

Communications Security Conference

(CSC 2014)

IET Conference Publications 653

**Beijing, China
22-24 May 2014**

ISBN: 978-1-63439-592-2

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2014) by the Institution of Engineering and Technology
All rights reserved.

Printed by Curran Associates, Inc. (2015)

For permission requests, please contact the Institution of Engineering and Technology
at the address below.

Institution of Engineering and Technology
P. O. Box 96
Stevenage, Hertfordshire
U.K. SG1 2SD

Phone: 01-441-438-767-328-328
Fax: 01-441-438-767-328-375

www.theiet.org

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2634
Email: curran@proceedings.com
Web: www.proceedings.com

TABLE OF CONTENTS

2014.0726: The Evaluation of Complex Networks' Robustness Based on Entropy Measure	1
<i>Y. Jiang, A.Q. Hu, Y.B. Song</i>	
2014.0727: An Improved Kademlia Protocol with Double-Layer Design for P2P Voice Communications	6
<i>Liquan Chen, Wee Seng Soh, Aiqun Hu</i>	
2014.0728: Detecting Hardware Trojan Through Heuristic Partition and Activity Driven Test Pattern Generation	14
<i>Xue Mingfu, Hu Aiqun, Li Guyue</i>	
2014.0729: Reverse Analysis of Secure Communication Protocol Based on Taint Analysis	20
<i>Meijian Li, Yongjun Wang, Zhijian Huang</i>	
2014.0730: A Detection System of Android Application Based on Permission Analysis	28
<i>Jinxin Zhang, Xiaohui Yang, Tao Li, Jiamin Bao</i>	
2014.0731: The Analysis and Design for a Network Protocol Analysis System Based on WinPcap	34
<i>Lili Jiang, Xiaohui Yang, Tao Li</i>	
2014.0732: Mobile Trusted Hierarchical Model and Its Applications	38
<i>Li Tao, Hu Aiqun</i>	
2014.0733: PVDF: An Automatic Patch-Based Vulnerability Description and Fuzzing Method	46
<i>Sha letian, Fu Jianming, Chen Jing, Peng Guojun</i>	
2014.0734: A Robust DWT-SVD Blind Watermarking Algorithm based on Zernike Moments	54
<i>Ye Xueyi, Deng Meng, Wang Yunlu, Zhang Jing</i>	
2014.0735: Improved Arbitrated Quantum Signature Scheme Using Bell States	60
<i>Chao Wang, Xiao Liu, Jianwei Liu, Tao Shang, Xiubo Chen</i>	
2014.0736: Implementation of Automated Testing System for Android Applications Based on Dynamic Taint Propagation	66
<i>Zhu Kelong, Song Yubo, Chen Fei</i>	
2014.0737: Certificateless and Pairing-free Key Agreement Scheme for Satellite Network	71
<i>D. Tong, J.W. Liu, K.F. Mao, L. Zhang</i>	
2014.0738: An Approach to Resist Blind Source Separation Attacks of Speech Signals	76
<i>Guyue Li, Aiqun Hu</i>	
2014.0739: Android PBC: A Pairing Based Cryptography Toolkit for Android Platform	83
<i>Weiran Liu, Jianwei Liu, Qianhong Wu, Bo Qin</i>	
2014.0740: A Versatile Cryptographic Toolkit for Flexible Access Control	89
<i>Weiran Liu, Xiao Liu, Qianhong Wu, Bo Qin, Yunya Zhou</i>	
2014.0741: Optimistic Fair Exchange of Distributed Signatures	95
<i>Yujue Wang, Qianhong Wu, D.S. Wong, Bo Qin, Jianwei Liu, Jian Mao</i>	
2014.0742: ETCIC: An Error-Tolerant Content Integrity Checking Scheme in Multi-Cloud Storing	101
<i>Jian Mao, Yan Zhang, Pei Li, Xiangdong Xu, Teng Li, Jianwei Liu</i>	
2014.0743: Enhanced Circular Quantum Secret Sharing for Remote Agents	108
<i>Chao Wang, Xiao Liu, Jianwei Liu, Xiubo Chen, Tao Shang</i>	
2014.0744: Research on Software Behavior Modeling Based on Extended Finite State Automata	114
<i>Xiaolin Zhao, Jingfeng Xue, Changzhen Hu, Rui Ma, Shanshan Zhang</i>	
2014.0745: User Revocation for Data Sharing Based on Broadcast CP-ABE in Cloud Computing	119
<i>Li Shuanbao, Fu Jianming</i>	
2014.0746: A Secure Fast Handoff Scheme with Attribute-Based Access Control for Secure Enterprise WLAN	127
<i>Meng Lv, Zhe Liu, Jianwei Liu, Qianhong Wu, Chengxiang Gong</i>	
2014.0747: A Note on Certificate-Based Encryption	133
<i>Yanfeng Qi, Chunming Tang, Maozhi Xu, Baoan Guo</i>	
2014.0748: Fuzz Testing Data Generation for Network Protocol Using Classification Tree	138
<i>Rui Ma, Wendong Ji, Changzhen Hu, Chun Shan, Wu Peng</i>	
2014.0749: Software Defect Prediction Model Based on LLE and SVM	143
<i>Chun Shan, Boyang Chen, Changzhen Hu, Jingfeng Xue, Ning Li</i>	
2014.0750: Detecting Community Structure in Trust Relationship Networks	148
<i>Jianwei Yang, Xiaolin Gui, Jian An, Feng Tian</i>	
2014.0751: Research on the Security Model of Mobile Application	153
<i>Hang Dong, Chengze Li, Ting Li, Yuejin Du, Guoai Xu</i>	

2014.0752: A White-Box CLEFIA Implementation for Mobile Devices	158
<i>Shuai Su, Hang Dong, Ge Fu, Chengpeng Zhang, Miao Zhang</i>	
2014.0753: Secure Performance of Time Reversal Precoding Technique in MISO OFDM Systems.....	166
<i>Wei Cao, Jing Lei, Wei Liu, Xiaotian Li</i>	
2014.0754: An Identity-Based Mutual Authentication with Key Agreement Scheme for Mobile Client-Server Environment	171
<i>Yanfeng Qi, Chunming Tang, Maozhi Xu, Baoan Guo</i>	
2014.0755: A Variance-Based Information Diffusion Coefficient Optimization Algorithm and Its Application in Missile Effectiveness Evaluation.....	176
<i>Li Wang, Xiaolan Tang, Longxing Kong, Libing Jiang</i>	
2014.0756: The Influence on Sensitivity of Hardware Trojans Detection by Test Vector	182
<i>Lin Ni, Shaoqing Li, Jihua Chen, Pei Wei, Zhixun Zhao</i>	
2014.0757: An Anonymous Roaming Authentication Scheme in Global Mobility Networks.....	188
<i>Kefei Mao, Jie Chen, Jianwei Liu, Dan Tong</i>	
2014.0758: A Novel Approach Using Mutual Information for Critical Nodes Detecting in Virtual Networking Environment.....	192
<i>Rongheng Lin, Peng Wang, Haimin Zheng, Yao Zhao, Hua Zou</i>	
2014.0759: Generating Verifiable Random Numbers Without a Trusted Party	198
<i>Xiao Yang, Zheng Tong, Zhe Xia, Yining Liu</i>	
2014.0760: Strongly Secure Group Signature Scheme	205
<i>Hefeng Chen, Wenping Ma, Youjiao Zou, Changxia Sun</i>	
Author Index	