

2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC 2016)

**Tehran, Iran
7-8 September 2016**



**IEEE Catalog Number: CFP1662R-POD
ISBN: 978-1-5090-3950-0**

**Copyright © 2016 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 publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1662R-POD
ISBN (Print-On-Demand):	978-1-5090-3950-0
ISBN (Online):	978-1-5090-3949-4

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 رمز ایران
Iranian Society of Cryptology

13th International ISC Conference on
Information Security and Cryptology (ISCISC2016)
September 7-8, 2016; Shahid Beheshti University – Tehran, Iran



Shahid Beheshti University

Table of Content

01- “Construction of New S-boxes Via Permuting the Inverse Mapping on Special Subsets”	
Mojtaba Dehnavi; Mohammadreza Mirzaee-Shamsabad; Akbar Mahmoodi-Rishakani	1
02- “An Identity-Based Digital Signature Scheme to Detect Pollution Attacks in Intra-Session Network Coding”	
Sogand SadrHaghighi; Siavash Khorsandi	7
03- “Counterfeiting Attack on Adjusted Expanded-bit Multiscale Quantization-based Semi-fragile Watermarking Technique”	
Samira Hosseini; Mojtaba Mahdavi	13
04- “A Secret Key Encryption Scheme Based on 1-Level QC-LDPC Lattices”	
Khadijeh Bagheri; Mohammad-Reza Sadeghi; Taraneh Eghlidos; Daniel Panario	20
05- “XABA: A Zero-Knowledge Anomaly-Based Behavioral Analysis Method to Detect Insider Threats”	
Abolfazl Zargar; Alireza Nowroozi; Rasool Jalili	26
06- “Feature Extraction for Detection of Watermarking Algorithm”	
Zahra Hatefi; Mojtaba Mahdavi; Pegah Nikbakht	32
07- “A New CPA Resistant Software Implementation for Symmetric Ciphers with Smoothed Power Consumption”	
Morteza Safaeipour; Mahmoud Salmasizadeh	38
08- “Biclique Cryptanalysis of Twine-128”	
Seyed Reza Hoseini-Najarkolaei; Mohammad Zare-Ahangarkolaei; Siavash Ahmadi; Mohammad Reza Aref	46
09- “A New Lightweight Authenticated Key Exchange Protocol for Internet of Things”	
Sima Arasteh; Seyed Farhad Aghili; Hamid Mala	52
10- “Preserving Privacy in Location Based Mobile Coupon Systems Using Anonymous Authentication Scheme”	
Mohsen Ahmadi; Behrooz Shahgholi-Ghahfarokhi	60
11- “Zero Correlation Linear Attack on Reduced Round Piccolo-80”	
Mohammad Zare-Ahangarkolaei; Seyed Reza Hoseini-Najarkolaei; Siavash Ahmadi; Mohammad Reza Aref	66
12- “FMNV Continuous Non-malleable Encoding Scheme is More Efficient Than Believed”	
Seyyed Amir Mortazavi; Mahmoud Salmasizadeh; Amir Daneshgar	72
13- “2entFOX: A Framework for High Survivable Ransomwares Detection”	
Mohammad Mehdi Ahmadian; Hamid Reza Shahriari	79



انجمن رمز ایران
Iranian Society of Cryptology

**13th International ISC Conference on
Information Security and Cryptology (ISCISC2016)
September 7-8, 2016; Shahid Beheshti University – Tehran, Iran**



Shahid Beheshti University

14- “Fine-Grained Access Control for Hybrid Mobile Applications in Android Using Restricted Paths”	
Shahrooz Pooryousef; Morteza Amini	85
15- “PapiaPass: Sentence-based Passwords Using Dependency Trees”	
Habibollah Yajam; Younes Karimi-Ahmadabadi; Mohammad Ali Akhaee	91
16- “Video Watermarking in the DT-CWT Domain Using Hyperbolic Function”	
Milad Ghalejugh; Mohammad Ali Akhaee	97
17- “Security Improvement of FPGA Configuration File Against the Reverse Engineering Attack”	
Sharareh ZamanZadeh; Shahram Shahabi; Ali Jahanian	101
18- “An Improved Certificateless Signcryption Scheme”	
Parvin Rastegari; Mehdi Berenjkoub	106
19- “A New Approach for Effective Malware Detection in Android-based Devices”	
Mahmood Deypir	112
20- “Spread Spectrum Watermarking Robust to SILK Vocoder”	
Ali Sattari; Mohammad Ali Akhaee	117