inner collisions in ECC: Vulnerabilities of complete addition formulas for NIST curves. , 2016, , .		5
68	The Conflicted Usage of RLUTs for Security-Critical Applications on FPGA. Journal of Hardware and Systems Security, 2018, 2, 162-178.	0.8	5
69	Divided We Stand, United We Fall: Security Analysis of Some SCA+SIFA Countermeasures Against SCA-Enhanced Fault Template Attacks. Lecture Notes in Computer Science, 2021, , 62-94.	1.0	5
70	Testability of Cryptographic Hardware and Detection of Hardware Trojans. , 2011, , .		4
71	An automated framework for exploitable fault identification in block ciphers. Journal of Cryptographic Engineering, 2019, 9, 203-219.	1.5	4
72	SACReD: An Attack Framework on SAC Resistant Delay-PUFs leveraging Bias and Reliability Factors. , 2021, , .		4

#	Article	IF	Citations
73	An Efficient Design of Cellular Automata Based Cryptographically Robust One-Way Function. , 2007, , .		3
74	Designing DPA Resistant Circuits Using BDD Architecture and Bottom Pre-charge Logic. , 2013, , .		3
75	Secure public key hardware for IoT applications. , 2016, , .		3
76	Template attack on SPA and FA resistant implementation of Montgomery ladder. IET Information Security, 2016, 10, 245-251.	1.1	3
77	A Machine Learning Based Approach to Predict Power Efficiency of S-Boxes. , 2019, , .		3
78	Fault Attack on SKINNY Cipher. Journal of Hardware and Systems Security, 2020, 4, 277-296.	0.8	3
79	A Formal Analysis of Prefetching in Profiled Cache-Timing Attacks on Block Ciphers. Journal of Cryptology, 2021, 34, 1.	2.1	3
80	Faultless to a fault?. , 2020, , .		3
81	Preventing the Side-Channel Leakage of Masked AES S-Box. , 2007, , .		2
82	Circuits and Synthesis Mechanism for Hardware Design to Counter Power Analysis Attacks. , 2014, , .		2
83	Accelerating OpenSSL's ECC with low cost reconfigurable hardware. , 2016, , .		2
84	A Practical Template Attack on MICKEY-128 2.0 Using PSO Generated IVs and LS-SVM. , 2016, , .		2
85	Online Detection and Reactive Countermeasure for Leakage from BPU Using TVLA. , 2018, , .		2
86	Customized Instructions for Protection Against Memory Integrity Attacks. IEEE Embedded Systems Letters, 2018, 10, 91-94.	1.3	2
87	Power Efficiency of S-Boxes: From a Machine-Learning-Based Tool to a Deterministic Model. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 2829-2841.	2.1	2
88	Performance, Security Tradeoffs in Secure Control. IEEE Embedded Systems Letters, 2019, 11, 102-105.	1.3	2
89	Evolution of Fault Attacks on Cryptosystems. , 2021, , 1-7.		2
90	FlexiPair: An Automated Programmable Framework for Pairing Cryptosystems. IEEE Transactions on Computers, 2022, 71, 506-519.	2.4	2

#	Article	IF	Citations
91	Fault based attack of the Rijndael cryptosystem. Journal of Discrete Mathematical Sciences and Cryptography, 2007, 10, 267-290.	0.5	1
92	Construction of RSBFs with improved cryptographic properties to resist differential fault attack on grain family of stream ciphers. Cryptography and Communications, 2015, 7, 35-69.	0.9	1
93	Opening pandora's box: Implication of RLUT on secure FPGA applications and IP security. , 2017, , .		1
94	Minimalistic Perspective to Public Key Implementations on FPGA. , 2018, , .		1
95	Design and Analysis of Logic Locking Techniques. , 2021, , .		1
96	Transform Without Encode is not Sufficient for SIFA and FTA Security: A Case Study. Lecture Notes in Computer Science, 2021, , 85-104.	1.0	1
97	On-line testing for differential fault attacks in cryptographic circuits. , 2013, , .		0
98	Parsimonious design strategy for linear layers with high diffusion in block ciphers. , 2016, , .		0
99	Editorial for the Special Issue in Journal of Hardware and Systems Security (HaSS) Based on Selected Papers from 6th International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE 2016). Journal of Hardware and Systems Security, 2017, 1, 201-202.	0.8	0
100	Guest Editorial: Special Section on Autonomous Intelligence for Security and Privacy Analytics. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 2703-2705.	2.1	0
101	Exploitable Fault Space Characterization: A Complementary Approach. , 2019, , 59-88.		0
102	Hardware Security in India: The Journey so Far. IITK Directions, 2020, , 71-96.	0.2	0
103	PAKAMAC: A PUF-based Keyless Automotive Entry System with Mutual Authentication. Journal of Hardware and Systems Security, 0, , .	0.8	0