# Edoardo Persichetti

List of Publications by Year
in descending order



| 26 | 291 | 933447 10 | 940533 16 |
|---|---|---|---|
| papers | citations | h-index | g-index |

| 29 | 29 | 29 | 129 |
|---|---|---|---|
| all docs | docs citations | times ranked | citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | On the hardness of the Lee syndrome decoding problem. Advances in Mathematics of Communications, 2024, 18, 233-266. | 0.7 | 8 |
| 2 | Designing a Practical Code-Based Signature Scheme from Zero-Knowledge Proofs with Trusted Setup. Cryptography, 2022, 6, 5. | 2.3 | 14 |
| 3 | Advanced signature functionalities from the code equivalence problem. International Journal of Computer Mathematics: Computer Systems Theory, 2022, 7, 112-128. | 1.1 | 8 |
| 4 | Reproducible families of codes and cryptographic applications. Journal of Mathematical Cryptology, 2021, 16, 20-48. | 0.7 | 4 |
| 5 | LESS-FM: Fine-Tuning Signatures from the Code Equivalence Problem. Lecture Notes in Computer Science, 2021, , 23-43. | 1.3 | 24 |
| 6 | On the applicability of the Fujisakiâ€“Okamoto transformation to the BIKE KEM. International Journal of Computer Mathematics: Computer Systems Theory, 2021, 6, 364-374. | 1.1 | 4 |
| 7 | Cryptanalysis of a code-based full-time signature. Designs, Codes, and Cryptography, 2021, 89, 2097-2112. | 1.6 | 2 |
| 8 | Cryptanalysis of a Code-Based Signature Scheme Based on the Schnorr-Lyubashevsky Framework. IEEE Communications Letters, 2021, 25, 2829-2833. | 4.1 | 1 |
| 9 | LESS is More: Code-Based Signatures Without Syndromes. Lecture Notes in Computer Science, 2020, , 45-65. | 1.3 | 25 |
| 10 | Designing Efficient Dyadic Operations for Cryptographic Applications. Journal of Mathematical Cryptology, 2020, 14, 95-109. | 0.7 | 3 |
| 11 | DAGS: Reloaded Revisiting Dyadic Key Encapsulation. Lecture Notes in Computer Science, 2019, , 69-85. | 1.3 | 3 |
| 12 | From Key Encapsulation to Authenticated Group Key Establishmentâ€”A Compiler for Post-Quantum Primitives â€. Entropy, 2019, 21, 1183. | 2.2 | 6 |
| 13 | A Reaction Attack Against Cryptosystems Based on LRPC Codes. Lecture Notes in Computer Science, 2019, , 197-216. | 1.3 | 11 |
| 14 | Tighter Proofs of CCA Security in the Quantum Random Oracle Model. Lecture Notes in Computer Science, 2019, , 61-90. | 1.3 | 40 |
| 15 | Efficient One-Time Signatures from Quasi-Cyclic Codes: A Full Treatment. Cryptography, 2018, 2, 30. | 2.3 | 17 |
| 16 | On the Performance and Security of Multiplication in GF(2N). Cryptography, 2018, 2, 25. | 2.3 | 5 |
| 17 | DAGS: Key encapsulation using dyadic GS codes. Journal of Mathematical Cryptology, 2018, 12, 221-239. | 0.7 | 18 |
| 18 | On the CCA2 Security of McEliece in the Standard Model. Lecture Notes in Computer Science, 2018, , 165-181. | 1.3 | 4 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | Efficient Implementation of Hybrid Encryption from Coding Theory. Lecture Notes in Computer Science, 2017, , 254-264. | 1.3 | 3 |
| 20 | CAKE: Code-Based Algorithm for Key Encapsulation. Lecture Notes in Computer Science, 2017, , 207-226. | 1.3 | 13 |
| 21 | On lower bounds for information set decoding over 𝔽<SUB align="right">q and on the effect of partial knowledge. International Journal of Information and Coding Theory, 2017, 4, 47. | 0.3 | 8 |
| 22 | On lower bounds for information set decoding over 𝔽<SUB align="right">q and on the effect of partial knowledge. International Journal of Information and Coding Theory, 2017, 4, 47. | 0.3 | 0 |
| 23 | Leakage-Resilient Cryptography over Large Finite Fields: Theory and Practice. Lecture Notes in Computer Science, 2015, , 655-674. | 1.3 | 2 |
| 24 | Secure and Anonymous Hybrid Encryption from Coding Theory. Lecture Notes in Computer Science, 2013, , 174-187. | 1.3 | 17 |
| 25 | Efficient Implementation of a CCA2-Secure Variant of McEliece Using Generalized Srivastava Codes. Lecture Notes in Computer Science, 2012, , 138-155. | 1.3 | 18 |
| 26 | Compact McEliece keys based on quasi-dyadic Srivastava codes. Journal of Mathematical Cryptology, 2012, 6, . | 0.7 | 30 |