

# **2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC 2015)**

**Rasht, Iran  
8 – 10 September 2015**



**IEEE Catalog Number: CFP1562R-POD  
ISBN: 978-1-4673-7610-5**

**Copyright © 2015 by the Institute of Electrical and Electronic 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:	CFP1562R-POD
ISBN (Print-On-Demand):	978-1-4673-7610-5
ISBN (Online):	978-1-4673-7609-9

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

## Table of Contents

Biclique Cryptanalysis of LBlock with Modified Key Schedule	1
A Chaotic Watermarking Scheme using Discrete Cosine Transform	6
A Novel Location-Based Key Distribution Scheme for Large-Scale Stationary Wireless Networks	11
Fast and Pipelined Bit-Parallel Montgomery Multiplication and Squaring over GF(2 <sup>m</sup> )	17
Sybil Attack Detection Using a Low Cost Short Group Signature in VANET	23
LRBAC: Flexible Function-Level Hierarchical Role Based Access Control for Linux	29
Illumination invariant encrypted face recognition using correlation filter	36
A Low-Cost and Flexible FPGA Implementation for SPECK Block Cipher	42
Construction of MDS matrices from minors of an MDS matrix	48
Tiny Jump-Oriented Programming Attack (A Class of Code Reuse Attacks)	52
Impossible Differential Cryptanalysis of reduced-round TEA and XTEA	58
Collaborative Privacy Management in P2P Online Social Networks	64
Ternary Timing Covert Channel in Wireless 802.11	73
Connection-Monitor & Connection-Breaker: A Novel Approach for Prevention and Detection of High Survivable Ransomwares	79
A New Self-healing Group Key Distribution Scheme	85
Cryptanalysis and Strengthening of SRP+ Protocol	91
Real Time Alert Correlation and Prediction using Bayesian Networks	98
Patulous Code Reuse Attack: A Novel Code Reuse Attack on ARM Architecture (A Proof of Concept on Android OS)	104

Tunneling Protocols Identification using Light Packet Inspection	110
Cryptanalysis of Two EPC-based RFID Security Schemes	116
A new robust video watermarking algorithm against cropping and rotating attacks	122
Behavior and System Based Backdoor Detection Focusing on CMD Phase	128
Modification in Spatial, Extraction from Transform: A new approach for JPEG steganography	134
Solving discrete logarithm problem on elliptic curves over rational numbers	141
A Software Solution for Realtime Malware Detection in Distributed Systems	144