Elisabeth Oswald

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/1198105/publications.pdf

Version: 2024-02-01

51 papers	2,389 citations	293460 24 h-index	252626 46 g-index
56 all docs	56 docs citations	56 times ranked	851 citing authors

#	Article	IF	Citations
1	A Novel Completeness Test forÂLeakage Models andÂIts Application toÂSide Channel Attacks andÂResponsibly Engineered Simulators. Lecture Notes in Computer Science, 2022, , 254-283.	1.0	1
2	Neymanâ€™s Smoothness Test: A Trade-Off Between Moment-Based and Distribution-Based Leakage Detections. IEEE Transactions on Information Forensics and Security, 2021, 16, 4494-4506.	4.5	0
3	Exploring Parallelism to Improve the Performance of FrodoKEM in Hardware. Journal of Cryptographic Engineering, 2021, 11, 317-327.	1.5	5
4	A Systematic Appraisal of Side Channel Evaluation Strategies. Lecture Notes in Computer Science, 2020, , 46-66.	1.0	11
5	Fault Attack Countermeasures for Error Samplers in Lattice-Based Cryptography. , 2019, , .		14
6	Assessing the Feasibility of Single Trace Power Analysis of Frodo. Lecture Notes in Computer Science, 2019, , 216-234.	1.0	13
7	A Critical Analysis of ISO 17825 (â€˜Testing Methods for the Mitigation of Non-invasive Attack Classes) Tj ETQq1 1 0.784314 rgBT /O	1.0	16
8	A Systematic Study of the Impact of Graphical Models on Inference-Based Attacks on AES. Lecture Notes in Computer Science, 2019, , 18-34.	1.0	4
9	Non-profiled Mask Recovery: The Impact of Independent Component Analysis. Lecture Notes in Computer Science, 2019, , 51-64.	1.0	0
10	Two Sides of the Same Coin: Counting and Enumerating Keys Post Side-Channel Attacks Revisited. Lecture Notes in Computer Science, 2018, , 394-412.	1.0	13
11	Quantum Key Search with Side Channel Advice. Lecture Notes in Computer Science, 2018, , 407-422.	1.0	11
12	Categorising and Comparing Cluster-Based DPA Distinguishers. Lecture Notes in Computer Science, 2018, , 442-458.	1.0	1
13	Authenticated Encryption in the Face of Protocol and Side Channel Leakage. Lecture Notes in Computer Science, 2017, , 693-723.	1.0	26
14	Cryptographic randomness on a CC2538: A case study. , 2016, , .		2
15	Characterisation and Estimation of the Key Rank Distribution in the Context of Side Channel Evaluations. Lecture Notes in Computer Science, 2016, , 548-572.	1.0	21
16	Characterising and Comparing the Energy Consumption of Side Channel Attack Countermeasures and Lightweight Cryptography on Embedded Devices. , 2015, , .		7
17	A Leakage Resilient MAC. Lecture Notes in Computer Science, 2015, , 295-310.	1.0	8
18	Robust Profiling for DPA-Style Attacks. Lecture Notes in Computer Science, 2015, , 3-21.	1.0	21

#	Article	IF	Citations
19	Counting Keys in Parallel After a Side Channel Attack. Lecture Notes in Computer Science, 2015, , 313-337.	1.0	43
20	Multi-target DPA Attacks: Pushing DPA Beyond the Limits of a Desktop Computer. Lecture Notes in Computer Science, 2014, , 243-261.	1.0	28
21	The Myth of Generic DPAâ€¦and the Magic of Learning. Lecture Notes in Computer Science, 2014, , 183-205.	1.0	43
22	Masking Tablesâ€”An Underestimated Security Risk. Lecture Notes in Computer Science, 2014, , 425-444.	1.0	22
23	Simulatable Leakage: Analysis, Pitfalls, and New Constructions. Lecture Notes in Computer Science, 2014, , 223-242.	1.0	12
24	Does My Device Leak Information? An a priori Statistical Power Analysis of Leakage Detection Tests. Lecture Notes in Computer Science, 2013, , 486-505.	1.0	51
25	Pinpointing side-channel information leaks in web applications. Journal of Cryptographic Engineering, 2012, 2, 161-177.	1.5	3
26	Compiler Assisted Masking. Lecture Notes in Computer Science, 2012, , 58-75.	1.0	50
27	One for all â€“ all for one: unifying standard differential power analysis attacks. IET Information Security, 2011, 5, 100.	1.1	132
28	A Comprehensive Evaluation of Mutual Information Analysis Using a Fair Evaluation Framework. Lecture Notes in Computer Science, 2011, , 316-334.	1.0	44
29	A fair evaluation framework for comparing side-channel distinguishers. Journal of Cryptographic Engineering, 2011, 1, 145-160.	1.5	45
30	An Exploration of the Kolmogorov-Smirnov Test as a Competitor to Mutual Information Analysis. Lecture Notes in Computer Science, 2011, , 234-251.	1.0	42
31	Counteracting Power Analysis Attacks by Masking. Integrated Circuits and Systems, 2010, , 159-178.	0.2	1
32	Side-Channel Analysis of Cryptographic Software via Early-Terminating Multiplications. Lecture Notes in Computer Science, 2010, , 176-192.	1.0	14
33	Leakage Resilient Cryptography in Practice. Information Security and Cryptography, 2010, , 99-134.	0.2	65
34	The World Is Not Enough: Another Look on Second-Order DPA. Lecture Notes in Computer Science, 2010, , 112-129.	1.0	128
35	Template Attacks on ECDSA. Lecture Notes in Computer Science, 2009, , 14-27.	1.0	40
36	Randomised representations. IET Information Security, 2008, 2, 19.	1.1	14

#	Article	IF	Citations
37	Power Analysis Attacks and Countermeasures. IEEE Design and Test of Computers, 2007, 24, 535-543.	1.4	66
38	Investigations of Power Analysis Attacks and Countermeasures for ARIA. , 2007, , 160-172.		3
39	Template Attacks on Maskingâ€"Resistance Is Futile. Lecture Notes in Computer Science, 2006, , 243-256.	1.0	73
40	An AES Smart Card Implementation Resistant to Power Analysis Attacks. Lecture Notes in Computer Science, 2006, , 239-252.	1.0	160
41	An Efficient Masking Scheme for AES Software Implementations. Lecture Notes in Computer Science, 2006, , 292-305.	1.0	40
42	Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers. Lecture Notes in Computer Science, 2006, , 192-207.	1.0	116
43	Searching for Differential Paths in MD4. Lecture Notes in Computer Science, 2006, , 242-261.	1.0	16
44	Practical Template Attacks. Lecture Notes in Computer Science, 2005, , 440-456.	1.0	104
45	Representations and Rijndael Descriptions. Lecture Notes in Computer Science, 2005, , 148-158.	1.0	4
46	A Side-Channel Analysis Resistant Description of the AES S-Box. Lecture Notes in Computer Science, 2005, , 413-423.	1.0	200
47	Successfully Attacking Masked AES Hardware Implementations. Lecture Notes in Computer Science, 2005, , 157-171.	1.0	221
48	Power-Analysis Attacks on an FPGA â€“ First Experimental Results. Lecture Notes in Computer Science, 2003, , 35-50.	1.0	72
49	Enhancing Simple Power-Analysis Attacks on Elliptic Curve Cryptosystems. Lecture Notes in Computer Science, 2003, , 82-97.	1.0	22
50	An ASIC Implementation of the AES SBoxes. , 2002, , 67-78.		180
51	Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks. Lecture Notes in Computer Science, 2001, , 39-50.	1.0	73