

# **International Conference on Information and Network Security**

**(ICINS 2014)**

**IET Conference Publications 657**

**Beijing, China  
14-16 November 2014**

**ISBN: 978-1-5108-0428-9**

**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](http://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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

# TABLE OF CONTENTS

<b>AN IMPROVED IMAGE WATERMARKING ALGORITHM BASED ON NMF AND DWT</b> .....	1
<i>Gong Yunfeng ; Cui Delong ; Yu Guilan ; Xiong Jianbin</i>	
<b>CLUSTER SYSTEM FOR BINARY DATA FRAME</b> .....	7
<i>Yang Yue ; Yuan Liu ; Chunrui Zhang ; Fanzhi Meng</i>	
<b>ATTRIBUTE-BASED HASH PROOF SYSTEM</b> .....	12
<i>Xia Feng ; Yang Bo ; Xiang Han ; Zhou Zaihong</i>	
<b>A HIGHLY STABLE R-DIODE-BASED PHYSICAL UNCLONABLE FUNCTION</b> .....	17
<i>Chuang Bai ; Xuecheng Zou ; Kui Dai</i>	
<b>CONTENT-BASED AUDIO WATERMARKING METHOD TO RESIST DE- SYNCHRONIZATION ATTACKS</b> .....	23
<i>Cui Delong ; Li Qirui ; Yu Guilan ; Xiong Jianbin</i>	
<b>ACHIEVE DISTRIBUTED, SCALABLE AND EFFECTIVE ACCESS CONTROL IN CLOUD STORAGE SERVICES</b> .....	28
<i>Su Huang ; Yuan Luo</i>	
<b>RS ERASURE CODING REPLICA PLACEMENT STRATEGY BASED ON EDUCATION RESOURCES MANAGEMENT</b> .....	35
<i>Lin Guo ; Xiliang Li ; Guang Li</i>	
<b>AN ACHIEVABLE SECRECY CAPACITY REGION FOR MULTIPLE-ACCESS WIRETAP CHANNEL WITH COMMON MESSAGE AND SIDE INFORMATION</b> .....	42
<i>Fangbiao L ; Zhi Xue</i>	
<b>A NOVEL AUTHENTICATION PROTOCOL FOR MOBILE NODES IN MULTI-BASE-STATION WIRELESS SENSOR NETWORK</b> .....	47
<i>Zhou Zhiping ; Shao Nannan ; Zhuang Xuebo</i>	
<b>EXTENDED VISUAL CRYPTOGRAPHY SCHEME WITH ASPECT RATIO INVARIANT</b> .....	55
<i>Wanli Dang ; Mingxing He ; Daoshun Wang</i>	
<b>A SELECTION ALGORITHM FOR FIREWALL IN DISTRIBUTED ENVIRONMENT</b> .....	62
<i>Liangjia Fu ; Chunhe Xia ; Xiaochen Liu ; Jinghua Gao</i>	
<b>A FULLY SECURE IDENTITY-BASED ENCRYPTION SCHEME AGAINST CHOSEN- CIPHERTEXT ATTACK</b> .....	70
<i>Jing Ren ; Ying Gao</i>	
<b>FAST SEARCHING OPTIMAL NEGATIVE SURVEYS</b> .....	77
<i>Yihui Lu ; Wenjian Luo ; Dongdong Zhao</i>	
<b>A CHORD-BASED LOAD BALANCING ALGORITHM FOR P2P NETWORK</b> .....	86
<i>Ding Zhi-min ; Qian Quan</i>	
<b>IMPROVED CRYPTANALYTIC OF TIME-MEMORY TRADE-OFF BASED ON RAINBOW TABLE</b> .....	92
<i>Yulong Tian ; Dawu Gu ; Haihua Gu ; Ning Ding</i>	
<b>DIGITAL ENCRYPT WATERMARKING BASED ON WAVELET TRANSFORM</b> .....	100
<i>Shibing Zhang ; Yanan Wu</i>	
<b>RESEARCH ON MONITORING PROBE DEPLOYMENT IN LARGE SCALE NETWORK</b> .....	105
<i>Ming Liang ; Miao Qing ; Wang Dongxia</i>	
<b>A BINARY TREE AUTHENTICATION SCHEME BASED ON MULTI-BIOMETRICS</b> .....	110
<i>Qi Deng ; Qiuyun Lv ; Qihua Wang</i>	
<b>MULTILEVEL THRESHOLD MULTI-SECRET SHARING SCHEME BASED ON LUC PUBLIC KEY ENCRYPTION</b> .....	116
<i>Tian Zeng ; Yousheng Zhou</i>	
<b>A SECURITY ROUTING PROTOCOL OF AD HOC NETWORK BASED ON NODE TRUST EVALUTION</b> .....	122
<i>Yahui Li ; Hongwa Yang ; Fei Xie</i>	
<b>THE MP3 STEGANOGRAPHY ALGORITHM BASED ON LINBITS</b> .....	129
<i>Yakun Dong ; Ru Zhang ; Jianyi Liu ; Chenlei Cao ; Di Xiao</i>	
<b>CRYPTANALYSIS AND IMPROVEMENT OF A SMART CARD-BASED IDENTITY AUTHENTICATION SCHEME</b> .....	134
<i>Siqiong Fan ; Zhenfu Cao ; Xiaolei Dong</i>	
<b>PARTIAL SUBBLOCK WEIGHTING PTS SCHEME FOR PAPR REDUCTION OF OFDM SIGNALS</b> .....	140
<i>Lingyin Wang</i>	

<b>GENERALIZED CIPOLLA-LEHMER ROOT COMPUTATION IN FINITE FIELDS</b> .....	145
<i>Zhe Li ; Xiaolei Dong ; Zhenfu Cao</i>	
<b>LEVERAGING MARKOV CHAIN AND OPTIMAL MUTATION STRATEGY FOR SMART FUZZING</b> .....	151
<i>Yongji Ouyang ; Zehui Wu ; Qing Mu ; Qingxian Wang</i>	
<b>A SECURITY MULTI-PATH TRANSMISSION ALGORITHM BASED ON LINK-SECURITY-LEVEL</b> .....	157
<i>Laiquan Han ; Haiyan Chen ; Jinkuan Wang ; Xingwei Wang</i>	
<b>RESEARCH ON MULTILEVEL SECURITY ACCESS CONTROL POLICY PROCESSING METHOD</b> .....	162
<i>Junshe Wang ; Shengjuan Liu ; Hongbin Zhang ; Jiang Chang</i>	
<b>HVSM: AN IN-OUTVM SECURITY MONITORING ARCHITECTURE IN IAAS CLOUD</b> .....	167
<i>Yaqiang Mao ; Xujian Chen ; Yuan Luo</i>	
<b>A SCHEME OF ATTRIBUTE-BASED ENCRYPTION ACCESS POLICY USED IN MOBILE CLOUD STORAGE FOR PERSONAL HEALTH RECORDS</b> .....	174
<i>S.E. Wang ; B.G. Lin</i>	
<b>AN IMPROVED HU MOMENT INVARIANTS BASED CLASSIFICATION METHOD FOR WATERMARKING ALGORITHM</b> .....	182
<i>Guiduo Duan ; Xi Zhao ; Aiguo Chen ; YueQiang Liu</i>	
<b>ADAPTIVE LTE UPLINK MODEL IN VEHICULAR NETWORK</b> .....	187
<i>H.M. Sendi ; Sun Wensheng</i>	
<b>Author Index</b>	