

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	Mutual Information Analysis. Lecture Notes in Computer Science, 2008, , 426-442.	1.3	383
2	Mutual Information Analysis: a Comprehensive Study. Journal of Cryptology, 2011, 24, 269-291.	2.8	203
3	Elliptic-Curve-Based Security Processor for RFID. IEEE Transactions on Computers, 2008, 57, 1514-1527.	3.4	181
4	EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. , 2008, , .		84
5	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
6	Revisiting Higher-Order DPA Attacks:. Lecture Notes in Computer Science, 2010, , 221-234.	1.3	45
7	Differential Cluster Analysis. Lecture Notes in Computer Science, 2009, , 112-127.	1.3	43
8	Extending ECC-based RFID authentication protocols to privacy-preserving multi-party grouping proofs. Personal and Ubiquitous Computing, 2012, 16, 323-335.	2.8	36
9	Online Template Attacks. Lecture Notes in Computer Science, 2014, , 21-36.	1.3	34
10	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
11	Online template attacks. Journal of Cryptographic Engineering, 2019, 9, 21-36.	1.8	18
12	High-performance Public-key Cryptoprocessor for Wireless Mobile Applications. Mobile Networks and Applications, 2007, 12, 245-258.	3.3	16
13	Untraceable RFID authentication protocols: Revision of EC-RAC. , 2009, , .		16
14	Breaking Elliptic Curve Cryptosystems Using Reconfigurable Hardware. , 2010, , .		14
15	Hierarchical ECC-Based RFID Authentication Protocol. Lecture Notes in Computer Science, 2012, , 183-201.	1.3	14
16	Wide-Weak Privacy-Preserving RFID Authentication Protocols. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 254-267.	0.3	12
17	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
18	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

#	ARTICLE	IF	CITATIONS
19	Side-channel evaluation of FPGA implementations of binary Edwards curves. , 2010, , .		11
20	Breaking Ed25519 in WolfSSL. Lecture Notes in Computer Science, 2018, , 1-20.	1.3	10
21	Auto-tune POIs: Estimation of distribution algorithms for efficient side-channel analysis. Computer Networks, 2021, 198, 108405.	5.1	10
22	Completing the Complete ECC Formulae with Countermeasures. Journal of Low Power Electronics and Applications, 2017, 7, 3.	2.0	9
23	Systematic Side-Channel Analysis of Curve25519 with Machine Learning. Journal of Hardware and Systems Security, 2020, 4, 314-328.	1.3	9
24	Bitsliced Masking and ARM: Friends or Foes?. Lecture Notes in Computer Science, 2017, , 91-109.	1.3	8
25	Online Template Attack on ECDSA:. Lecture Notes in Computer Science, 2020, , 323-336.	1.3	7
26	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
27	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
28	Signal Processing for Cryptography and Security Applications. , 2013, , 223-241.		3
29	An Elliptic Curve Cryptographic Processor Using Edwards Curves and the Number Theoretic Transform. Lecture Notes in Computer Science, 2015, , 94-102.	1.3	3
30	LDA-Based Clustering as a Side-Channel Distinguisher. Lecture Notes in Computer Science, 2017, , 62-75.	1.3	2
31	Compact Public-Key Implementations for RFID and Sensor Nodes. Integrated Circuits and Systems, 2010, , 179-195.	0.2	1
32	Balancing elliptic curve coprocessors from bottom to top. Microprocessors and Microsystems, 2019, 71, 102866.	2.8	0
33	Signal Processing for Cryptography and Security Applications. , 2010, , 161-177.		0
34	High-Speed Dating Privacy-Preserving Attribute Matching for RFID. Lecture Notes in Computer Science, 2014, , 19-35.	1.3	0