# Table of Contents

## Workshop 1: AlKindi Student Workshop on Cryptology (Part 1)

<table>
<thead>
<tr>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Implementations of Elliptic Curve Cryptography in Wireless Sensor Networks (Hilal Houssain, Mohamad Badra, Turki F. Al-Somani)</td>
<td>1 - 6</td>
</tr>
<tr>
<td>Implementation of GF(2m) Elliptic Curve Cryptoprocessor on a Nano FPGA (Turki F. Al-Somani, Hilal Houssain)</td>
<td>7 - 12</td>
</tr>
<tr>
<td>A Unified Countermeasure Against Side Channel Attacks on Cryptographic RFID (Hamad Marzouqi, Mahmoud Al-Qutayri, Chan Yeob Yeun)</td>
<td>3 - 18</td>
</tr>
<tr>
<td>Forensics and War-Driving on Unsecured Wireless Network (Huwida Said, Mario Guimaraes, Noora Al Mutawa, Ihtesam Al Awadhi)</td>
<td>19 - 24</td>
</tr>
<tr>
<td>FPGA Implementation of High Speed XTS-AES for Data Storage Devices (Mohamed Elmoghany, Mohamed Diab, Moustafa Kassem, Mustafa Khairallah, Omar El Shahat, Wael Sharkasy)</td>
<td>25 - 28</td>
</tr>
<tr>
<td>The Use of Boolean Functions in Stream Ciphers (Muna Al Shehhi, Joonsang Baek, Chan Yeob Yeun)</td>
<td>29 - 33</td>
</tr>
</tbody>
</table>

## Workshop 1: AlKindi Student Workshop on Cryptology (Part 2)

<table>
<thead>
<tr>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the Security of Inclusion or Omission of MixColumns in AES Cipher (Khalfan AlMarashda, Yousuf AlSalami, Khaled Salah, Thomas Martin)</td>
<td>34 - 39</td>
</tr>
<tr>
<td>Study on Secret Sharing Schemes (SSS) and Their Applications (Noura Al Ebri, Joonsang Baek, Chan Yeob Yeun)</td>
<td>40 - 45</td>
</tr>
<tr>
<td>Survey on Computationally Hard Problems and Their Applications to Cryptography (Ameera Abdouli, Joonsang Baek, Chan Yeob Yeun)</td>
<td>46 - 52</td>
</tr>
<tr>
<td>Survey on Certificateless Public Key Cryptography (Hajer Al Housani, Joonsang Baek, Chan Yeob Yeun)</td>
<td>53 - 58</td>
</tr>
<tr>
<td>Anonymous Electronic Voting Protocol with Traceability (Lezhen Ling, Junguo Liao)</td>
<td>59 - 66</td>
</tr>
</tbody>
</table>

## Session 1

### InfoSecurity: Virtualization and Chaos

<table>
<thead>
<tr>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding the Security Challenges of Virtualized Environments (Fatma Ahmad Bazargan, Chan Yeob Yeun, Mohamed Jamal Zemerly)</td>
<td>67 - 72</td>
</tr>
<tr>
<td>Synchronization Recovery of Chaotic Signal Through Imperfect Channel Using Optimization Approach (Amr Sayed Abdel Fattah, Salwa Elramly, Magdy Ibrahim, Ahmed A. Abdel-Hafez)</td>
<td>73 - 78</td>
</tr>
<tr>
<td>Denoising Algorithm for Noisy Chaotic Signal by Using Wavelet Transform: Comprehensive Study (Amr Sayed Abdel Fattah, Salwa Elramly, Magdy Ibrahim, Ahmed A. Abdel-Hafez)</td>
<td>79 - 85</td>
</tr>
</tbody>
</table>
Workshop 2:

Chaos Generation From 1D or 2D Circuits Including Switches
(Danièle Fournier-Prunaret, Pascal Chargé, Laura Gardini) 86 - 90

Noise-resisting Ciphering Based on a Chaotic Multi-Stream Pseudo-Random Number Generator
(René Lozi, Estelle Cherrier) 91 - 96

Multicast Security Protocol Over Satellite DVB Based on Chaotic Sequences
(Kassem Ahmad, Bassem Bakhache, Safwan El Assad, Daniel Caragata, Maryline Chetto) 97 - 102

Workshop 3:
Cloud Applications and Security (CAS’11)

A Secure Public Cloud Storage System
(SeongHan Shin, Kazukuni Kobara, Hideki Imai) 103 - 109

Dynamics of Trust in Clouds — Challenges and Research Agenda
(Imad Abbadi, Cornelius Namiluko) 110 - 115

Secured Virtual Diffused File System for the Cloud
(Kheng Kok Mar) 116 - 121

A Parameterized RBAC Access Control Model for WS-BPEL Orchestrated Composite Web Services
(Nezar Nassr, Eric Steegmans) 122 - 127

Research, Design and Development Review of the Cloud Computing Management System
(CCMS)
(Glyn Hughes, Dhiya Al-Jumeily, Abir J Hussain) 128 - 131

Security Concerns for Cloud Computing in Aircraft Data Networks
(Nitha Rachel Suresh, Suresh Mathew) 132 - 136

Workshop 4:
International Workshop on Distributed Systems: Security, Privacy and Trust Challenges
(DS: SPT -2011)

A Novel Key Establishment Scheme for Wireless Sensor Networks Based on Complex Network Synchronization
(Bo Mi, Jianqiu Cao) 137 - 141

Two Algorithms for Network Security Gradient Marking
(Xin Hu, Yonglin Sun, Yongjun Wang, Zhanrui Ren, Jie Liu) 142 - 147

A Decentralized Access Control Mechanism Using Authorization Certificate for Distributed File Systems
(Jumpei Arakawa, Koichi Sasada) 148 - 153

A Survey on Space-Time & High-Rate Redundant
(Majid Bavafa, Zahra Taheri Hanjani, Neda Navidi) 154 - 158

A New Perspective of Network Vulnerability Analysis Using Network Security Gradient
(Yonglin Sun, Yongjun Wang, Xin Hu, Zhanrui Ren, Jie Liu) 159 - 163
Automated Trust Negotiation in Identity Federations Using OWL-based Abduction of Missing Credentials  
(Martin Kuba)

Session 2
InfoSecurity: Biometrics

An Automated System for Fingerprint Classification Using Singular Points for Biometric Security  
(Anam Tariq, M. Usman Akram, Shoab A. Khan)

Handwriting Dynamics as a Means of Authentication  
(Pavel Lozhnikov, Oksana Chernikova)

Retinal Recognition: Personal Identification Using Blood Vessels  
(Muhammad Usman Akram, Anam Tariq, Shoab A. Khan)

Fingerprint Templates with High Recognition Accuracy and High Security Generated by Discrete Fractional Sine Transform  
(Hiroyuki Yoshimura)

Dorsal Hand Vein Biometric Using Independent Component Analysis (ICA)  
(Maleika Heenaye-Mamode Khan, Naushad Mamode Khan)

Multiple SEIMCHA: Multiple SEmantic IMage CAPTCHA  
(Maryam Mehrnejad, Abbas Ghaemi Bafghi, Ahad Harati, Ehsan Toreini)

Workshop 2:  

Study of the Robustness of an Enhanced CSK System by Using the Extended Kalman Filter  
(Léa Dominique Cot, Christian Bès)

FPGA Implementation of Cellular Automata Based Encryption Algorithm for Internet Communications  
(Petre Anghelescu, Silviu Ionita, Vasile-Gabriel Iana)

Security Threats in Cloud Computing  
(Farhan Bashir Shaikh, Sajjad Haider)

Low Complexity High Security Image Encryption Based on Nested PWLCM Chaotic Map  
(Hadi Abdlrudha, Qassim Nasir)

An Efficient and Secure SPN Cryptosystem Based on Chaotic Control Parameters  
(Hassan Noura, Safwan El Assad, Calin Vladeanu, Daniel Caragata)

An EAP ID-Based Authentication Method for Wireless Networks  
(Aymen Boudguiga, Maryline Laurent)

Session 3:  
IntAppTech Session: Internet Architecture

Hop Count Variability  
(Ayman Mukaddam, Imad H Elhajj)

Mailbook: A Social Network Against Spamming  
(Dimitris Zisiadis, Spyros Kopsidas, Argyris Varalis, Leandros Tassiulas)
Designing a Hierarchical DHCP Server's Model to Automatically Provide Dedicated IP Address Anywhere in the World with Mobility
(Asjad Amin, Haseeb Ahmed, Abubakar Rafique, Muhammad Junaid Nawaz, Muhammad Salahudin, Zulfiqar Ahmed)

Toward an Abstract Language on Top of XACML for Web Services Security
(Azzam Mourad, Hadi Otrok, Hamdi Yahyaoui, Lama Baajour)

A Thin Client Application Development Using OCL and Conceptual Schema
(Jane Saetent, Nattawut Vejkanchana, Suphamit Chittayasothorn)

Dynamically Complex System Using Adaptive Simulation for Interconnected Nodes
(Ramez Shamseldin)

Session 4:
InfoSec: Secure Communications

Reed-Muller Decoder with Associative Memories
(Laurentiu Ionescu, Constantin Anton, Ion Tutanescu, Alin Mazare, Gheorghe Serban)

UMTS Security: Enhancement of Identification, Authentication and Key Agreement Protocols
(Daniel Caragata, Safwan El Assad, Charles Shoniregun, Galyna Akmayeva)

A Record Composition/Decomposition Attack on the NDEF Signature Record Type Definition
(Muhammad Qasim Saeed, Colin Walter)

Texture Analysis-Based Image Spam Filtering
(Basheer N. Al-Duwairi, Ismail Khater, Omar M Al-Jarrah)

Critical Infrastructure Protection Through Distributed Reactive Demand-Side Management
(Hanno Hildmann, Sébastien Nicolas, Fabrice Saffre)

Secure Delay-Tolerant Communications in the Presence of Oppressive Governments
(Soulaf Saab, Wassim Itani, Ayman Kayssi, Ali Chehab, Cesar Ghali)

Workshop 2:

Mobile Adhoc Networks: A Simulation Based Security Evaluation and Intrusion Prevention
(Maitha Salem Al Mazrouei, Sundaravalli Narayanaswami)

Securing Information Systems in Airports: A Practical Approach
(Arben Asllani, Amjad Ali)

Synchronization of Sigma Delta Modulators
(Georgi Tsenov, Valeri M. Mladenov, Ina Taralova)

Towards an Automatic Exploit Pipeline
(Jared D. DeMott, Richard J. Enbody, William F. Punch)

Immunizing the SAODV Protocol Against Routing Information Disclosure
(Ayman Hanafy, Sherif Noureldin, Marianne Azer)

A Novel Method in Fuzzy Data Clustering Based on Chaotic PSO
(Ehsan Toreini, Maryam Mehrnejad)
Session 5:
**Ubi & Cloud Computing: Distributed Information Systems**

Proximity Aware Overlays in Peer-to-Peer Networks  
(Tina Francis)  
341 - 344

Performance Evaluation of Popular Cloud IaaS Providers  
(Khaled Salah, M. Al-Saba, M. Akhdhor, O. Shaaban, M.I. Buhari)  
345 - 349

Insiders Analysis in Cloud Computing Focusing on Home Healthcare System  
(Imad Abbadi, Cornelius Namiluko, Andrew Martin)  
350 - 357

Evaluation of Popular Application Sandboxing  
(Faisal Al Ameiri, Khaled Salah)  
358 - 362

Mobile Arabic Sign Language  
(Faisal Al Ameiri, Mohamed Jamal Zemerly, Mohamed Al Marzouqi)  
363 - 367

Key Complication Procedure In Data Driven Ciphers Based on Controlled Substitution-Permutation Networks  
(George S. Oreku)  
368 - 372

Session 6:  
**IntAppTech Session: Database and Knowledge Management**

Using Keystroke-Level Model to Analyze IOS Optimization Techniques  
(Umm-e-Laila, Syed Zain Ali Shah, Nadia Ishaque)  
373 - 377

The Challenges of Arabic Language Use on the Internet  
(Noora Albalooshi, Nader Mohamed, Jameela Al-Jaroodi)  
378 - 382

Design and Implementation of the Geo-Context Engine for Semantic Social Media Service  
(Jong-Hoon Lee, Jung Tae Kim, Hoon-Ki Lee, Eui-Hyun Paik)  
383 - 387

The Process of Summarization in the Pre-Processing Stage in Order to Improve Measurement of Texts When Clustering  
(Marcus Vinicius Guelpeli, Ana Cristina Garcia, António Horta Branco)  
388 - 395

Real-Time Scheduling for Energy Harvesting Sensors  
(Maryline Chetto, Hussein EL Ghorr, Rafic Hage Chehade)  
396 - 402

A Process Framework for Securing an e-Learning Ecosystem  
(Ponnappu Lakshmi Eswari)  
403 - 407

Session 7:  
**InfoSec: Cyber Security**

A Distributed Virtual Laboratory Architecture for Cybersecurity Training  
(Christian Willems, Thomas Klingbeil, Lukas Radvilavicius, Antanas Cenys, Christoph Meinel)  
408 - 415

Mitigation of Spear Phishing Attacks: A Content-Based Authorship Identification Framework  
(Mahmoud Khonji, Youssef Iraqi, Andrew Jones)  
416 - 421

Lexical URL Analysis for Discriminating Phishing and Legitimate E-Mail Messages  
(Mahmoud Khonji, Youssef Iraqi, Andrew Jones)  
422 - 427

Users' Perceptions on Mobile Devices Security Awareness in Malaysia  
(Ahmed A. Sabeeh, Arash Habibi Lashkari)  
428 - 435
Propagation of Trust and Confidence Using Intervals
(Hassan Shakeri, Abbas Ghaemi Bafghi) 436 - 441

Trapping and Analyzing Malicious VoIP Traffic Using a Honeynet Approach
(Markus Gruber, Florian Fankhauser, Stefan Taber, Christian Schanes, Thomas Grechenig) 442 - 447

Session 8:
MultiMedia Session: Security and Intelligent Services

Access Control and Content Authentication for Hybrid DVB-T2/P2P Broadcasting
(Jens Hasselbach, Patrick Aichroth) 448 - 453

(Pradhumna Lal Shrestha, Michael Hempel, Tao Ma, Dongming Peng, Hamid Sharif) 454 - 459

An Effective Hybrid Thresholding Technique for Degraded Documents Images Binarization
(Mohamed Zayed, Asma Ouari, Meriem Derraschouk, Youcef Chibani) 460 - 465

Pro-Active Multi-Agent Recommender System for Travelers
(Hend Al Tair, Mohamed Jamal Zemerly, Mahmoud Al-Quatayri, Marcello Leida) 466 - 471

A Policy Based Access Control Model for Web Services
(Hadise Seyyed Alipour, Mehdi Sabbari, Eslam Nazemi) 472 - 477

A Framework of VI-based Ranking and Recommendation of Web Services
(Gang Wang, Kunming Nie) 478 - 483

Session 9:
RISC Session (Part 1)

Ownership Transfer Protocol for RFID Objects Using Lightweight Computing Operators
(Nai-Wei Lo, Shiou-Huei Ruan, Tzong-Chen Wu) 484 - 489

A Study on RFID Code Structure for Traceability System of Electric Vehicle Batteries
(Woo Ram Kim, Yoon Seok Chang) 490 - 494

A PUF-Based Ultra-Lightweight Mutual-Authentication RFID Protocol
(Ramzi Bassil, Wissam El-Beaino, Ayman Kayssi, Ali Chehab) 495 - 499

Vulnerabilities in a New RFID Access Control Protocol
(Masoumeh Safkhani, Nasour Bagheri, Majid Naderi) 500 - 503

A Decentralized Energy-Aware Key Management Scheme for Wireless Sensor Networks
(Salwa Adriana Saab, Ayman Kayssi, Ali Chehab) 504 - 508

Implementation of a Modified Lightweight Cryptographic TEA Algorithm in RFID System
(Mohamed B Abdelhalim, Mohamed El-Mahallawy, Mohammad Ayyad, Adel Elhennawy) 509 - 513

Session 10:
Ubi & Cloud Computing: Novel Mechanisms and Applications

Encrypted Processes for Oblivious Data Retrieval
(Youssef Gahi, Mouhcine Guennoun, Zouhair Guennoun, Khalil El-Khatib) 514 - 518

Demand-Side Management for Air Conditioning
(Hanno Hildmann, Sébastien Nicolas, Fabrice Saffre) 519 - 524
2-Phase Optimization Method for Energy Efficient Scheduling of Virtual Machines in Cloud Data Centers
(Mohammad Moein Taheri, Kamran Zamanifar)

Context-Aware Real-Time Framework for Local Collaboration
(Kris Scott, Rachid Benlamri)

Virtual Cloud: Rent Out the Rented Resources
(Shereyar Malik, Fabrice C. Huet)

Performance Evaluation of Relative Positioning Based on Low-cost GPS and VANET
(Hun-Jung Lim, Tai-Myoung Chung)

Session 11:
IntAppTech Session: AI

A MILP Based Design Tool for FTTH Access Networks with Consideration of Demand Growth
(Kin Fai Poon, Anis Ouali)

Behavioural Game AI - a Theoretical Approach
(Hanno Hildmann)

Evaluating USARsim for Use in Fire Search and Rescue
(Amina AlDahak AlShamsi, Mohamed AlMarzouqi and Lakmal Seneviratne)

An Application of Imperialist Competitive Algorithm to Solve the Quadratic Assignment Problem
(Ali Safari Mamaghani, Mohammad Reza Meybodi)

An Economical Mechanism for Multicasting of Content Among Servers of Hybrid CDN-P2P Networks
(Mehran Garmehi, Morteza Analoui)

Policy Rule-Sets for Policy Based Systems
(Abdur Rahim Choudhary)

Session 12:
InfoSec: Privacy and Data Security

Formal Modeling and Verification of DLK Protocol
(Hussam Al-Hamadi, Chan Yeob Yeun, Mohamed Jamal Zemerly, Mahmoud Al-Qutayri, Amjad Gawanmeh)

Privacy Enabled Web Service Access Control Using SAML and XACML for Home Automation Gateways
(Markus Jung, Georg Kienesberger, Wolfgang Granzer, Martin Unger, Wolfgang Kastner)

Automated Healthcare Information Privacy and Security: UAE Case
(Mohamed Zineddine)

Segmentation Based Encryption Method for Medical Images
(Ahmed Mahmood, Robert D. Dony)

Privacy Requirements Specification for Digital Identity Management Systems Implementation:
Towards a Digital Society of Privacy
(Ghazi Ben Ayed, Solange Ghernaouti Hélie)

Encoding Default-Based SELinux-security Policy in Organization-Based Access Control Model
(Salem Benferhat, Khalid Bouriche, Mohamed Ouzarf)

Solutions to Security Issues with Legacy Integration of GSM Into UMTS
(Eric Southern, Abdellaker Ouda, Abdallah Shami) 614 - 619

A Real-Time Traffic Classification Approach
(Eduardo Rocha, Paulo Salvador, Antônio Nogueira) 620 - 626

Network Behaviour Anomaly Detection Using Holt-Winters Algorithm
(Jarkko Ekberg, Jorma Ylinen, Pekka Loula) 527 - 631

Security-Functionality Tradeoffs in IP Transition Phase
(Tomasz Bilski) 632 - 638

A Note on Modified SET Protocol for Mobile Payment
(Devendra Mani Tripathi) 639 - 641

Modeling and Verification of Firewall Configurations Using Domain Restriction Method
(Amjad Gawanmeh, Sofiene Tahar) 642 - 647

Session 14: MultiMedia Session: Web Mining and Information Systems

Design and Implementation of a Web Structure Mining Algorithm Using Breadth First Search Strategy for Academic Search Application
(Sivaramakrishnan Jeyalatha, B Vijayakumar) 648 - 654

Location-based Personalized Social Media Service for the Smart Phone: Distributed Social Contents Sharings
(Jung Tae Kim, Jong-Hoon Lee, Hoon-Ki Lee, Eui-Hyun Paik) 655 - 659

XSLT Transformation Generating OWL Ontologies Automatically Based on XML Schemas
(Thomas Bosch, Brigitte Mathiak) 660 - 667

Modified Run Length Encoding Scheme with Introduction of Bit Stuffing for Efficient Data Compression
(Ajaj Amin, Haseeb Ahmad Qureshi, Muhammad Junaid, Muhammad Yasir Habib, Waqas Anjum) 668 - 672

An Agent-Based Modeling Approach for Decision-Making in Gravity Irrigation Systems
(Salwa Belaqziz, Abdelaziz El Fazziki, Mohamed Eladnani, Michel Le Page) 673 - 680

Identity Management Architecture for Integrated Personalized Service on TV
(Chigusa Yamamura, Kazuhiro Otsuki, Arisa Fujii, Kiyohiko Ishikawa) 681 - 682

Session 15: RISC Session (Part 2)

On the Privacy of Two Tag Ownership Transfer Protocols for RFIDs
(Mohammad Reza Sohizadeh Abyaneh) 683 - 688

Security Analysis of LMAP++, an RFID Authentication Protocol
(Masoume Safkhani, Nasour Bagheri, Majid Naderi, Somitra Kumar Sanadhya) 689 - 694

Redundant Reader Elimination for Directional Antenna in RFID Systems
(Nazish Irfan, Mustapha C.E. Yagoub, Khalifa Hettak) 695 - 700
Session 16:
Infonomics Session: e-Commerce, e-Society, e-Government

Technologies Enabling Sustainability in the Built Environment
(Mahmoud Alahmad, Muhammad Zulfiqar, Hosen Hasna, Timothy Wisnieski, Nasser Aljuhaishi, Hamid Sharif)  
Desktop Search Engines - a State of the Art Comparison
(Bernd Markscheffel, Daniela Büttner, Daniel Fischer)  
A-CitizenMobile: A Case Study for Blind Users
(Flávio Dumortout de Mendonça Junior, Daniela Gorski Trevisan, Thiago Cortat Tavares, José Luiz Nogueira)  
Education Beyond the Cloud: Anytime-anywhere Learning in a Smart Campus Environment
(Benjamin Hirsch, Jason W.P. Ng)  
The use of detection systems to improve the quality of the Italian Public Administration
(Arianna Del Soldato, Pasquale Lazzareschi, Maurizio Martinelli, Giuseppe Vasarelli)  
E-banking in Morocco: Study of Some Specifying Factors
(Hicham Sadok)

Session 17:
InfoSec: Privacy and Data Security & Organization

SeKMAC: A Secure Model for Key Management and Access Control in Cryptographic File System
(Farshad Rahimiasl, Reza Azmi)  
Systematic Literature Review of Virtual Role
(Sami Noponen, Jarno Salonen, Hanna-Miina Sihvonen, Taina Kurki)  
An Event Pattern Language for Runtime Monitoring Based on AOP
(Xian Zhang, Martin Leucker, Wei Dong)  
Extrapolating Security Requirements to an Established Software Process: Version 1.0
(Galah Rashidah Haron, Ng Kang Siong)  
Temporal Context in Multilevel Access Control Model
(Narfimene Boustia, Aicha Mokhtari)  
Trust-Based Access Control for XML Databases
(Norah Farooqi, Siobhán North)

Session 18:
InfoSec: MANET and Forensics

Digital Forensics Education in UAE
(Hanan Yousef Al Obaidli, Asif Iqbal)  
Forensic Artifacts of Facebook's Instant Messaging Service
(Noora Al Mutawa, Ibtesam Al Awadh, Ibrahim Baggili, Andrew Marrington)  
Quaternary Privacy-Levels Preservation in Computer Forensics Investigation Process
(Waleed Halboob, Muhammad Abulaish, Khaled S. Alghathbar)  
A Robust Watermarking Scheme for Relational Databases
(Theodoros Tzouramanis)
Performance Assessment of OLSR Protocol Under Routing Attacks
(Mahmood Salehi, Hamed Samavati, Mehdi Dehghan)

791 - 796

Concurrent Realization of the Multiply-By-7 Elliptic Curve Scalar Multiplication Algorithm
(Michael Naseimo Daikpor, Olouwole Adegbenro)

797 - 804