

Elena Pagnin

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/6130303/publications.pdf>

Version: 2024-02-01

21
papers

168
citations

1307594

7
h-index

1125743

13
g-index

21
all docs

21
docs citations

21
times ranked

159
citing authors

#	ARTICLE	IF	CITATIONS
1	Privacy-Preserving Biometric Authentication: Challenges and Directions. Security and Communication Networks, 2017, 2017, 1-9.	1.5	30
2	Multi-key Homomorphic Authenticators. Lecture Notes in Computer Science, 2016, , 499-530.	1.3	28
3	Two-Hop Distance-Bounding Protocols: Keep Your Friends Close. IEEE Transactions on Mobile Computing, 2018, 17, 1723-1736.	5.8	16
4	On the Leakage of Information in Biometric Authentication. Lecture Notes in Computer Science, 2014, , 265-280.	1.3	15
5	Using Distance-Bounding Protocols to Securely Verify the Proximity of Two-Hop Neighbours. IEEE Communications Letters, 2015, 19, 1173-1176.	4.1	11
6	$\text{HB} + \text{DB}$ Distance bounding meets human based authentication. Future Generation Computer Systems, 2018, 80, 627-639.		
7	TOPPool: Time-aware Optimized Privacy-Preserving Ridesharing. Proceedings on Privacy Enhancing Technologies, 2019, 2019, 93-111.	2.8	11
8	Multi-key homomorphic authenticators. IET Information Security, 2019, 13, 618-638.	1.7	6
9	The Simplest Multi-key Linearly Homomorphic Signature Scheme. Lecture Notes in Computer Science, 2019, , 280-300.	1.3	6
10	LOVE a Pairing. Lecture Notes in Computer Science, 2021, , 320-340.	1.3	5
11	Matrioska: A Compiler for Multi-key Homomorphic Signatures. Lecture Notes in Computer Science, 2018, , 43-62.	1.3	5
12	HB+DB, mitigating man-in-the-middle attacks against HB+ with distance bounding. , 2015, , .		4
13	SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol with Authenticated Ratcheting. , 2019, , .		4
14	Yggdrasil: Privacy-Aware Dual Deduplication in Multi Client Settings. , 2021, , .		4
15	Where Are You Bob? Privacy-Preserving Proximity Testing with a Napping Party. Lecture Notes in Computer Science, 2020, , 677-697.	1.3	4
16	Secure Generalized Deduplication via Multi-Key Revealing Encryption. Lecture Notes in Computer Science, 2020, , 298-318.	1.3	3
17	Outsourcing MPC Precomputation for Location Privacy. , 2022, , .		2
18	\mathcal{HIKE} : Walking the Privacy Trail. Lecture Notes in Computer Science, 2018, , 43-66.	1.3	1

#	ARTICLE	IF	CITATIONS
19	Anonymous Single-Round Server-Aided Verification. Lecture Notes in Computer Science, 2019, , 23-43.	1.3	1
20	Progressive and Efficient Verification for Digital Signatures. Lecture Notes in Computer Science, 2022, , 440-458.	1.3	1
21	Revisiting Yasuda et al.'s Biometric Authentication Protocol: Are You Private Enough?. Lecture Notes in Computer Science, 2018, , 161-178.	1.3	0