# Jean-Claude Bajard

List of Publications by Year
in descending order



| 39 | 858 | 759055 | 677027 |
|---|---|---|---|
| papers | citations | 12 h-index | 22 g-index |

| 41 | 41 | 41 | 376 |
|---|---|---|---|
| all docs | docs citations | times ranked | citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | a full RNS implementation of RSA. IEEE Transactions on Computers, 2004, 53, 769-774. | 2.4 | 183 |
| 2 | An RNS Montgomery modular multiplication algorithm. IEEE Transactions on Computers, 1998, 47, 766-776. | 2.4 | 104 |
| 3 | A Full RNS Variant of FV Like Somewhat Homomorphic Encryption Schemes. Lecture Notes in Computer Science, 2017, , 423-442. | 1.0 | 76 |
| 4 | Leak Resistant Arithmetic. Lecture Notes in Computer Science, 2004, , 62-75. | 1.0 | 50 |
| 5 | RNS-Based Elliptic Curve Point Multiplication for Massive Parallel Architectures. Computer Journal, 2012, 55, 629-647. | 1.5 | 49 |
| 6 | A New Security Model for Authenticated Key Agreement. Lecture Notes in Computer Science, 2010, , 219-234. | 1.0 | 49 |
| 7 | An Algorithmic and Architectural Study on Montgomery Exponentiation in RNS. IEEE Transactions on Computers, 2012, 61, 1071-1083. | 2.4 | 36 |
| 8 | A Secure and Efficient Authenticated Diffieâ€“Hellman Protocol. Lecture Notes in Computer Science, 2010, , 83-98. | 1.0 | 35 |
| 9 | BKM: a new hardware algorithm for complex elementary functions. IEEE Transactions on Computers, 1994, 43, 955-963. | 2.4 | 31 |
| 10 | Elliptic Curve point multiplication on GPUs. , 2010, , . | | 30 |
| 11 | Some Operators for On-Line Radix-2 Computations. Journal of Parallel and Distributed Computing, 1994, 22, 336-345. | 2.7 | 27 |
| 12 | Arithmetic Operations in Finite Fields of Medium Prime Characteristic Using the Lagrange Representation. IEEE Transactions on Computers, 2006, 55, 1167-1177. | 2.4 | 20 |
| 13 | Montgomery reduction within the context of residue number system arithmetic. Journal of Cryptographic Engineering, 2018, 8, 189-200. | 1.5 | 18 |
| 14 | A General Approach for Improving RNS Montgomery Exponentiation Using Pre-processing. , 2011, , . | | 17 |
| 15 | Fault Detection in RNS Montgomery Modular Multiplication. , 2013, , . | | 14 |
| 16 | Improving the Efficiency of SVM Classification With FHE. IEEE Transactions on Information Forensics and Security, 2020, 15, 1709-1722. | 4.5 | 13 |
| 17 | RNS Arithmetic Approach in Lattice-Based Cryptography: Accelerating the "Rounding-off" Core Procedure. , 2015, , . | | 11 |
| 18 | Multi-fault Attack Detection for RNS Cryptographic Architecture. , 2016, , . | | 11 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | Double Level Montgomery Cox-Rower Architecture, New Bounds. Lecture Notes in Computer Science, 2015, , 139-153. | 1.0 | 11 |
| 20 | RNS bases and conversions. , 2004, , . | | 10 |
| 21 | Direct Effect in DNA Radiolysis. Boron Neutron Capture Enhancement of Radiolysis in a Medical Fast-Neutron Beam. Radiation Research, 2002, 158, 292-301. | 0.7 | 9 |
| 22 | Programmable RNS lattice-based parallel cryptographic decryption. , 2015, , . | | 8 |
| 23 | Resilience of Randomized RNS Arithmetic with Respect to Side-Channel Leaks of Cryptographic Computation. IEEE Transactions on Computers, 2019, 68, 1720-1730. | 2.4 | 8 |
| 24 | Babaï round-off CVP method in RNS: Application to lattice based cryptographic protocols. , 2014, , . | | 6 |
| 25 | Montgomery-friendly primes and applications to cryptography. Journal of Cryptographic Engineering, 2021, 11, 399-415. | 1.5 | 6 |
| 26 | Study of modular inversion in RNS. , 2005, 5910, 247. | | 4 |
| 27 | ρ-Direct Form transposed and Residue Number Systems for Filter implementations. , 2011, , . | | 4 |
| 28 | Arithmetical Improvement of the Round-Off for Cryptosystems in High-Dimensional Lattices. IEEE Transactions on Computers, 2017, 66, 2005-2018. | 2.4 | 4 |
| 29 | A Leak Resistant Architecture Against Side Channel Attacks. , 2006, , . | | 2 |
| 30 | Subquadratic Space Complexity Binary Field Multiplier Using Double Polynomial Representation. IEEE Transactions on Computers, 2010, 59, 1585-1597. | 2.4 | 2 |
| 31 | HyPoRes: An Hybrid Representation System for ECC. , 2019, , . | | 2 |
| 32 | Efficient Reductions in Cyclotomic Rings - Application to Ring-LWE Based FHE Schemes. Lecture Notes in Computer Science, 2018, , 151-171. | 1.0 | 2 |
| 33 | Generating Residue Number System Bases. , 2021, , . | | 2 |
| 34 | <title>Some improvements on RNS Montgomery modular multiplication</title>. , 2000, 4116, 214. | | 1 |
| 35 | A Residue Approach of the Finite Fields Arithmetics. Conference Record of the Asilomar Conference on Signals, Systems and Computers, 2007, , . | 0.0 | 1 |
| 36 | Pseudo-random generator based on Chinese Remainder Theorem. , 2009, , . | | 1 |

| # | Article | IF | Citations |
|---|---|---|---|
| 37 | On Polynomial Modular Number Systems over $ mathbb{Z}/{p}mathbb{Z} $. Advances in Mathematics of Communications, 2022, . | 0.4 | 1 |
| 38 | Floating-point geometry: toward guaranteed geometric computations with approximate arithmetics. , 2008, , . | | 0 |
| 39 | RNS Approach in Lattice-Based Cryptography. , 2017, , 345-368. | | 0 |