

# **2012 9th International ISC Conference on Information Security and Cryptology**

**(ISCISC 2012)**

**Tabriz, Iran  
13 – 14 September 2012**



**IEEE Catalog Number: CFP1262R-PRT  
ISBN: 978-1-4673-2387-1**

## Table of Contents

---

<b>Generalization of Statistical Criteria for Sboxes</b>	<b>1</b>
<b>Statistical Properties of Modular Multiplication Modulo a Power of Two</b>	<b>6</b>
<b>A dynamic, zero-message broadcast encryption scheme based on Secure Multiparty Computation</b>	<b>12</b>
<b>A New Image Steganography Based on Denoising Methods in Wavelet Domain</b>	<b>18</b>
<b>Authentication Based on Signature Verification Using Position, Velocity, Acceleration and Jerk Signals</b>	<b>26</b>
<b>An ID-Based Key Agreement Protocol Based on ECC Among Users of Separate Networks</b>	<b>32</b>
<b>An Improvement of Image Secret Sharing and Hiding With Authentication</b>	<b>38</b>
<b>Mutual Implementation of Predefined and Random Challenges over RFID Distance Bounding Protocol</b>	<b>43</b>
<b>Policy Specification and Enforcement in Online Social Networks using MKNF+</b>	<b>48</b>
<b>Dynamic Malware Detection Using Registers Values Set Analysis</b>	<b>54</b>
<b>A Modified Dual watermarking Scheme for digital images with Tamper Localization/detection and recovery Capabilities</b>	<b>60</b>
<b>Using User Similarity to Infer Trust Values in Social Networks Regardless of Direct Ratings</b>	<b>66</b>
<b>An Efficient End to End Key Establishment Protocol for Wireless Sensor Networks</b>	<b>73</b>
<b>Measuring Software Security Using SAN Models</b>	<b>80</b>

---

<b>Non-monotonicity in OrBAC through Default and Exception Policy Rules</b>	87
<b>Real-Time Attack Scenario Detection via Intrusion Detection Alert Correlation</b>	95
<b>Two Efficient Generic Patterns for Convertible Limited Multi-Verifier Signature</b>	103
<b>On the Security of an ECC Based RFID Authentication Protocol</b>	111
<b>KerNeeS: A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions</b>	115
<b>A Trust and Reputation-based Access Control Model for Virtual Organizations</b>	121
<b>FOO e-Voting Protocol: Inductive Analysis of the Eligibility Property</b>	128
<b>An Image watermarking Algorithm Based on Chaotic Maps and Wavelet Transform</b>	135
<b>PCPD: A Novel Illustration of Pivotal Parameters of an Attack for Security Systems</b>	141
<b>Searchable Encryption Schemes</b>	147
<b>A New Method for Forensics Detection Based on 2D-Histogram and Zernike Moments</b>	151
<b>Structural TLR Algorithm for Anomaly Detection Based on Danger Theory</b>	156
<b>Modeling Sybil Attacker Behavior in VANETs</b>	162

---