2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC 2018)

Tehran, Iran
28 – 29 August 2018

IEEE Catalog Number:	CFP1862R-POD
ISBN:	978-1-5386-7583-0

Copyright © 2018 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:	CFP1862R-POD
ISBN (Print-On-Demand):	978-1-5386-7583-0
ISBN (Online):	978-1-5386-7582-3
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

No.	Papers Titles
B1	Polynomials over $\mathbb{Z}_{2n}$ and their applications in symmetric cryptography.....1
B2	An efficient user identification approach based on Netflow analysis.....7
B3	Modular Construction A Lattices from Cyclotomic Fields and their Applications in Information Security.....12
B4	Threat Extraction Method Based on UML Software Description.....20
B5	Compressed Video Watermarking for Authentication and Reconstruction of the Audio part.....28
B6	A Practical and Secure Lattice-based Scheme for Full-Duplex Gaussian One-Way Relay Channels.....34
B7	Software Security Analysis Based on the Principle of Defense-in-Depth...42
B8	BLProM: Business-layer Process Miner of the web application.....48
B9	Cryptanalysis and improvement of a pairing-free certificateless signature scheme.....54
C10	A Novel Approach for Detecting DGA-based Ransomwares.....59
C11	A New Statistical Method for Wormhole Attack Detection in MANETs...66
C12	Detecting Privacy Leaks in Android Apps using Inter-Component Information Flow Control Analysis.....72
C13	BotcoinTrap: Detection of Bitcoin Miner Botnet Using Host Based Approach.....78
D14	SMSBotHunter: A Novel Anomaly Detection Technique to Detect SMS Botnets.....84

D15	Phase Jamming Attack: A Practical Attack on Physical layer-Based Key Derivation.....90
D16	Tampering Detection and Restoration of Compressed Video.....94