Mehdi Tibouchi

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/3705708/publications.pdf

Version: 2024-02-01

79 papers	2,083 citations	346980 22 h-index	274796 44 g-index
81 all docs	81 docs citations	81 times ranked	762 citing authors

#	Article	IF	Citations
1	Security notions for stateful signature schemes. IET Information Security, 2022, 16, 1.	1.1	0
2	On subset-resilient hash function families. Designs, Codes, and Cryptography, 2022, 90, 719-758.	1.0	1
3	Two-Round n-out-of-n and Multi-Signatures and Trapdoor Commitment from Lattices. Journal of Cryptology, 2022, 35, .	2.1	10
4	Mitaka: A Simpler, Parallelizable, Maskable Variant ofÂFalcon. Lecture Notes in Computer Science, 2022, , 222-253.	1.0	18
5	Two-Round n-out-of-n and Multi-signatures and Trapdoor Commitment from Lattices. Lecture Notes in Computer Science, 2021, , 99-130.	1.0	15
6	On the Impossibility of NIZKs for Disjunctive Languages From Commit-and-Prove NIZKs. IEEE Access, 2021, 9, 51368-51379.	2.6	1
7	LadderLeak: Breaking ECDSA with Less than One Bit of Nonce Leakage. , 2020, , .		34
8	Multiparty Non-Interactive Key Exchange and More From Isogenies on Elliptic Curves. Journal of Mathematical Cryptology, 2020, 14, 5-14.	0.4	9
9	Recovering Secrets From Prefix-Dependent Leakage. Journal of Mathematical Cryptology, 2020, 14, 15-24.	0.4	0
10	Equidistribution Among Cosets of Elliptic Curve Points in Intervals. Journal of Mathematical Cryptology, 2020, 14, 339-345.	0.4	0
11	Close to Uniform Prime Number Generation With Fewer Random Bits. IEEE Transactions on Information Theory, 2019, 65, 1307-1317.	1.5	4
12	GALACTICS. , 2019, , .		30
13	Efficient Fully Structure-Preserving Signatures and Shrinking Commitments. Journal of Cryptology, 2019, 32, 973-1025.	2.1	2
14	Masking the GLP Lattice-Based Signature Scheme at Any Order. Lecture Notes in Computer Science, 2018, , 354-384.	1.0	31
15	Constructing Permutation Rational Functions from Isogenies. SIAM Journal on Discrete Mathematics, 2018, 32, 1741-1749.	0.4	1
16	Lower Bounds on Structure-Preserving Signatures for Bilateral Messages. Lecture Notes in Computer Science, 2018, , 3-22.	1.0	5
17	FHE over the integers and modular arithmetic circuits. IET Information Security, 2018, 12, 257-264.	1.1	1
18	Loop-Abort Faults on Lattice-Based Signatures and Key Exchange Protocols. IEEE Transactions on Computers, 2018, , 1-1.	2.4	11

#	Article	IF	Citations
19	Degenerate curve attacks: extending invalid curve attacks to Edwards curves and other models. IET Information Security, 2018, 12, 217-225.	1.1	5
20	Cryptanalysis of Compact-LWE. Lecture Notes in Computer Science, 2018, , 80-97.	1.0	3
21	LWE Without Modular Reduction and Improved Side-Channel Attacks Against BLISS. Lecture Notes in Computer Science, 2018, , 494-524.	1.0	23
22	Improved elliptic curve hashing and point representation. Designs, Codes, and Cryptography, 2017, 82, 161-177.	1.0	11
23	Zeroizing Attacks on Indistinguishability Obfuscation over CLT13. Lecture Notes in Computer Science, 2017, , 41-58.	1.0	33
24	Secure GLS Recomposition for Sum-of-Square Cofactors. Lecture Notes in Computer Science, 2017, , 349-365.	1.0	0
25	Stronglyâ€optimal structure preserving signatures from Type II pairings: synthesis and lower bounds. IET Information Security, 2016, 10, 358-371.	1.1	1
26	FHE Over the Integers and Modular Arithmetic Circuits. Lecture Notes in Computer Science, 2016, , 435-450.	1.0	2
27	Side-Channel Analysis of Weierstrass and Koblitz Curve ECDSA on Android Smartphones. Lecture Notes in Computer Science, 2016, , 236-252.	1.0	23
28	Tightly Secure Signatures From Lossy Identification Schemes. Journal of Cryptology, 2016, 29, 597-631.	2.1	22
29	Practical Cryptanalysis of ISO 9796-2 and EMV Signatures. Journal of Cryptology, 2016, 29, 632-656.	2.1	2
30	Degenerate Curve Attacks. Lecture Notes in Computer Science, 2016, , 19-35.	1.0	3
31	Cryptanalysis of GGH15 Multilinear Maps. Lecture Notes in Computer Science, 2016, , 607-628.	1.0	50
32	Fully Structure-Preserving Signatures and Shrinking Commitments. Lecture Notes in Computer Science, 2015, , 35-65.	1.0	15
33	Invalid Curve Attacks in a GLS Setting. Lecture Notes in Computer Science, 2015, , 41-55.	1.0	7
34	Strongly-Optimal Structure Preserving Signatures from TypeÂII Pairings: Synthesis and Lower Bounds. Lecture Notes in Computer Science, 2015, , 355-376.	1.0	25
35	Zeroizing Without Low-Level Zeroes: New MMAP Attacks and their Limitations. Lecture Notes in Computer Science, 2015, , 247-266.	1.0	92
36	New Multilinear Maps Over the Integers. Lecture Notes in Computer Science, 2015, , 267-286.	1.0	73

#	Article	IF	Citations
37	Cryptanalysis of the Co-ACD Assumption. Lecture Notes in Computer Science, 2015, , 561-580.	1.0	3
38	Cryptanalysis of a (Somewhat) Additively Homomorphic Encryption Scheme Used in PIR. Lecture Notes in Computer Science, 2015, , 184-193.	1.0	10
39	Conversion from Arithmetic to Boolean Masking with Logarithmic Complexity. Lecture Notes in Computer Science, 2015, , 130-149.	1.0	27
40	Bit-Flip Faults on Elliptic Curve Base Fields, Revisited. Lecture Notes in Computer Science, 2014, , 163-180.	1.0	6
41	Impossibility of Surjective Icart-Like Encodings. Lecture Notes in Computer Science, 2014, , 29-39.	1.0	5
42	Binary Elligator Squared. Lecture Notes in Computer Science, 2014, , 20-37.	1.0	12
43	Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures. Lecture Notes in Computer Science, 2014, , 688-712.	1.0	38
44	Scale-Invariant Fully Homomorphic Encryption over the Integers. Lecture Notes in Computer Science, 2014, , 311-328.	1.0	99
45	Structure-Preserving Signatures from Type II Pairings. Lecture Notes in Computer Science, 2014, , 390-407.	1.0	24
46	Making RSAâ€"PSS Provably Secure against Non-random Faults. Lecture Notes in Computer Science, 2014, , 206-222.	1.0	11
47	Elligator Squared: Uniform Points on Elliptic Curves of Prime Order as Uniform Random Strings. Lecture Notes in Computer Science, 2014, , 139-156.	1.0	22
48	GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA Signatures with Single-Bit Nonce Bias. Lecture Notes in Computer Science, 2014, , 262-281.	1.0	21
49	Close to Uniform Prime Number Generation with Fewer Random Bits. Lecture Notes in Computer Science, 2014, , 991-1002.	1.0	8
50	Attacking RSAâ€"CRT signatures with faults on montgomery multiplication. Journal of Cryptographic Engineering, 2013, 3, 59-72.	1.5	9
51	A Note on the Bivariate Coppersmith Theorem. Journal of Cryptology, 2013, 26, 246-250.	2.1	3
52	Injective Encodings to Elliptic Curves. Lecture Notes in Computer Science, 2013, , 203-218.	1.0	24
53	Batch Fully Homomorphic Encryption over the Integers. Lecture Notes in Computer Science, 2013, , 315-335.	1.0	189
54	Fault Attacks on Projective-to-Affine Coordinates Conversion. Lecture Notes in Computer Science, 2013, , 46-61.	1.0	4

#	Article	IF	Citations
55	Practical Multilinear Maps over the Integers. Lecture Notes in Computer Science, 2013, , 476-493.	1.0	260
56	Recovering Private Keys Generated with Weak PRNGs. Lecture Notes in Computer Science, 2013, , 158-172.	1.0	5
57	Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. Mathematics of Computation, 2012, 82, 491-512.	1.1	33
58	Indifferentiable Hashing to Barretoâ€"Naehrig Curves. Lecture Notes in Computer Science, 2012, , 1-17.	1.0	18
59	Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers. Lecture Notes in Computer Science, 2012, , 446-464.	1.0	135
60	Tightly-Secure Signatures from Lossy Identification Schemes. Lecture Notes in Computer Science, 2012, , 572-590.	1.0	58
61	Lattice-Based Fault Attacks on Signatures. Information Security and Cryptography, 2012, , 201-220.	0.2	10
62	Attacking RSAâ€"CRT Signatures with Faults on Montgomery Multiplication. Lecture Notes in Computer Science, 2012, , 447-462.	1.0	9
63	A Nagell Algorithm in Any Characteristic. Lecture Notes in Computer Science, 2012, , 474-479.	1.0	0
64	Securing E-passports with Elliptic Curves. IEEE Security and Privacy, 2011, 9, 75-78.	1.5	5
65	Fully Homomorphic Encryption over the Integers with Shorter Public Keys. Lecture Notes in Computer Science, 2011, , 487-504.	1.0	242
66	Modulus fault attacks against RSAâ€"CRT signatures. Journal of Cryptographic Engineering, 2011, 1, 243-253.	1.5	5
67	Cryptanalysis of the RSA Subgroup Assumption from TCC 2005. Lecture Notes in Computer Science, 2011, , 147-155.	1.0	15
68	Modulus Fault Attacks against RSA-CRT Signatures. Lecture Notes in Computer Science, 2011, , 192-206.	1.0	10
69	ISO-9796 Signature Standards. , 2011, , 649-650.		0
70	Security Reduction. , 2011, , 1167-1168.		0
71	Huffâ€™s Model for Elliptic Curves. Lecture Notes in Computer Science, 2010, , 234-250.	1.0	39
72	Estimating the Size of the Image of Deterministic Hash Functions to Elliptic Curves. Lecture Notes in Computer Science, 2010, , 81-91.	1.0	19

#	Article	IF	Citations
73	Deterministic Encoding and Hashing to Odd Hyperelliptic Curves. Lecture Notes in Computer Science, 2010, , 265-277.	1.0	19
74	Efficient Indifferentiable Hashing into Ordinary Elliptic Curves. Lecture Notes in Computer Science, 2010, , 237-254.	1.0	68
75	Fault Attacks Against emv Signatures. Lecture Notes in Computer Science, 2010, , 208-220.	1.0	24
76	On the Broadcast and Validity-Checking Security of pkcs#1 v1.5 Encryption. Lecture Notes in Computer Science, 2010, , 1-18.	1.0	7
77	Factoring Unbalanced Moduli with Known Bits. Lecture Notes in Computer Science, 2010, , 65-72.	1.0	0
78	Practical Cryptanalysis of iso/iec 9796-2 and emv Signatures. Lecture Notes in Computer Science, 2009, , 428-444.	1.0	11
79	Elliptic Curve Multiset Hash. Computer Journal, 0, , .	1.5	5