

Billy Bob Brumley

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/1993036/publications.pdf>

Version: 2024-02-01

30
papers

537
citations

1478505

6
h-index

940533

16
g-index

32
all docs

32
docs citations

32
times ranked

255
citing authors

#	ARTICLE	IF	CITATIONS
1	SoK: Remote Power Analysis. , 2021, , .		3
2	Set It and Forget It! Turnkey ECC for Instant Integration. , 2020, , .		3
3	DÃ©jÃ© Vu: Side-Channel Analysis of Mozilla's NSS. , 2020, , .		2
4	Port Contention for Fun and Profit. , 2019, , .		67
5	Start Your ENGINES: Dynamically Loadable Contemporary Crypto. , 2019, , .		2
6	Memory Tampering Attack on Binary GCD Based Inversion Algorithms. International Journal of Parallel Programming, 2019, 47, 621-640.	1.5	3
7	Triggerflow: Regression Testing by Advanced Execution Path Inspection. Lecture Notes in Computer Science, 2019, , 330-350.	1.3	1
8	Batch Binary Weierstrass. Lecture Notes in Computer Science, 2019, , 364-384.	1.3	2
9	Side-Channel Analysis of SM2. , 2018, , .		12
10	Amplifying side channels through performance degradation. , 2016, , .		51
11	"Make Sure DSA Signing Exponentiations Really are Constant-Time". , 2016, , .		24
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	Faster 128-EEA3 and 128-EIA3 Software. Lecture Notes in Computer Science, 2015, , 199-208.	1.3	2
15	WHIRLBOB, the Whirlpool Based Variant of STRIBOB. Lecture Notes in Computer Science, 2015, , 106-122.	1.3	1
16	Faster Binary Curve Software: A Case Study. Lecture Notes in Computer Science, 2015, , 91-105.	1.3	0
17	Secure and Fast Implementations of Two Involution Ciphers. Lecture Notes in Computer Science, 2012, , 269-282.	1.3	2
18	Bit-Sliced Binary Normal Basis Multiplication. , 2011, , .		1

#	ARTICLE	IF	CITATIONS
19	Remote Timing Attacks Are Still Practical. Lecture Notes in Computer Science, 2011, , 355-371.	1.3	117
20	Conversion Algorithms and Implementations for Koblitz Curve Cryptography. IEEE Transactions on Computers, 2010, 59, 81-92.	3.4	19
21	New Results on Instruction Cache Attacks. Lecture Notes in Computer Science, 2010, , 110-124.	1.3	58
22	Consecutive S-box Lookups: A Timing Attack on SNOW ^{3G} . Lecture Notes in Computer Science, 2010, , 171-185.	1.3	13
23	On Modular Decomposition of Integers. Lecture Notes in Computer Science, 2009, , 386-402.	1.3	2
24	Cache-Timing Template Attacks. Lecture Notes in Computer Science, 2009, , 667-684.	1.3	82
25	Fast Point Decompression for Standard Elliptic Curves. , 2008, , 134-149.		24
26	Koblitz Curves and Integer Equivalents of Frobenius Expansions. , 2007, , 126-137.		6
27	Differential Properties of Elliptic Curves and Blind Signatures. Lecture Notes in Computer Science, 2007, , 376-389.	1.3	3
28	Left-to-Right Signed-Bit \mathbb{F}_q -Adic Representations of n Integers (Short Paper). Lecture Notes in Computer Science, 2006, , 469-478.	1.3	2
29	Online Template Attacks: Revisited. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 28-59.	0.0	5
30	Cache-Timing Attacks on RSA Key Generation. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 213-242.	0.0	17