Werner Schindler

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/3867008/publications.pdf

Version: 2024-02-01

20	719	858243	889612
papers	citations	12	19
		h-index	g-index

23	23	23	304
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Timing attacks and local timing attacks against Barrettâ€™s modular multiplication algorithm. Journal of Cryptographic Engineering, 2021, 11, 369-397.	1.5	0
2	Stochastic methods defeat regular RSA exponentiation algorithms with combined blinding methods. Journal of Mathematical Cryptology, 2021, 15, 408-433.	0.4	1
3	Generic power attacks on RSA with CRT and exponent blinding: new results. Journal of Cryptographic Engineering, 2017, 7, 255-272.	1.5	9
4	Exclusive exponent blinding is not enough to prevent any timing attack on RSA. Journal of Cryptographic Engineering, 2016, 6, 101-119.	1.5	5
5	Exclusive Exponent Blinding May Not Suffice to Prevent Timing Attacks on RSA. Lecture Notes in Computer Science, 2015, , 229-247.	1.0	14
6	Practical improvements of side-channel attacks on AES: feedback from the 2nd DPA contest. Journal of Cryptographic Engineering, 2014, 4, 259-274.	1.5	27
7	Power attacks in the presence of exponent blinding. Journal of Cryptographic Engineering, 2014, 4, 213-236.	1.5	12
8	A New Difference Method for Side-Channel Analysis with High-Dimensional Leakage Models. Lecture Notes in Computer Science, 2012, , 365-382.	1.0	22
9	How a Symmetry Metric Assists Side-Channel Evaluation - A Novel Model Verification Method for Power Analysis. , 2011, , .		10
10	Exponent Blinding Does Not Always Lift (Partial) Spa Resistance to Higher-Level Security. Lecture Notes in Computer Science, 2011, , 73-90.	1.0	19
11	Advanced stochastic methods in side channel analysis on block ciphers in the presence of masking. Journal of Mathematical Cryptology, 2008, 2, .	0.4	29
12	A Vulnerability in RSA Implementations Due to Instruction Cache Analysis and Its Demonstration on OpenSSL. Lecture Notes in Computer Science, 2008, , 256-273.	1.0	41
13	Improving Brumley and Boneh timing attack on unprotected SSL implementations. , 2005, , .		41
14	A Stochastic Model for Differential Side Channel Cryptanalysis. Lecture Notes in Computer Science, 2005, , 30-46.	1.0	293
15	On the Optimization of Side-Channel Attacks by Advanced Stochastic Methods. Lecture Notes in Computer Science, 2005, , 85-103.	1.0	20
16	More Detail for a Combined Timing and Power Attack against Implementations of RSA. Lecture Notes in Computer Science, 2003, , 245-263.	1.0	13
17	OPTIMIZED TIMING ATTACKS AGAINST PUBLIC KEY CRYPTOSYSTEMS. Statistics and Risk Modeling, 2002, 20, .	0.7	9
18	A Combined Timing and Power Attack. Lecture Notes in Computer Science, 2002, , 263-279.	1.0	35

#	Article	IF	Citations
19	Improving Divide and Conquer Attacks against Cryptosystems by Better Error Detection / Correction Strategies. Lecture Notes in Computer Science, 2001, , 245-267.	1.0	19
20	A Timing Attack against RSA with the Chinese Remainder Theorem. Lecture Notes in Computer Science, 2000, , 109-124.	1.0	98