# 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 | 880 | 623188 | 476904 |
|---|---|---|---|
| papers | citations | 14 | 29 |
| | | h-index | g-index |

| 34 | 34 | 34 | 685 |
|---|---|---|---|
| all docs | docs citations | times ranked | citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | A Smart Contract for Boardroom Voting with Maximum Voter Privacy. Lecture Notes in Computer Science, 2017, , 357-375. | 1.0 | 284 |
| 2 | Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems. Lecture Notes in Computer Science, 2009, , 198-216. | 1.0 | 151 |
| 3 | Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts. International Journal of Information Security, 2013, 12, 251-265. | 2.3 | 50 |
| 4 | Stealing PINs via mobile sensors: actual risk versus user perception. International Journal of Information Security, 2018, 17, 291-313. | 2.3 | 40 |
| 5 | TouchSignatures: Identification of user touch actions and PINs based on mobile sensor data via JavaScript. Journal of Information Security and Applications, 2016, 26, 23-38. | 1.8 | 33 |
| 6 | Reconciling user privacy and implicit authentication for mobile devices. Computers and Security, 2015, 53, 215-233. | 4.0 | 23 |
| 7 | DRE-ip: A Verifiable E-Voting Scheme Without Tallying Authorities. Lecture Notes in Computer Science, 2016, , 223-240. | 1.0 | 23 |
| 8 | Attribute-based encryption without key cloning. International Journal of Applied Cryptography, 2012, 2, 250. | 0.4 | 22 |
| 9 | Battery draining attacks against edge computing nodes in IoT networks. Cyber-Physical Systems, 2020, 6, 96-116. | 1.6 | 22 |
| 10 | Private Fingerprint Matching. Lecture Notes in Computer Science, 2012, , 426-433. | 1.0 | 19 |
| 11 | Privacy-Preserving Implicit Authentication. IFIP Advances in Information and Communication Technology, 2014, , 471-484. | 0.5 | 17 |
| 12 | The SPEKE Protocol Revisited. Lecture Notes in Computer Science, 2014, , 26-38. | 1.0 | 17 |
| 13 | Adaptive CCA Broadcast Encryption with Constant-Size Secret Keys and Ciphertexts. Lecture Notes in Computer Science, 2012, , 308-321. | 1.0 | 15 |
| 14 | SEAL: Sealed-Bid Auction Without Auctioneers. IEEE Transactions on Information Forensics and Security, 2020, 15, 2042-2052. | 4.5 | 14 |
| 15 | Construction of Universal Designated-Verifier Signatures and Identity-Based Signatures from Standard Signatures. , 2008, , 121-140. | | 14 |
| 16 | Refund Attacks on Bitcoinâ€™s Payment Protocol. Lecture Notes in Computer Science, 2017, , 581-599. | 1.0 | 14 |
| 17 | Authenticated Key Exchange over Bitcoin. Lecture Notes in Computer Science, 2015, , 3-20. | 1.0 | 13 |
| 18 | Tap-Tap and Pay (TTP): Preventing the Mafia Attack in NFC Payment. Lecture Notes in Computer Science, 2015, , 21-39. | 1.0 | 13 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | A Provably Secure Short Transitive Signature Scheme from Bilinear Group Pairs. Lecture Notes in Computer Science, 2005, , 60-76. | 1.0 | 13 |
| 20 | A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks. Journal of Cybersecurity and Privacy, 2022, 2, 124-152. | 2.4 | 12 |
| 21 | Texture to the Rescue. ACM Transactions on Privacy and Security, 2017, 20, 1-29. | 2.2 | 11 |
| 22 | DOMtegrity: ensuring web page integrity against malicious browser extensions. International Journal of Information Security, 2019, 18, 801-814. | 2.3 | 10 |
| 23 | Analyzing and Patching SPEKE in ISO/IEC. IEEE Transactions on Information Forensics and Security, 2018, 13, 2844-2855. | 4.5 | 8 |
| 24 | On Secure E-Voting over Blockchain. Digital Threats Research and Practice, 2021, 2, 1-13. | 1.7 | 8 |
| 25 | TouchSignatures. , 2015, , . | | 7 |
| 26 | Generic constructions for universal designated-verifier signatures and identity-based signatures from standard signatures. IET Information Security, 2009, 3, 152-176. | 1.1 | 6 |
| 27 | Verifiable Classroom Voting in Practice. IEEE Security and Privacy, 2018, 16, 72-81. | 1.5 | 5 |
| 28 | Formal modelling and security analysis of Bitcoinâ€™s payment protocol. Computers and Security, 2021, 107, 102279. | 4.0 | 5 |
| 29 | Concurrently-secure credential ownership proofs. , 2007, , . | | 3 |
| 30 | End-to-End Verifiable E-Voting Trial for Polling Station Voting. IEEE Security and Privacy, 2020, 18, 6-13. | 1.5 | 3 |
| 31 | The Fairy-Ring Dance. , 2015, , . | | 2 |
| 32 | New security notions and relations for public-key encryption. Journal of Mathematical Cryptology, 2012, 6, 183-227. | 0.4 | 1 |
| 33 | Performance and Usability of Visual and Verbal Verification of Word-Based Key Fingerprints. IFIP Advances in Information and Communication Technology, 2021, , 199-210. | 0.5 | 1 |