2011 International Conference for Internet Technology and Secured Transactions

(ICITST 2011)

Abu Dhabi, United Arab Emirates
11 – 14 December 2011

IEEE Catalog Number: CFP1181I-PRT
ISBN: 978-1-4577-0884-8

Table of Contents

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

Hardware Implementations of Elliptic Curve Cryptography in Wireless Sensor Networks 1 - 6
(Hilal Houssain, Mohamad Badra, Turki F. Al-Somani)

Implementation of GF(2m) Elliptic Curve Cryptoprocessor on a Nano FPGA 7 - 12
(Turki F. Al-Somani, Hilal Houssain)

A Unified Countermeasure Against Side Channel Attacks on Cryptographic RFID 13 - 18
(Hamad Marzouqi, Mahmoud Al-Qutayri, Chan Yeob Yeun)

Forensics and War-Driving on Unsecured Wireless Network 19 - 24
(Huwida Said, Mario Guimaraes, Noora Al Mutawa, Ibtesam Al Awadhi)

FPGA Implementation of High Speed XTS-AES for Data Storage Devices 25 - 28
(Mohamed Elmoghany, Mohamed Diab, Moustafa Kassem, Mustafa Khairallah, Omar El Shahat, Wael Sharkasy)

The Use of Boolean Functions in Stream Ciphers 29 - 33
(Muna Al Shehhi, Joonsang Baek, Chan Yeob Yeun)

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

On the Security of Inclusion or Omission of MixColumns in AES Cipher 34 - 39
(Khalfan AlMarashda, Yousuf AlSalami, Khaled Salah, Thomas Martin)

Study on Secret Sharing Schemes (SSS) and Their Applications 40 - 45
(Noura Al Ebri, Joonsang Baek, Chan Yeob Yeun)

Survey on Computationally Hard Problems and Their Applications to Cryptography 46 - 52
(Ameera Abdouli, Joonsang Baek, Chan Yeob Yeun)

Survey on Certificateless Public Key Cryptography 53 - 58
(Hajer Al Housani, Joonsang Baek, Chan Yeob Yeun)

Anonymous Electronic Voting Protocol with Traceability 59 - 66
(Lezhen Ling, Junguo Liao)

Session 1
InfoSecurity: Virtualization and Chaos

Understanding the Security Challenges of Virtualized Environments 67 - 72
(Fatma Ahmad Bazargan, Chan Yeob Yeun, Mohamed Jamal Zemerly)

Synchronization Recovery of Chaotic Signal Through Imperfect Channel Using Optimization Approach 73 - 78
(Amr Sayed Abdel Fattah, Salwa Elramly, Magdy Ibrahim, Ahmed A. Abdel-Hafez)

Denoising Algorithm for Noisy Chaotic Signal by Using Wavelet Transform: Comprehensive Study 79 - 85
(Amr Sayed Abdel Fattah, Salwa Elramly, Magdy Ibrahim, Ahmed A. Abdel-Hafez)

Workshop 2:
International Workshop on Information Security, Theory and Practice (ISTP-2011) (Part 1)

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

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

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

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

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

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

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

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

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

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

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 137 - 141
(Bo Mi, Jianqiu Cao)

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

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

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

A New Perspective of Network Vulnerability Analysis Using Network Security Gradient 159 - 163
(Yonglin Sun, Yongjun Wang, Xin Hu, Zhanrui Ren, Jie Liu)

Automated Trust Negotiation in Identity Federations Using OWL-based Abduction of Missing Credentials 164 - 169
(Martin Kuba)

Session 2
InfoSecurity: Biometrics

An Automated System for Fingerprint Classification Using Singular Points for Biometric Security 170 - 175
(Anam Tariq, M. Usman Akram, Shoab A. Khan)

Handwriting Dynamics as a Means of Authentication 176 - 179
(Pavel Lozhnikov, Oksana Chernikova)

Retinal Recognition: Personal Identification Using Blood Vessels 180 - 184
(Muhammad Usman Akram, Anam Tariq, Shoab A. Khan)

Fingerprint Templates with High Recognition Accuracy and High Security Generated by Discrete Fractional Sine Transform 185 - 190
(Hiroyuki Yoshimura)

Dorsal Hand Vein Biometric Using Independent Component Analysis (ICA) 191 - 195
(Maleika Heenaye-Mamode Khan, Naushad Mamode Khan)

Multiple SEIMCHA: Multiple SEmantic IMage CAPTCHA 196 - 201
(Maryam Mehrnejad, Abbas Ghaemi Bafghi, Ahad Harati, Ehsan Toreini)

Workshop 2:
International Workshop on Information Security, Theory and Practice (ISTP-2011) (Part 2)

Study of the Robustness of an Enhanced CSK System by Using the Extended Kalman Filter 202 -207
(Léa Dominique Cot, Christian Bès)

FPGA Implementation of Cellular Automata Based Encryption Algorithm for Internet Communications 208 - 213
(Petre Anghelescu, Silviu Ionita, Vasile-Gabriel Iana)

Security Threats in Cloud Computing 214 - 219
(Farhan Bashir Shaikh, Sajjad Haider)

Low Complexity High Security Image Encryption Based on Nested PWLCM Chaotic Map 220 - 225
(Hadi Abdlrudha, Qassim Nasir)

An Efficient and Secure SPN Cryptosystem Based on Chaotic Control Parameters 226 - 231
(Hassan Noura, Safwan El Assad, Calin Vladeanu, Daniel Caragata)

An EAP ID-Based Authentication Method for Wireless Networks 232 - 239
(Aymen Boudguiga, Maryline Laurent)

Session 3:
IntAppTech Session: Internet Architecture

Hop Count Variability 240 - 244
(Ayman Mukaddam, Imad H Elhajj)

Mailbook: A Social Network Against Spamming 245 - 249
(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 250 - 253
(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 254 - 259
(Azzam Mourad, Hadi Otrok, Hamdi Yahyaoui, Lama Baajour)

A Thin Client Application Development Using OCL and Conceptual Schema 260 - 265
(Jane Saetent, Nattawut Vejkanchana, Suphamit Chittayasothorn)

Dynamically Complex System Using Adaptive Simulation for Interconnected Nodes 266 - 273
(Ramez Shamseldin)

Session 4:
InfoSec: Secure Communications

Reed-Muller Decoder with Associative Memories 274 - 277
(Laurentiu Ionescu, Constantin Anton, Ion Tutanescu, Alin Mazare, Gheorghe Serban)

UMTS Security: Enhancement of Identification, Authentication and Key Agreement Protocols 278 - 282
(Daniel Caragata, Safwan El Assad, Charles Shoniregun, Galyna Akmayeva)

A Record Composition/Decomposition Attack on the NDEF Signature Record Type Definition 283 - 287
(Muhammad Qasim Saeed, Colin Walter)

Texture Analysis-Based Image Spam Filtering 288 - 293
(Basheer N. Al-Duwairi, Ismail Khater, Omar M Al-Jarrah)

Critical Infrastructure Protection Through Distributed Reactive Demand-Side Management 294 - 301
(Hanno Hildmann, Sébastien Nicolas, Fabrice Saffre)

Secure Delay-Tolerant Communications in the Presence of Oppressive Governments 302 - 307
(Soulaf Saab, Wassim Itani, Ayman Kayssi, Ali Chehab, Cesar Ghali)

Workshop 2:
International Workshop on Information Security, Theory and Practice (ISTP-2011) (Part 3)

Mobile Adhoc Networks: A Simulation Based Security Evaluation and Intrusion Prevention 308 - 313
(Maitha Salem Al Mazrouei, Sundaravalli Narayanaswami)

Securing Information Systems in Airports: A Practical Approach 314 - 318
(Arben Asllani, Amjad Ali)

Synchronization of Sigma Delta Modulators 319 - 322
(Georgi Tsenov, Valeri M. Mladenov, Ina Taralova)

Towards an Automatic Exploit Pipeline 323 - 329
(Jared D. DeMott, Richard J. Enbody, William F. Punch)

Immunizing the SAODV Protocol Against Routing Information Disclosure 330 - 334
(Ayman Hanafy, Sherif Noureldin, Marianne Azer)

A Novel Method in Fuzzy Data Clustering Based on Chaotic PSO 335 - 340
(Ehsan Toreini, Maryam Mehrnejad)

Session 5:
Ubi & Cloud Computing: Distributed Information Systems

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

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

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

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

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

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

Session 6:
IntAppTech Session: Database and Knowledge Management

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

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

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

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

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

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

Session 7:
InfoSec: Cyber Security

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

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

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

Users' Perceptions on Mobile Devices Security Awareness in Malaysia 428 - 435
(Ahmed A. Sabeeh, Arash Habibi Lashkari)

Propagation of Trust and Confidence Using Intervals 436 - 441
(Hassan Shakeri, Abbas Ghaemi Bafghi)

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

Session 8:
MultiMedia Session: Security and Intelligent Services

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

A General Attack Method for Steganography Removal Using Pseudo-CFA Re-interpolation 454 - 459
(Pradhumna Lal Shrestha, Michael Hempel, Tao Ma, Dongming Peng, Hamid Sharif)

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

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

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

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

Session 9:
RISC Session (Part 1)

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

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

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

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

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

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

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

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

Demand-Side Management for Air Conditioning 519 - 524
(Hanno Hildmann, Sébastien Nicolas, Fabrice Saffre)

2-Phase Optimization Method for Energy Efficient Scheduling of Virtual Machines in Cloud Data Centers 525 - 530
(Mohammad Moein Taheri, Kamran Zamanifar)

Context-Aware Real-Time Framework for Local Collaboration 531 - 535
(Kris Scott, Rachid Benlamri)

Virtual Cloud: Rent Out the Rented Resources 536 - 541
(Sheheryar Malik, Fabrice C. Huet)

Performace Evaluation of Relative Positioning Based on Low-cost GPS and VANET 542 - 543
(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 544 - 549
(Kin Fai Poon, Anis Ouali)

Behavioural Game AI - a Theoretical Approach 550 - 555
(Hanno Hildmann)

Evaluating USARsim for Use in Fire Search and Rescue 556 - 561
(Amna AlDahak AlShamsi, Mohamed AlMarzouqi and Lakmal Seneviratne)

An Application of Imperialist Competitive Algorithm to Solve the Quadratic Assignment Problem 562 - 565
(Ali Safari Mamaghani, Mohammad Reza Meybodi)

An Economical Mechanism for Multicasting of Content Among Servers of Hybrid CDN-P2P Networks 566 - 571
(Mehran Garmehi, Morteza Analoui)

Policy Rule-Sets for Policy Based Systems 572 - 577
(Abdur Rahim Choudhary)

Session 12:
InfoSec: Privacy and Data Security

Formal Modeling and Verification of DLK Protocol 578 - 583
(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 584 - 591
(Markus Jung, Georg Kienesberger, Wolfgang Granzer, Martin Unger, Wolfgang Kastner)

Automated Healthcare Information Privacy and Security: UAE Case 592 - 595
(Mhamed Zineddine)

Segmentation Based Encryption Method for Medical Images 596 - 601
(Ahmed Mahmood, Robert D. Dony)

Privacy Requirements Specification for Digital Identity Management Systems Implementation: Towards a Digital Society of Privacy 602 - 607
(Ghazi Ben Ayed, Solange Ghernaouti Hélie)

Encoding Default-Based SELinux-security Policy in Organization-Based Access Control Model 608 - 613
(Salem Benferhat, Khalid Bouriche, Mohamed Ouzarf)

Session 13:
InfoSec: Network Security Issues and Protocols

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

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

Network Behaviour Anomaly Detection Using Holt-Winters Algorithm 627 - 631
(Jarkko Ekberg, Jorma Ylinen, Pekka Loula)

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

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

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

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 648 - 654
(Sivaramakrishnan Jeyalatha, B Vijayakumar)

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

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

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

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

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

Session 15:
RISC Session (Part 2)

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

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

Redundant Reader Elimination for Directional Antenna in RFID Systems 695 - 700
(Nazish Irfan, Mustapha C.E. Yagoub, Khalifa Hettak)

Session 16:
Infonomics Session: e-Commerce, e-Society, e-Government

Technologies Enabling Sustainability in the Built Environment 701 - 706
(Mahmoud Alahmad, Muhammad Zulfiqar, Hosen Hasna, Timothy Wisnieski, Nasser Aljuhaishi, Hamid Sharif)

Desktop Search Engines - a State of the Art Comparison 707 - 712
(Bernd Markscheffel, Daniela Büttner, Daniel Fischer)

A-CitizenMobile: A Case Study for Blind Users 713 - 717
(Flávio Dumortout de Mendonça Júnior, Daniela Gorski Trevisan, Thiago Cortat Tavares, José Luiz Nogueira)

Education Beyond the Cloud: Anytime-anywhere Learning in a Smart Campus Environment 718 - 723
(Benjamin Hirsch, Jason W.P. Ng)

The use of detection systems to improve the quality of the Italian Public Administration 724 - 725
(Arianna Del Soldato, Pasquale Lazzareschi, Maurizio Martinelli, Giuseppe Vasarelli)

E-banking in Morocco: Study of Some Specifying Factors 726 - 731
(Hicham Sadok)

Session 17:
InfoSec: Privacy and Data Security & Organization

SeKMAC: A Secure Model for Key Management and Access Control in Cryptographic File System 732 - 737
(Farshad Rahimiasl, Reza Azmi)

Systematic Literature Review of Virtual Role 738 - 743
(Sami Noponen, Jarno Salonen, Hanna-Miina Sihvonen, Taina Kurki)

An Event Pattern Language for Runtime Monitoring Based on AOP 744 - 751
(Xian Zhang, Martin Leucker, Wei Dong)

Extrapolating Security Requirements to an Established Software Process: Version 1.0 752 - 757
(Galoh Rashidah Haron, Ng Kang Siong)

Temporal Context in Multilevel Access Control Model 758 - 763
(Narhimene Boustia, Aicha Mokhtari)

Trust-Based Access Control for XML Databases 764 - 765
(Norah Farooqi, Siobhán North)

Session 18:
InfoSec: MANET and Forensics

Digital Forensics Education in UAE 766 - 770
(Hanan Yousef Al Obaidli, Asif Iqbal)

Forensic Artifacts of Facebook's Instant Messaging Service 771 - 776
(Noora Al Mutawa, Ibtesam Al Awadhi, Ibrahim Baggili, Andrew Marrington)

Quaternary Privacy-Levels Preservation in Computer Forensics Investigation Process 777 - 782
(Waleed Halboob, Muhammad Abulaish, Khaled S. Alghathbar)

A Robust Watermarking Scheme for Relational Databases 783 - 790
(Theodoros Tzouramanis)

Performance Assessment of OLSR Protocol Under Routing Attacks 791 - 796
(Mahmood Salehi, Hamed Samavati, Mehdi Dehghan)

Concurrent Realization of the Multiply-By-7 Elliptic Curve Scalar Multiplication Algorithm 797 - 804
(Michael Naseimo Daikpor, Olouwole Adegbenro)