Albert Levi

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/7043972/publications.pdf

Version: 2024-02-01

83 papers	959 citations	759233 12 h-index	526287 27 g-index
87 all docs	87 docs citations	87 times ranked	845 citing authors

#	ARTICLE	IF	CITATIONS
1	A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems. IEEE Communications Surveys and Tutorials, 2018, 20, 2543-2585.	39.4	170
2	Privacy preserving clustering on horizontally partitioned data. Data and Knowledge Engineering, 2007, 63, 646-666.	3.4	98
3	A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ACM Computing Surveys, 2022, 54, 1-37.	23.0	67
4	Distributed privacy preserving k-means clustering with additive secret sharing. , 2008, , .		53
5	PUF-enhanced offline RFID security and privacy. Journal of Network and Computer Applications, 2012, 35, 2059-2067.	9.1	50
6	Public key cryptography based privacy preserving multi-context RFID infrastructure. Ad Hoc Networks, 2009, 7, 136-152.	5.5	42
7	Relay Attacks on Bluetooth Authentication and Solutions. Lecture Notes in Computer Science, 2004, , 278-288.	1.3	33
8	Deriving cryptographic keys from physiological signals. Pervasive and Mobile Computing, 2017, 39, 65-79.	3.3	25
9	Two-tier anomaly detection based on traffic profiling of the home automation system. Computer Networks, 2019, 158, 46-60.	5.1	23
10	Disclosure Risks of Distance Preserving Data Transformations. Lecture Notes in Computer Science, 2008, , 79-94.	1.3	18
11	Performance evaluation of public-key cryptosystem operations in WTLS protocol. , 0, , .		17
12	Increasing Resiliency in Multi-phase Wireless Sensor Networks: Generationwise Key Predistribution Approach. Computer Journal, 2011, 54, 602-616.	2.4	17
13	Quarantine region scheme to mitigate spam attacks in wireless-sensor networks. IEEE Transactions on Mobile Computing, 2006, 5, 1074-1086.	5.8	16
14	A highly resilient and zone-based key predistribution protocol for multiphase wireless sensor networks. , 2009, , .		16
15	A Survey on the Development of Security Mechanisms for Body Area Networks. Computer Journal, 2014, 57, 1484-1512.	2.4	16
16	Secure key agreement protocols: Pure biometrics and cancelable biometrics. Computer Networks, 2018, 142, 33-48.	5.1	13
17	Inside risks: Risks in email security. Communications of the ACM, 2001, 44, 112.	4.5	12
18	Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure. ACM Transactions on Information and System Security, 2004, 7, 21-59.	4.5	12

#	Article	IF	Citations
19	A New Security and Privacy Framework for RFID in Cloud Computing. , 2013, , .		12
20	Utilizing hash graphs for key distribution for mobile and replaceable interconnected sensorsin the IoT context. Ad Hoc Networks, 2017, 57, 3-18.	5.5	12
21	An Efficient 2-Party Private Function Evaluation Protocol Based on Half Gates. Computer Journal, 2019, 62, 598-613.	2.4	12
22	CONSEPP: CONvenient and secure electronic payment protocol based on X9.59. , 0, , .		11
23	Distributed Privacy Preserving Clustering via Homomorphic Secret Sharing and Its Application to (Vertically) Partitioned Spatio-Temporal Data. International Journal of Data Warehousing and Mining, 2011, 7, 46-66.	0.6	11
24	Simple, extensible and flexible random key predistribution schemes for wireless sensor networks using reusable key pools. Journal of Intelligent Manufacturing, 2010, 21, 635-645.	7.3	10
25	Enhancing privacy in collaborative trafficâ€monitoring systems using autonomous location update. IET Intelligent Transport Systems, 2013, 7, 388-395.	3.0	10
26	Key distribution scheme for peer-to-peer communication in mobile underwater wireless sensor networks. Peer-to-Peer Networking and Applications, 2014, 7, 698-709.	3.9	10
27	Efficient Secure Building Blocks With Application to Privacy Preserving Machine Learning Algorithms. IEEE Access, 2021, 9, 8324-8353.	4.2	10
28	Highly Efficient and Re-executable Private Function Evaluation with Linear Complexity. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	5.4	9
29	A game theoretic model for digital identity and trust in online communities. , 2010, , .		8
30	k-strong privacy for radio frequency identification authentication protocols based on physically unclonable functions. Wireless Communications and Mobile Computing, 2015, 15, 2150-2166.	1.2	8
31	Sensor wars: detecting and defending against spam attacks in wireless sensor networks. , 2004, , .		7
32	Secret sharing using biometric traits. , 2006, 6202, 259.		7
33	Understanding the limitations of S/MIME digital signatures for e-mails: A GUI based approach. Computers and Security, 2009, 28, 105-120.	6.0	6
34	A resilient key predistribution scheme for multiphase wireless sensor networks. , 2009, , .		6
35	Two-Tier, Scalable and Highly Resilient Key Predistribution Scheme for Location-Aware Wireless Sensor Network Deployments. Mobile Networks and Applications, 2010, 15, 517-529.	3.3	6
36	Key Predistribution Schemes for Sensor Networks for Continuous Deployment Scenario. Lecture Notes in Computer Science, 2007, , 239-250.	1.3	6

#	Article	IF	Citations
37	Analytical performance evaluation of nested certificates. Performance Evaluation, 1999, 36-37, 213-232.	1.2	5
38	Simple and Flexible Random Key Predistribution Schemes for Wireless Sensor Networks Using Deployment Knowledge. , 2008, , .		5
39	HaG: Hash graph based key predistribution scheme for multiphase wireless sensor networks. , 2013, , .		5
40	DKEM: Secure and efficient Distributed Key Establishment Protocol for Wireless Mesh Networks. Ad Hoc Networks, 2017, 54, 53-68.	5.5	5
41	SeFER: secure, flexible and efficient routing protocol for distributed sensor networks. , 0, , .		4
42	Towards a framework for security analysis of multiple password schemes. , 2008, , .		4
43	Energy Efficient Privacy Preserved Data Gathering in Wireless Sensor Networks Having Multiple Sinks. , 2009, , .		4
44	A distributed key establishment scheme for wireless mesh networks using identity-based cryptography. , 2010, , .		4
45	Towards Using Physiological Signals as Cryptographic Keys in Body Area Networks. , 2015, , .		4
46	How secure is secure Web browsing?. Communications of the ACM, 2003, 46, 152.	4.5	3
47	P2-CTM. , 2010, , .		3
48	Providing Resistance against Server Information Leakage in RFID Systems. , 2011, , .		3
49	Secure key agreement using pure biometrics. , 2015, , .		3
50	A Role and Activity Based Access Control for Secure Healthcare Systems. Lecture Notes in Electrical Engineering, 2016, , 93-103.	0.4	3
51	TRAPDROID: Bare-Metal Android Malware Behavior Analysis Framework. , 2019, , .		3
52	SKA-PS: Secure key agreement protocol using physiological signals. Ad Hoc Networks, 2019, 83, 111-124.	5.5	3
53	Uneven Key Pre-Distribution Scheme for Multi-Phase Wireless Sensor Networks. Lecture Notes in Electrical Engineering, 2013, , 359-368.	0.4	3
54	Secure and privacy preserving IoT gateway for home automation. Computers and Electrical Engineering, 2022, 102, 108036.	4.8	3

#	Article	IF	Citations
55	Data Collection Framework for Energy Efficient Privacy Preservation in Wireless Sensor Networks Having Many-to-Many Structures. Sensors, 2010, 10, 8375-8397.	3.8	2
56	CoRPPS: Collusion Resistant Pseudonym Providing System. , 2011, , .		2
57	WebRTC based augmented secure communication. , 2016, , .		2
58	Two-Tier, Location-Aware and Highly Resilient Key Predistribution Scheme for Wireless Sensor Networks. , 0, , .		2
59	Secure Matrix Operations for Machine Learning Classifications Over Encrypted Data in Post Quantum Industrial IoT. , 2021, , .		2
60	An Optimistic Fair E-Commerce Protocol for Large E-Goods. , 0, , .		1
61	Resilient key establishment for mobile sensor networks. , 2011, , .		1
62	PA-CTM. , 2011, , .		1
63	Maintaining trajectory privacy in mobile wireless sensor networks. , 2013, , .		1
64	Mobile malware classification based on permission data. , 2015, , .		1
65	Feature-level fusion of physiological parameters to be used as cryptographic keys. , 2017, , .		1
66	Robust Two-factor smart card authentication. , 2017, , .		1
67	SU-PhysioDB: A physiological signals database for body area network security. , 2017, , .		1
68	Generating One-Time Keys for Secure Multimedia Communication. , 2018, , .		1
69	Secure key agreement based on ordered biometric features. Computer Networks, 2019, 163, 106885.	5.1	1
70	SKA-CaNPT. , 2019, , .		1
71	Scalable Wi-Fi Intrusion Detection for IoT Systems. , 2021, , .		1
72	A Distributed Scheme to Detect Wormhole Attacks in Mobile Wireless Sensor Networks. , 2011, , 157-163.		1

#	Article	IF	Citations
73	Distributed Privacy Preserving Clustering via Homomorphic Secret Sharing and its Application to (Vertically) Partitioned Spatio-Temporal Data. , 2013, , 45-65.		1
74	Investigation and Application of Differential Privacy in Bitcoin. IEEE Access, 2022, 10, 25534-25554.	4.2	1
75	Development of Novel Materials for Proton Exchange Membrane Fuel Cells. Materials Research Society Symposia Proceedings, 2006, 948, 1.	0.1	0
76	Dynamic Resiliency Analysis of Key Predistribution in Wireless Sensor Networks. , 2009, , .		0
77	Using combined keying materials for key distribution in wireless sensor networks. , 2010, , .		0
78	Dynamic key ring update mechanism for Mobile Wireless Sensor Networks. , 2013, , .		0
79	Augmented Randomness for Secure Key Agreement using Physiological Signals. , 2020, , .		0
80	Practical and Secure E-Mail System (PractiSES). Lecture Notes in Computer Science, 2004, , 410-419.	1.3	0
81	A Fair Multimedia Exchange Protocol. Lecture Notes in Computer Science, 2005, , 342-351.	1.3	0
82	Achieving Fast Self Healing in Wireless Sensor Networks Using Multi-generation Deployment Schemes. Communications in Computer and Information Science, 2009, , 180-198.	0.5	0
83	Securing Internet of Things Networks with Gateways and Multi-SSID Technology. , 2021, , .		0