Lejla Batina

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/10565165/publications.pdf

Version: 2024-02-01

34
papers

1,385
citations

623734
14
h-index

501196
28
g-index

36
all docs

36
docs citations

36
times ranked

706
citing authors

#	Article	IF	Citations
1	Fake It Till You Make It: Data Augmentation Using Generative Adversarial Networks for All the Crypto You Need on Small Devices. Lecture Notes in Computer Science, 2022, , 297-321.	1.3	4
2	The Uncertainty of Side-channel Analysis: A Way to Leverage from Heuristics. ACM Journal on Emerging Technologies in Computing Systems, 2021, 17, 1-27.	2.3	3
3	Auto-tune POIs: Estimation of distribution algorithms for efficient side-channel analysis. Computer Networks, 2021, 198, 108405.	5.1	10
4	Systematic Side-Channel Analysis of Curve25519 with Machine Learning. Journal of Hardware and Systems Security, 2020, 4, 314-328.	1.3	9
5	Online Template Attack on ECDSA:. Lecture Notes in Computer Science, 2020, , 323-336.	1.3	7
6	Balancing elliptic curve coprocessors from bottom to top. Microprocessors and Microsystems, 2019, 71, 102866.	2.8	0
7	Online template attacks. Journal of Cryptographic Engineering, 2019, 9, 21-36.	1.8	18
8	One Trace Is All It Takes: Machine Learning-Based Side-Channel Attack on EdDSA. Lecture Notes in Computer Science, 2019, , 86-105.	1.3	27
9	Breaking Ed25519 in WolfSSL. Lecture Notes in Computer Science, 2018, , 1-20.	1.3	10
10	Completing the Complete ECC Formulae with Countermeasures. Journal of Low Power Electronics and Applications, 2017, 7, 3.	2.0	9
11	Bitsliced Masking and ARM: Friends or Foes?. Lecture Notes in Computer Science, 2017, , 91-109.	1.3	8
12	LDA-Based Clustering as a Side-Channel Distinguisher. Lecture Notes in Computer Science, 2017, , 62-75.	1.3	2
13	An Elliptic Curve Cryptographic Processor Using Edwards Curves and the Number Theoretic Transform. Lecture Notes in Computer Science, 2015, , 94-102.	1.3	3
14	Online Template Attacks. Lecture Notes in Computer Science, 2014, , 21-36.	1.3	34
15	High-Speed Dating Privacy-Preserving Attribute Matching for RFID. Lecture Notes in Computer Science, 2014, , 19-35.	1.3	0
16	Signal Processing for Cryptography and Security Applications. , 2013, , 223-241.		3
17	Extending ECC-based RFID authentication protocols to privacy-preserving multi-party grouping proofs. Personal and Ubiquitous Computing, 2012, 16, 323-335.	2.8	36
18	Hierarchical ECC-Based RFID Authentication Protocol. Lecture Notes in Computer Science, 2012, , 183-201.	1.3	14

#	Article	IF	Citations
19	Mutual Information Analysis: aÂComprehensive Study. Journal of Cryptology, 2011, 24, 269-291.	2.8	203
20	Design and design methods for unified multiplier and inverter and its application for HECC. The Integration VLSI Journal, 2011, 44, 280-289.	2.1	12
21	Wideâ€"Weak Privacyâ€"Preserving RFID Authentication Protocols. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 254-267.	0.3	12
22	Side-channel evaluation of FPGA implementations of binary Edwards curves. , 2010, , .		11
23	Breaking Elliptic Curve Cryptosystems Using Reconfigurable Hardware. , 2010, , .		14
24	Compact Public-Key Implementations for RFID and Sensor Nodes. Integrated Circuits and Systems, 2010, , 179-195.	0.2	1
25	Revisiting Higher-Order DPA Attacks:. Lecture Notes in Computer Science, 2010, , 221-234.	1.3	45
26	Anti-counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware. Information Security and Cryptography, 2010, , 237-257.	0.3	12
27	Signal Processing for Cryptography and Security Applications. , 2010, , 161-177.		0
28	Untraceable RFID authentication protocols: Revision of EC-RAC. , 2009, , .		16
29	Differential Cluster Analysis. Lecture Notes in Computer Science, 2009, , 112-127.	1.3	43
30	EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. , 2008, , .		84
31	Elliptic-Curve-Based Security Processor for RFID. IEEE Transactions on Computers, 2008, 57, 1514-1527.	3.4	181
32	Mutual Information Analysis. Lecture Notes in Computer Science, 2008, , 426-442.	1.3	383
33	Multicore Curve-Based Cryptoprocessor with Reconfigurable Modular Arithmetic Logic Units over GF(2^n). IEEE Transactions on Computers, 2007, 56, 1269-1282.	3.4	46
34	High-performance Public-key Cryptoprocessor for Wireless Mobile Applications. Mobile Networks and Applications, 2007, 12, 245-258.	3.3	16