Daniele Venturi

List of Publications by Year
in descending order

63	1,230	566801 15	500791 28
papers	citations	h-index	g-index

65	65	65	482
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	The Mother of All Leakages: How to Simulate Noisy Leakages via Bounded Leakage (Almost) for Free. Lecture Notes in Computer Science, 2021, , 408-437.	1.0	1
2	Continuously Non-malleable Secret Sharing: Joint Tampering, Plain Model and Capacity. Lecture Notes in Computer Science, 2021, , 333-364.	1.0	3
3	Identity-Based Matchmaking Encryption Without Random Oracles. Lecture Notes in Computer Science, 2021, , 415-435.	1.0	15
4	Non-malleable Encryption: Simpler, Shorter, Stronger. Journal of Cryptology, 2020, 33, 1984-2033.	2.1	1
5	Continuously Non-malleable Codes in the Split-State Model. Journal of Cryptology, 2020, 33, 2034-2077.	2.1	2
6	Subversion-resilient signatures: Definitions, constructions and applications. Theoretical Computer Science, 2020, 820, 91-122.	0.5	7
7	Non-malleable Secret Sharing Against Bounded Joint-Tampering Attacks in the Plain Model. Lecture Notes in Computer Science, 2020, , 127-155.	1.0	11
8	On Adaptive Security of Delayed-Input Sigma Protocols and Fiat-Shamir NIZKs. Lecture Notes in Computer Science, 2020, , 670-690.	1.0	13
9	Affordable Security or Big Guy vs Small Guy. Lecture Notes in Computer Science, 2020, , 135-147.	1.0	0
10	Public Immunization Against Complete Subversion Without Random Oracles. Lecture Notes in Computer Science, 2019, , 465-485.	1.0	7
11	Continuously non-malleable codes with split-state refresh. Theoretical Computer Science, 2019, 759, 98-132.	0.5	3
12	Rate-Optimizing Compilers for Continuously Non-malleable Codes. Lecture Notes in Computer Science, 2019, , 3-23.	1.0	8
13	Non-malleable Secret Sharing in the Computational Setting: Adaptive Tampering, Noisy-Leakage Resilience, and Improved Rate. Lecture Notes in Computer Science, 2019, , 448-479.	1.0	11
14	A Black-Box Construction of Fully-Simulatable, Round-Optimal Oblivious Transfer from Strongly Uniform Key Agreement. Lecture Notes in Computer Science, 2019, , 111-130.	1.0	12
15	Continuously Non-malleable Secret Sharing for General Access Structures. Lecture Notes in Computer Science, 2019, , 211-232.	1.0	10
16	Match Me if You Can: Matchmaking Encryption and Its Applications. Lecture Notes in Computer Science, 2019, , 701-731.	1.0	27
17	Outsourced pattern matching. International Journal of Information Security, 2018, 17, 327-346.	2.3	6
18	Continuously Non-malleable Codes with Split-State Refresh. Lecture Notes in Computer Science, 2018, , 121-139.	1.0	14

#	Article	IF	Citations
19	FuturesMEX: Secure, Distributed Futures Market Exchange. , 2018, , .		21
20	Continuously Non-Malleable Codes in the Split-State Model from Minimal Assumptions. Lecture Notes in Computer Science, 2018, , 608-639.	1.0	18
21	Fiatâ€“Shamir for highly sound protocols is instantiable. Theoretical Computer Science, 2018, 740, 28-62.	0.5	1
22	Secure Outsourcing of Cryptographic Circuits Manufacturing. Lecture Notes in Computer Science, 2018, , 75-93.	1.0	5
23	Bounded Tamper Resilience: How to Go Beyond the Algebraic Barrier. Journal of Cryptology, 2017, 30, 152-190.	2.1	6
24	Fully leakage-resilient signatures revisited: Graceful degradation, noisy leakage, and construction in the bounded-retrieval model. Theoretical Computer Science, 2017, 660, 23-56.	0.5	6
25	Non-Malleable Codes for Space-Bounded Tampering. Lecture Notes in Computer Science, 2017, , 95-126.	1.0	18
26	Naorâ€“Yung paradigm with shared randomness and applications. Theoretical Computer Science, 2017, 692, 90-113.	0.5	1
27	Efficient Authentication from Hard Learning Problems. Journal of Cryptology, 2017, 30, 1238-1275.	2.1	7
28	Redactable Blockchain â€“ or â€“ Rewriting History in Bitcoin and Friends. , 2017, , .		214
29	Securing Underwater Communications. , 2017, , .		8
30	The Seconomics (Security-Economics) Vulnerabilities of Decentralized Autonomous Organizations. Lecture Notes in Computer Science, 2017, , 171-179.	1.0	11
31	Predictable Arguments of Knowledge. Lecture Notes in Computer Science, 2017, , 121-150.	1.0	14
32	Efficient Non-Malleable Codes and Key Derivation for Poly-Size Tampering Circuits. IEEE Transactions on Information Theory, 2016, 62, 7179-7194.	1.5	8
33	Rate-limited secure function evaluation. Theoretical Computer Science, 2016, 653, 53-78.	0.5	0
34	Naor-Yung Paradigm with Shared Randomness and Applications. Lecture Notes in Computer Science, 2016, , 62-80.	1.0	3
35	Entangled cloud storage. Future Generation Computer Systems, 2016, 62, 104-118.	4.9	13
36	Fiatâ€“Shamir for Highly Sound Protocols Is Instantiable. Lecture Notes in Computer Science, 2016, , 198-215.	1.0	8

#	Article	IF	Citations
37	Non-Malleable Encryption: Simpler, Shorter, Stronger. Lecture Notes in Computer Science, 2016, , 306-335.	1.0	32
38	Chosen-Ciphertext Security from Subset Sum. Lecture Notes in Computer Science, 2016, , 35-46.	1.0	5
39	Efficient Public-Key Cryptography with Bounded Leakage and Tamper Resilience. Lecture Notes in Computer Science, 2016, , 877-907.	1.0	14
40	Subversion-Resilient Signature Schemes. , 2015, , .		64
41	Secure Data Sharing and Processing in Heterogeneous Clouds. Procedia Computer Science, 2015, 68, 116-126.	1.2	13
42	(De-)Constructing TLS 1.3. Lecture Notes in Computer Science, 2015, , 85-102.	1.0	21
43	Entangled Encodings and Data Entanglement. , 2015, , .		3
44	The Chaining Lemma and Its Application. Lecture Notes in Computer Science, 2015, , 181-196.	1.0	11
45	A Multi-Party Protocol for Privacy-Preserving Cooperative Linear Systems of Equations. Lecture Notes in Computer Science, 2015, , 161-172.	1.0	6
46	A Tamper and Leakage Resilient von Neumann Architecture. Lecture Notes in Computer Science, 2015, , 579-603.	1.0	22
47	From Single-Bit to Multi-bit Public-Key Encryption via Non-malleable Codes. Lecture Notes in Computer Science, 2015, , 532-560.	1.0	42
48	Mind Your Coins: Fully Leakage-Resilient Signatures with Graceful Degradation. Lecture Notes in Computer Science, 2015, , 456-468.	1.0	12
49	Efficient Non-malleable Codes and Key-Derivation for Poly-size Tampering Circuits. Lecture Notes in Computer Science, 2014, , 111-128.	1.0	61
50	A Second Look at Fischlinâ€™s Transformation. Lecture Notes in Computer Science, 2014, , 356-376.	1.0	7
51	Continuous Non-malleable Codes. Lecture Notes in Computer Science, 2014, , 465-488.	1.0	84
52	Leakage-Resilient Signatures with Graceful Degradation. Lecture Notes in Computer Science, 2014, , 362-379.	1.0	13
53	Outsourced Pattern Matching. Lecture Notes in Computer Science, 2013, , 545-556.	1.0	23
54	On the Connection between Leakage Tolerance and Adaptive Security. Lecture Notes in Computer Science, 2013, , 497-515.	1.0	8

#	Article	IF	Citations
55	Rate-Limited Secure Function Evaluation: Definitions and Constructions. Lecture Notes in Computer Science, 2013, , 461-478.	1.0	5
56	Bounded Tamper Resilience: How to Go beyond the Algebraic Barrier. Lecture Notes in Computer Science, 2013, , 140-160.	1.0	39
57	Anonymity-Preserving Public-Key Encryption: A Constructive Approach. Lecture Notes in Computer Science, 2013, , 19-39.	1.0	10
58	On the Non-malleability of the Fiat-Shamir Transform. Lecture Notes in Computer Science, 2012, , 60-79.	1.0	70
59	Reticoli e crittografia. Unitext, 2012, , 235-255.	0.0	0
60	â€žScambi di manoâ€œ sicuri. Unitext, 2012, , 281-323.	0.0	0
61	Efficient Authentication from Hard Learning Problems. Lecture Notes in Computer Science, 2011, , 7-26.	1.0	63
62	Tamper-Proof Circuits: How to Trade Leakage for Tamper-Resilience. Lecture Notes in Computer Science, 2011, , 391-402.	1.0	25
63	Leakage-Resilient Storage. Lecture Notes in Computer Science, 2010, , 121-137.	1.0	60