Michael Tunstall

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/5797483/publications.pdf

Version: 2024-02-01

40 papers	927 citations	430754 18 h-index	454834 30 g-index
45 all docs	45 docs citations	45 times ranked	524 citing authors

#	Article	IF	Citations
1	Constant-time higher-order Boolean-to-arithmetic masking. Journal of Cryptographic Engineering, 2019, 9, 173-184.	1.5	10
2	Online template attacks. Journal of Cryptographic Engineering, 2019, 9, 21-36.	1.5	18
3	Smart Card Security. , 2017, , 217-251.		5
4	Key extraction from the primary side of a switched-mode power supply. , 2016, , .		1
5	The distributions of individual bits in the output of multiplicative operations. Cryptography and Communications, 2015, 7, 71-90.	0.9	2
6	Exploiting Collisions in Addition Chain-Based Exponentiation Algorithms Using a Single Trace. Lecture Notes in Computer Science, 2015, , 431-448.	1.0	22
7	Randomizing the Montgomery Powering Ladder. Lecture Notes in Computer Science, 2015, , 169-184.	1.0	7
8	Empirical evaluation of multi-device profiling side-channel attacks. , 2014, , .		4
9	All-or-Nothing Transforms as a countermeasure to differential side-channel analysis. International Journal of Information Security, 2014, 13, 291-304.	2.3	7
10	Online Template Attacks. Lecture Notes in Computer Science, 2014, , 21-36.	1.0	34
11	Masking Tablesâ€”An Underestimated Security Risk. Lecture Notes in Computer Science, 2014, , 425-444.	1.0	22
12	Smart Card Security. , 2014, , 145-177.		0
13	Differential fault analysis of AES: towards reaching its limits. Journal of Cryptographic Engineering, 2013, 3, 73-97.	1.5	41
14	Harnessing Biased Faults in Attacks on ECC-Based Signature Schemes. , 2012, , .		10
15	Compiler Assisted Masking. Lecture Notes in Computer Science, 2012, , 58-75.	1.0	50
16	Infective Computation and Dummy Rounds: Fault Protection for Block Ciphers without Check-before-Output. Lecture Notes in Computer Science, 2012, , 305-321.	1.0	64
17	Using templates to distinguish multiplications from squaring operations. International Journal of Information Security, 2011, 10, 255-266.	2.3	18
18	Practical complexity differential cryptanalysis and fault analysis of AES. Journal of Cryptographic Engineering, 2011, 1, 219-230.	1.5	8

#	Article	IF	Citations
19	Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems. Journal of Cryptographic Engineering, 2011, 1, 271-281.	1.5	25
20	Can Code Polymorphism Limit Information Leakage?. Lecture Notes in Computer Science, 2011, , 1-21.	1.0	5
21	Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault. Lecture Notes in Computer Science, 2011, , 224-233.	1.0	166
22	Improved Fault Analysis of Signature Schemes. Lecture Notes in Computer Science, 2010, , 164-181.	1.0	5
23	Side-Channel Analysis of Cryptographic Software via Early-Terminating Multiplications. Lecture Notes in Computer Science, 2010, , 176-192.	1.0	14
24	Combined Implementation Attack Resistant Exponentiation. Lecture Notes in Computer Science, 2010, , 305-322.	1.0	14
25	Coordinate Blinding over Large Prime Fields. Lecture Notes in Computer Science, 2010, , 443-455.	1.0	6
26	Isolated WDDL. ACM Transactions on Reconfigurable Technology and Systems, 2009, 2, 1-23.	1.9	36
27	Attacking smart card systems: Theory and practice. Information Security Technical Report, 2009, 14, 46-56.	1.3	70
28	Exponent Recoding and Regular Exponentiation Algorithms. Lecture Notes in Computer Science, 2009, , 334-349.	1.0	46
29	Distinguishing Multiplications from Squaring Operations. Lecture Notes in Computer Science, 2009, , 346-360.	1.0	22
30	Unknown Plaintext Template Attacks. Lecture Notes in Computer Science, 2009, , 148-162.	1.0	15
31	Random Order m-ary Exponentiation. Lecture Notes in Computer Science, 2009, , 437-451.	1.0	1
32	Smart Card Security. , 2008, , 195-228.		2
33	Montgomery Multiplication with Redundancy Check. , 2007, , .		2
34	Smart Card Security. Studies in Computational Intelligence, 2007, , 201-233.	0.7	8
35	Efficient Use of Random Delays in Embedded Software. Lecture Notes in Computer Science, 2007, , 27-38.	1.0	25
36	Differential Power Analysis of HMAC Based on SHA-2, and Countermeasures. Lecture Notes in Computer Science, 2007, , 317-332.	1.0	30

#	Article	IF	Citations
37	Montgomery Multiplication with Redundancy Check. , 2007, , .		0
38	Fault Analysis of DPA-Resistant Algorithms. Lecture Notes in Computer Science, 2006, , 223-236.	1.0	23
39	Experimenting with Faults, Lattices and the DSA. Lecture Notes in Computer Science, 2005, , 16-28.	1.0	53
40	Asymmetric Currency Rounding. Lecture Notes in Computer Science, 2001, , 192-201.	1.0	1