

Siamak F Shahandashti

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/4925813/publications.pdf>

Version: 2024-02-01

33
papers

880
citations

623188

14
h-index

476904

29
g-index

34
all docs

34
docs citations

34
times ranked

685
citing authors

#	ARTICLE	IF	CITATIONS
1	A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks. <i>Journal of Cybersecurity and Privacy</i> , 2022, 2, 124-152.	2.4	12
2	Performance and Usability of Visual and Verbal Verification of Word-Based Key Fingerprints. <i>IFIP Advances in Information and Communication Technology</i> , 2021, , 199-210.	0.5	1
3	Formal modelling and security analysis of Bitcoin's payment protocol. <i>Computers and Security</i> , 2021, 107, 102279.	4.0	5
4	On Secure E-Voting over Blockchain. <i>Digital Threats Research and Practice</i> , 2021, 2, 1-13.	1.7	8
5	SEAL: Sealed-Bid Auction Without Auctioneers. <i>IEEE Transactions on Information Forensics and Security</i> , 2020, 15, 2042-2052.	4.5	14
6	End-to-End Verifiable E-Voting Trial for Polling Station Voting. <i>IEEE Security and Privacy</i> , 2020, 18, 6-13.	1.5	3
7	Battery draining attacks against edge computing nodes in IoT networks. <i>Cyber-Physical Systems</i> , 2020, 6, 96-116.	1.6	22
8	DOMtegrity: ensuring web page integrity against malicious browser extensions. <i>International Journal of Information Security</i> , 2019, 18, 801-814.	2.3	10
9	Verifiable Classroom Voting in Practice. <i>IEEE Security and Privacy</i> , 2018, 16, 72-81.	1.5	5
10	Stealing PINs via mobile sensors: actual risk versus user perception. <i>International Journal of Information Security</i> , 2018, 17, 291-313.	2.3	40
11	Analyzing and Patching SPEKE in ISO/IEC. <i>IEEE Transactions on Information Forensics and Security</i> , 2018, 13, 2844-2855.	4.5	8
12	Texture to the Rescue. <i>ACM Transactions on Privacy and Security</i> , 2017, 20, 1-29.	2.2	11
13	A Smart Contract for Boardroom Voting with Maximum Voter Privacy. <i>Lecture Notes in Computer Science</i> , 2017, , 357-375.	1.0	284
14	Refund Attacks on Bitcoin's Payment Protocol. <i>Lecture Notes in Computer Science</i> , 2017, , 581-599.	1.0	14
15	DRE-ip: A Verifiable E-Voting Scheme Without Tallying Authorities. <i>Lecture Notes in Computer Science</i> , 2016, , 223-240.	1.0	23
16	TouchSignatures: Identification of user touch actions and PINs based on mobile sensor data via JavaScript. <i>Journal of Information Security and Applications</i> , 2016, 26, 23-38.	1.8	33
17	Reconciling user privacy and implicit authentication for mobile devices. <i>Computers and Security</i> , 2015, 53, 215-233.	4.0	23
18	TouchSignatures. , 2015, , .		7

#	ARTICLE	IF	CITATIONS
19	The Fairy-Ring Dance. , 2015, , .		2
20	Authenticated Key Exchange over Bitcoin. Lecture Notes in Computer Science, 2015, , 3-20.	1.0	13
21	Tap-Tap and Pay (TTP): Preventing the Mafia Attack in NFC Payment. Lecture Notes in Computer Science, 2015, , 21-39.	1.0	13
22	Privacy-Preserving Implicit Authentication. IFIP Advances in Information and Communication Technology, 2014, , 471-484.	0.5	17
23	The SPEKE Protocol Revisited. Lecture Notes in Computer Science, 2014, , 26-38.	1.0	17
24	Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts. International Journal of Information Security, 2013, 12, 251-265.	2.3	50
25	New security notions and relations for public-key encryption. Journal of Mathematical Cryptology, 2012, 6, 183-227.	0.4	1
26	Attribute-based encryption without key cloning. International Journal of Applied Cryptography, 2012, 2, 250.	0.4	22
27	Private Fingerprint Matching. Lecture Notes in Computer Science, 2012, , 426-433.	1.0	19
28	Adaptive CCA Broadcast Encryption with Constant-Size Secret Keys and Ciphertexts. Lecture Notes in Computer Science, 2012, , 308-321.	1.0	15
29	Generic constructions for universal designated-verifier signatures and identity-based signatures from standard signatures. IET Information Security, 2009, 3, 152-176.	1.1	6
30	Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems. Lecture Notes in Computer Science, 2009, , 198-216.	1.0	151
31	Construction of Universal Designated-Verifier Signatures and Identity-Based Signatures from Standard Signatures. , 2008, , 121-140.		14
32	Concurrently-secure credential ownership proofs. , 2007, , .		3
33	A Provably Secure Short Transitive Signature Scheme from Bilinear Group Pairs. Lecture Notes in Computer Science, 2005, , 60-76.	1.0	13