Dario Catalano

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/10822091/publications.pdf

Version: 2024-02-01

		586496	685536
27	1,451	16	24
papers	citations	h-index	g-index
27	27	27	781
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Homomorphic signatures with sublinear public keys via asymmetric programmable hash functions. Designs, Codes, and Cryptography, 2018, 86, 2197-2246.	1.0	2
2	Practical Homomorphic Message Authenticators for Arithmetic Circuits. Journal of Cryptology, 2018, 31, 23-59.	2.1	15
3	On the Security Notions for Homomorphic Signatures. Lecture Notes in Computer Science, 2018, , 183-201.	1.0	5
4	A certificateless approach to onion routing. International Journal of Information Security, 2017, 16, 327-343.	2.3	6
5	Algebraic (trapdoor) one-way functions: Constructions and applications. Theoretical Computer Science, 2015, 592, 143-165.	0.5	4
6	Programmable Hash Functions Go Private: Constructions and Applications to (Homomorphic) Signatures with Shorter Public Keys. Lecture Notes in Computer Science, 2015, , 254-274.	1.0	26
7	Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions. Journal of Cryptology, 2014, 27, 544-593.	2.1	25
8	Generalizing Homomorphic MACs for Arithmetic Circuits. Lecture Notes in Computer Science, 2014, , 538-555.	1.0	26
9	Homomorphic Signatures with Efficient Verification for Polynomial Functions. Lecture Notes in Computer Science, 2014, , 371-389.	1.0	72
10	Off-line/on-line signatures revisited: a general unifying paradigm, efficient threshold variants and experimental results. International Journal of Information Security, 2013, 12, 439-465.	2.3	1
11	Fully non-interactive onion routing with forward secrecy. International Journal of Information Security, 2013, 12, 33-47.	2.3	4
12	Algebraic (Trapdoor) One-Way Functions and Their Applications. Lecture Notes in Computer Science, 2013, , 680-699.	1.0	40
13	Vector Commitments and Their Applications. Lecture Notes in Computer Science, 2013, , 55-72.	1.0	167
14	Practical Homomorphic MACs for Arithmetic Circuits. Lecture Notes in Computer Science, 2013, , 336-352.	1.0	60
15	Efficient Network Coding Signatures in the Standard Model. Lecture Notes in Computer Science, 2012, , 680-696.	1.0	71
16	Zero-Knowledge Sets With Short Proofs. IEEE Transactions on Information Theory, 2011, 57, 2488-2502.	1.5	10
17	Wildcarded Identity-Based Encryption. Journal of Cryptology, 2011, 24, 42-82.	2.1	25
18	Adaptive Pseudo-free Groups and Applications. Lecture Notes in Computer Science, 2011, , 207-223.	1.0	46

#	Article	IF	Citations
19	Certificateless onion routing. , 2009, , .		22
20	Verifiable Random Functions from Identity-Based Key Encapsulation. Lecture Notes in Computer Science, 2009, , 554-571.	1.0	30
21	Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. Journal of Cryptology, 2008, 21, 350-391.	2.1	247
22	Off-Line/On-Line Signatures: Theoretical Aspects and Experimental Results. Lecture Notes in Computer Science, 2008, , 101-120.	1.0	26
23	Zero-Knowledge Sets with Short Proofs. , 2008, , 433-450.		38
24	Improved On-Line/Off-Line Threshold Signatures. , 2007, , 217-232.		21
25	Mercurial Commitments: Minimal Assumptions and Efficient Constructions. Lecture Notes in Computer Science, 2006, , 120-144.	1.0	29
26	Identity-Based Encryption Gone Wild. Lecture Notes in Computer Science, 2006, , 300-311.	1.0	76
27	Searchable Encryption Revisited:ÂConsistency Properties, Relation to Anonymous IBE, and Extensions. Lecture Notes in Computer Science, 2005, , 205-222.	1.0	357