# Jean-SÃ©bastien Coron

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/7670194/publications.pdf

Version: 2024-02-01

| | | | |
|---|---|---|---|
| 18<br>papers | 841<br>citations | 858243<br>12<br>h-index | 939365<br>18<br>g-index |
| 19<br>all docs | 19<br>docs citations | 19<br>times ranked | 354<br>citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Improved cryptanalysis of the AJPS Mersenne based cryptosystem. Journal of Mathematical Cryptology, 2020, 14, 218-223. | 0.4 | 2 |
| 2 | How to Build an Ideal Cipher: The Indifferentiability of the Feistel Construction. Journal of Cryptology, 2016, 29, 61-114. | 2.1 | 32 |
| 3 | Practical Cryptanalysis of ISO 9796-2 and EMV Signatures. Journal of Cryptology, 2016, 29, 632-656. | 2.1 | 2 |
| 4 | Fast evaluation of polynomials over binary finite fields and application to side-channel countermeasures. Journal of Cryptographic Engineering, 2015, 5, 73-83. | 1.5 | 13 |
| 5 | Introduction to the CHES 2013 special issue. Journal of Cryptographic Engineering, 2014, 4, 1-1. | 1.5 | 10 |
| 6 | Higher Order Masking of Look-Up Tables. Lecture Notes in Computer Science, 2014, , 441-458. | 1.0 | 98 |
| 7 | Higher-Order Side Channel Security and Mask Refreshing. Lecture Notes in Computer Science, 2014, , 410-424. | 1.0 | 83 |
| 8 | A Note on the Bivariate Coppersmith Theorem. Journal of Cryptology, 2013, 26, 246-250. | 2.1 | 3 |
| 9 | A variant of Boneh-Franklin IBE with a tight reduction in the random oracle model. Designs, Codes, and Cryptography, 2009, 50, 115-133. | 1.0 | 19 |
| 10 | Cryptanalysis of ISO/IEC 9796-1. Journal of Cryptology, 2008, 21, 27-51. | 2.1 | 8 |
| 11 | The Random Oracle Model and the Ideal Cipher Model Are Equivalent. Lecture Notes in Computer Science, 2008, , 1-20. | 1.0 | 64 |
| 12 | Deterministic Polynomial-Time Equivalence of Computing the RSA Secret Key and Factoring. Journal of Cryptology, 2007, 20, 39-50. | 2.1 | 60 |
| 13 | Finding Small Roots of Bivariate Integer Polynomial Equations: A Direct Approach. , 2007, , 379-394. |  | 30 |
| 14 | Index Calculation Attacks on RSA Signature and Encryption. Designs, Codes, and Cryptography, 2006, 38, 41-53. | 1.0 | 6 |
| 15 | Merkle-DamgÃ¥rd Revisited: How to Construct a Hash Function. Lecture Notes in Computer Science, 2005, , 430-448. | 1.0 | 290 |
| 16 | Finding Small Roots of Bivariate Integer Polynomial Equations Revisited. Lecture Notes in Computer Science, 2004, , 492-505. | 1.0 | 52 |
| 17 | Security Proof for Partial-Domain Hash Signature Schemes. Lecture Notes in Computer Science, 2002, , 613-626. | 1.0 | 17 |
| 18 | On the Security of RSA Padding. Lecture Notes in Computer Science, 1999, , 1-18. | 1.0 | 34 |