Billy Bob Brumley

List of Publications by Year
in descending order

30	537	1478505 6	940533 16
papers	citations	h-index	g-index

32	32	32	255
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Remote Timing Attacks Are Still Practical. Lecture Notes in Computer Science, 2011, , 355-371.	1.3	117
2	Cache-Timing Template Attacks. Lecture Notes in Computer Science, 2009, , 667-684.	1.3	82
3	Port Contention for Fun and Profit. , 2019, , .		67
4	New Results on Instruction Cache Attacks. Lecture Notes in Computer Science, 2010, , 110-124.	1.3	58
5	Amplifying side channels through performance degradation. , 2016, , .		51
6	Fast Point Decompression for Standard Elliptic Curves. , 2008, , 134-149.		24
7	"Make Sure DSA Signing Exponentiations Really are Constant-Time". , 2016, , .		24
8	Conversion Algorithms and Implementations for Koblitz Curve Cryptography. IEEE Transactions on Computers, 2010, 59, 81-92.	3.4	19
9	Cache-Timing Attacks on RSA Key Generation. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 213-242.	0.0	17
10	Consecutive S-box Lookups: A Timing Attack on SNOWÂ3G. Lecture Notes in Computer Science, 2010, , 171-185.	1.3	13
11	Side-Channel Analysis of SM2. , 2018, , .		12
12	Cache Storage Attacks. Lecture Notes in Computer Science, 2015, , 22-34.	1.3	7
13	Faster Software for Fast Endomorphisms. Lecture Notes in Computer Science, 2015, , 127-140.	1.3	6
14	Koblitz Curves and Integer Equivalents of Frobenius Expansions. , 2007, , 126-137.		6
15	Online Template Attacks: Revisited. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 28-59.	0.0	5
16	Memory Tampering Attack on Binary GCD Based Inversion Algorithms. International Journal of Parallel Programming, 2019, 47, 621-640.	1.5	3
17	SoK: Remote Power Analysis. , 2021, , .		3
18	Set It and Forget It! Turnkey ECC for Instant Integration. , 2020, , .		3

#	Article	IF	Citations
19	Differential Properties of Elliptic Curves and Blind Signatures. Lecture Notes in Computer Science, 2007, , 376-389.	1.3	3
20	On Modular Decomposition of Integers. Lecture Notes in Computer Science, 2009, , 386-402.	1.3	2
21	Secure and Fast Implementations of Two Involution Ciphers. Lecture Notes in Computer Science, 2012, , 269-282.	1.3	2
22	Start Your ENGINEs: Dynamically Loadable Contemporary Crypto. , 2019, , .		2
23	Faster 128-EEA3 and 128-EIA3 Software. Lecture Notes in Computer Science, 2015, , 199-208.	1.3	2
24	Left-to-Right Signed-Bit Ï„-Adic Representations of n Integers (Short Paper). Lecture Notes in Computer Science, 2006, , 469-478.	1.3	2
25	Batch Binary Weierstrass. Lecture Notes in Computer Science, 2019, , 364-384.	1.3	2
26	DÃ©jÃ Vu: Side-Channel Analysis of Mozilla's NSS. , 2020, , .		2
27	Bit-Sliced Binary Normal Basis Multiplication. , 2011, , .		1
28	Triggerflow: Regression Testing by Advanced Execution Path Inspection. Lecture Notes in Computer Science, 2019, , 330-350.	1.3	1
29	WHIRLBOB, the Whirlpool Based Variant of STRIBOB. Lecture Notes in Computer Science, 2015, , 106-122.	1.3	1
30	Faster Binary Curve Software: A Case Study. Lecture Notes in Computer Science, 2015, , 91-105.	1.3	0