

**2019 16th International ISC
(Iranian Society of Cryptology)
Conference on Information
Security and Cryptology
(ISCISC 2019)**

**Mashhad, Iran
28-29 August 2019**



**IEEE Catalog Number: CFP1962R-POD
ISBN: 978-1-7281-4375-0**

**Copyright © 2019 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1962R-POD
ISBN (Print-On-Demand):	978-1-7281-4375-0
ISBN (Online):	978-1-7281-4374-3
ISSN:	2475-2363

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

ISCISC 2019 Papers

No.	Paper Title	Authors	Pages
1	Blind Multipurpose Image Watermarking Based on Secret Sharing	Sorour Sheidani, Ziba Eslami	1
2	Improvement of Digest Based Authentication for Biometric Verification	Faezeh Sadat Babamir, Mervet Kirci	9
3	GSLHA: Group-based Secure Lightweight Handover Authentication Protocol for M2M Communication	Mohammad Mahdi Modiri, Javad Mohajeri, Mahmoud Salmasizadeh	15
4	A New RF-PUF Based Authentication of Internet of Things Using Random Forest Classification	Amir Ashtari, Ahmad Shabani, Bijan Alizadeh	21
5	An Ultra-Lightweight RFID Mutual Authentication Protocol	Abbas Rahnama, Mohammad Beheshti-Atashgah, Taraneh Eghlidos, Mohammad Reza Aref	27
6	Investigating the Streaming Algorithms Usage in Website Fingerprinting Attack Against Tor Privacy Enhancing Technology	Reyhane Attarian, Sattar Hashemi	33
7	A Lightweight Anonymous Authentication Protocol for IoT Wireless Sensor Networks	Abbas Rahnama, Mohammad Beheshti-Atashgah, Taraneh Eghlidos, Mohammad Reza Aref	39
8	Cryptanalysis of sp2das and 3PDA, Two Data Aggregation Schemes for Smart Grid	Hamid Amiryousefi, Zahra Ahmadian	45
9	A Novel Steganography Algorithm Using Edge Detection and MPC Algorithm	Aref Rezaei, Leili Farzinvash, Ali Farzamnia	49
10	Lightweight Involutive Components for Symmetric Cryptography	S. M. Dehnavi, M. R. Mirzaee Shamsabad, A. Mahmoodi Rishakani	61
11	Cryptanalysis of a Certificateless Signcryption Scheme	Parvin Rastegari, Mohammad Dakhilalian	67
12	Ransomware Detection Using Process Mining and Classification Algorithms	Ala Bahrani, Amir Jalaly Bidgly	73
13	Inferring API Correct Usage Rules: A Tree-based Approach	Majid Zolfaghari, Solmaz Salimi, Mehdi Kharrazi	78
14	An Anonymous Attribute-based Access Control System Supporting Access Structure Update	Mostafa Chegenizadeh, Mohammad Ali, Javad Mohajeri, Mohammad Reza Aref	85
15	Threat Extraction in IoT-Based Systems Focusing on Smart Cities	Abbas Nejatifar, Mohammad Ali Hadavi	92
16	Classical-Quantum Multiple Access Wiretap Channel	Hadi Aghaee, Bahareh Akhbari	99
17	Fault Tolerant Non-Linear Techniques for Scalar Multiplication in ECC	Zahra Saffar, Siamak Mohammadi	104
18	IoT-Based Anonymous Authentication Protocol Using Biometrics in Smart Homes	ShayanMehranpoor, Naser Mohammadzadeh, Hossein Gharaee	114
19	An Efficient Secret Sharing-Based Storage System for Cloud-Based IoTs	Majid Farhadi, Hamideh Bypour, Reza Mortazavi	155

No.	Paper Title	Authors	Pages
20	Analysis of Machine Learning Techniques for Ransomware Detection	Fakhroddin Noorbehbahani, Farzaneh Rasouli, Mohammad Saberi	128
21	CRT-Based Robust Data Hiding Method by Extracting Features in DCT Domain	Alireza Ghaemi, Habibollah Danyali	134
22	SANUB: A New Method for Sharing and Analyzing News Using Blockchain	Arian balouchestani, Mojtaba Mahdavi, Yeganeh Hallaj, Delaram Javdani	139