Jean-Sbastien Coron

List of Publications by Citations

19 papers	675 citations	12 h-index	19 g-index
19 ext. papers	723 ext. citations	1.3 avg, IF	4.27 L-index

#	Paper	IF	Citations
19	Merkle-Damgård Revisited: How to Construct a Hash Function. *Lecture Notes in Computer Science*, **2005**, 430-448	0.9	232
18	Higher Order Masking of Look-Up Tables. *Lecture Notes in Computer Science*, **2014**, 441-458	0.9	77
17	Higher-Order Side Channel Security and Mask Refreshing. *Lecture Notes in Computer Science*, **2014**, 410-424	0.9	65
16	The Random Oracle Model and the Ideal Cipher Model Are Equivalent. *Lecture Notes in Computer Science*, **2008**, 1-20	0.9	56
15	Deterministic Polynomial-Time Equivalence of Computing the RSA Secret Key and Factoring. *Journal of Cryptology*, **2007**, 20, 39-50	2.1	48
14	Finding Small Roots of Bivariate Integer Polynomial Equations Revisited. *Lecture Notes in Computer Science*, **2004**, 492-505	0.9	44
13	How to Build an Ideal Cipher: The Indifferentiability of the Feistel Construction. *Journal of Cryptology*, **2016**, 29, 61-114	2.1	25
12	Finding Small Roots of Bivariate Integer Polynomial Equations: A Direct Approach **2007**, 379-394		25
11	On the Security of RSA Padding. *Lecture Notes in Computer Science*, **1999**, 1-18	0.9	21
10	Security Proof for Partial-Domain Hash Signature Schemes. *Lecture Notes in Computer Science*, **2002** , 613-626	0.9	17
9	A variant of Boneh-Franklin IBE with a tight reduction in the random oracle model. *Designs, Codes, and Cryptography*, **2009**, 50, 115-133	1.2	16
8	New Attacks on PKCS#1 v1.5 Encryption. *Lecture Notes in Computer Science*, **2000**, 369-381	0.9	16
7	Fast evaluation of polynomials over binary finite fields and application to side-channel countermeasures. *Journal of Cryptographic Engineering*, **2015**, 5, 73-83	1.9	11
6	Introduction to the CHES 2013 special issue. *Journal of Cryptographic Engineering*, **2014**, 4, 1-1	1.9	7
5	Cryptanalysis of ISO/IEC 9796-1. *Journal of Cryptology*, **2008**, 21, 27-51	2.1	5
4	Index Calculation Attacks on RSA Signature and Encryption. *Designs, Codes, and Cryptography*, **2006**, 38, 41-53	1.2	5
3	A Note on the Bivariate Coppersmith Theorem. *Journal of Cryptology*, **2013**, 26, 246-250	2.1	3

2	Practical Cryptanalysis of ISO 9796-2 and EMV Signatures. *Journal of Cryptology*, **2016**, 29, 632-656	2.1	1
1	Improved cryptanalysis of the AJPS Mersenne based cryptosystem. *Journal of Mathematical Cryptology*, **2020**, 14, 218-223	0.6	1