

**2017 14th International ISC
(Iranian Society of Cryptology)
Conference on Information
Security and Cryptology
(ISCISC 2017)**

**Shiraz, Iran
6-7 September 2017**



**IEEE Catalog Number: CFP1762R-POD
ISBN: 978-1-5386-6561-9**

**Copyright © 2017 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: | CFP1762R-POD |
| ISBN (Print-On-Demand): | 978-1-5386-6561-9 |
| ISBN (Online): | 978-1-5386-6560-2 |
| 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



انجمن رمزایران
Iranian Society of Cryptology

14th International ISC Conference on
Information Security and Cryptology (ISCISC)
September 6-7, 2017; Shiraz University - Shiraz, Iran



Table of Content

01-“Lightweight and Secure Authentication Protocol for the Internet of Things in Vehicular Systems”

Sima Arasteh; Maede Ashouri-Talouki; Seyed Farhad Aghili1

02-“Hybrid Intrusion Detection: Combining Decision Tree and Gaussian Mixture Model”

Marzieh Bitaab; Sattar Hashemi8

03-“A Formal Model for Security Analysis of Trust and Reputation systems”

Seyed Asgary Ghasempouri; Behrouz Tork Ladani13

04-“WAVE: Black Box Detection of XSS, CSRF and Information Leakage Vulnerabilities”

Hamed Soleimani; Mohmmad Ali Hadavi; Arash Bagherdaei19

05-“Utilizing Features of Aggregated Flows to Identify Botnet Network Traffic”

Banafsheh Heydari; Habib Yajam; Mohammad Ali Akhaee; Sadaf Salehkalaibar25

06-“Analysis of a Distance Bounding Protocol for Verifying the Proximity of Two-Hop Neighbors”

Hoda Jannati; Nasour Bagheri; Masoumeh Safkhani31

07-“A New Distributed Group Key Management Scheme for Wireless Sensor Networks”

Mojtaba Mohammadi; Alireza Keshavarz-Haddad37

| | |
|---|----|
| 08-“A Lightweight and Secure Data Sharing Protocol for D2D Communications” | |
| Atefeh Mohseni-Ejiyeh; Maede Ashouri-Talouki; Mojtaba Mahdavi | 42 |
| | |
| 09-“CAFD: Detecting Collusive Frauds in Online Auction Networks by Combining One-Class Classification and Collective Classification” | |
| Nazanin Habibollahi; Mahdi Abadi; Mahila Dadfarnia | 48 |
| | |
| 10-“Improved Fixed Point Attack on Gost2” | |
| Siavash Ahmadi; Mohammad Reza Aref | 54 |
| | |
| 11-“Finite State Machine Based Countermeasure for Cryptographic Algorithms” | |
| Sadegh Attari; Aein Rezaei Shahmirzadi; Mahmoud Salmasizadeh; Iman Gholampour | 58 |
| | |
| 12-“A New Approach to Key Schedule Designing” | |
| Seyed Reza Hoseini Najarkolaei; Siavash Ahmadi; Mohammad Reza Aref | 64 |
| | |
| 13-“New Techniques for Localization Based Information Theoretic Secret Key Agreement” | |
| Narges Kazempour; Mahtab Mirmohseni; Mohammad Reza Aref | 70 |
| | |
| 14-“On the Security of O-PSI a Delegated Private Set Intersection on Outsourced Datasets” | |
| Mehdi Mahdavi Oliaaee; Mahshid Delavar; Mohammad Hassan Ameri; Javad Mohajeri; Mohammad Reza Aref | 77 |
| | |
| 15-“Cryptanalysis of an Asymmetric Searchable Encryption Scheme” | |
| Fahimeh Zare; Hamid Mala | 82 |
| | |
| 16-“Physical Layer Security in AF and CF Relay Networks with RF-Energy Harvesting” | |
| Ali Soleimani; Mahtab Mirmohseni; Mohammad Reza Aref | 86 |

| | |
|---|-----|
| 17-“Proposing a New Feature for Structure-Aware Analysis of Android Malwares” | |
| Shahrooz Pooryousef; Kazim Fouladi..... | 93 |
| | |
| 18-“Impossible Differential Cryptanalysis of Reduced-Round Midori64 Block Cipher” | |
| Aein Rezaei Shahmirzadi; Seyyed Arash Azimi; Mahmoud Salmasizadeh | 99 |
| | |
| 19-“A Novel Multiplicative Steganography Technique in Contourlet Domain” | |
| Farid Saleh; Maryam Amirmazlaghani..... | 105 |
| | |
| 20-“An Efficient Cooperative Message Authentication Scheme in Vehicular Ad-hoc Networks” | |
| Amirreza Sarenchah; Maryam Rajabzadeh Asaar; Mahmoud Salmasizadeh; Mohammad Reza Aref | 111 |
| | |
| 21-“Enforcing Access Control Policies over Data Stored on Untrusted Server” | |
| Naeimeh Soltani; Rasool Jalili | 119 |
| | |
| 22-“A Novel and Efficient Privacy Preserving TETRA Authentication Protocol” | |
| Behnam Zahednejad; Mahdi Azizi; Morteza Pournaghi..... | 125 |