

# Contents

## Invited Paper

While Mobile Encounters with Clouds. . . . .	3
<i>Man Ho Au, Kaitai Liang, Joseph K. Liu, and Rongxing Lu</i>	

## Authentication Mechanism

Multi-device Anonymous Authentication . . . . .	21
<i>Kamil Kluczniak, Jianfeng Wang, Xiaofeng Chen, and Mirosław Kutyłowski</i>	
A Mobile Device-Based Antishoulder-Surfing Identity Authentication Mechanism. . . . .	37
<i>Jia-Ning Luo, Ming-Hour Yang, and Cho-Luen Tsai</i>	
Mutual Authentication with Anonymity for Roaming Service with Smart Cards in Wireless Communications . . . . .	47
<i>Chang-Shiun Liu, Li Xu, Limei Lin, Min-Chi Tseng, Shih-Ya Lin, and Hung-Min Sun</i>	

## Cloud Computing Security

Efficient Fine-Grained Access Control for Secure Personal Health Records in Cloud Computing . . . . .	65
<i>Kai He, Jian Weng, Joseph K. Liu, Wanlei Zhou, and Jia-Nan Liu</i>	
An Energy-Efficient Task Scheduling Heuristic Algorithm Without Virtual Machine Migration in Real-Time Cloud Environments. . . . .	80
<i>Yi Zhang, Liuhua Chen, Haiying Shen, and Xiaohui Cheng</i>	
An Infrastructure-Based Framework for the Alleviation of JavaScript Worms from OSN in Mobile Cloud Platforms . . . . .	98
<i>Shashank Gupta and Brij B. Gupta</i>	

## Data Mining for Security Application

Ld-CNNs: A Deep Learning System for Structured Text Categorization Based on LDA in Content Security . . . . .	113
<i>Jinshuo Liu, Yabo Xu, Juan Deng, Lina Wang, and Lanxin Zhang</i>	

Realtime DDoS Detection in SIP Ecosystems: Machine Learning Tools  
of the Trade . . . . . 126  
*Zisis Tsiatsikas, Dimitris Geneiatakis, Georgios Kambourakis,  
and Stefanos Gritzalis*

**Digital Signature**

Two-in-One Oblivious Signatures Secure in the Random Oracle Model . . . . . 143  
*Raylin Tso*

A New Transitive Signature Scheme . . . . . 156  
*Chao Lin, Fei Zhu, Wei Wu, Kaitai Liang,  
and Kim-Kwang Raymond Choo*

**Privacy-Preserving Technologies**

Privacy-Preserving Profile Matching Protocol Considering Conditions . . . . . 171  
*Yosuke Ishikuro and Kazumasa Omote*

Privacy Preserving Credit Systems . . . . . 184  
*Sherman S.M. Chow, Russell W.F. Lai, Xiuhua Wang,  
and Yongjun Zhao*

Evading System-Calls Based Intrusion Detection Systems . . . . . 200  
*Ishai Rosenberg and Ehud Gudes*

**Network Security and Forensic**

HeapRevolver: Delaying and Randomizing Timing of Release of Freed  
Memory Area to Prevent Use-After-Free Attacks . . . . . 219  
*Toshihiro Yamauchi and Yuta Ikegami*

Timestamp Analysis for Quality Validation of Network Forensic Data . . . . . 235  
*Nikolai Hampton and Zubair A. Baig*

**Searchable Encryption**

An Efficient Secure Channel Free Searchable Encryption Scheme with  
Multiple Keywords . . . . . 251  
*Tingting Wang, Man Ho Au, and Wei Wu*

Searchable Symmetric Encryption Supporting Queries with  
Multiple-Character Wildcards . . . . . 266  
*Fangming Zhao and Takashi Nishide*

A System of Shareable Keyword Search on Encrypted Data . . . . . 283  
*Wei-Ting Lu, Wei Wu, Shih-Ya Lin, Min-Chi Tseng, and Hung-Min Sun*

## Security Policy and Access Control

An Attribute-Based Protection Model for JSON Documents . . . . .	303
<i>Prosunjit Biswas, Ravi Sandhu, and Ram Krishnan</i>	
The GURAG Administrative Model for User and Group Attribute Assignment . . . . .	318
<i>Maanak Gupta and Ravi Sandhu</i>	
On the Relationship Between Finite Domain ABAM and PreUCON <sub>A</sub> . . . . .	333
<i>Asma Alshehri and Ravi Sandhu</i>	

## Security Protocols

MD- $\mathcal{VC}_{Matrix}$ : An Efficient Scheme for Publicly Verifiable Computation of Outsourced Matrix Multiplication . . . . .	349
<i>Gang Sheng, Chunming Tang, Wei Gao, and Ying Yin</i>	
Expressive Rating Scheme by Signatures with Predications on Ratees . . . . .	363
<i>Hiroaki Anada, Sushmita Ruj, and Kouichi Sakurai</i>	

## Symmetric Key Cryptography

A New Adaptable Construction of Modulo Addition with Scalable Security for Stream Ciphers . . . . .	383
<i>Min Hsuan Cheng, Reza Sedaghat, and Prathap Siddavaatam</i>	
Extension of Meet-in-the-Middle Technique for Truncated Differential and Its Application to RoadRunneR . . . . .	398
<i>Qianqian Yang, Lei Hu, Siwei Sun, and Ling Song</i>	

## System Security

DF-ORAM: A Practical Dummy Free Oblivious RAM to Protect Outsourced Data Access Pattern . . . . .	415
<i>Qiumao Ma, Wensheng Zhang, and Jinsheng Zhang</i>	
PMFA: Toward Passive Message Fingerprint Attacks on Challenge-Based Collaborative Intrusion Detection Networks . . . . .	433
<i>Wenjuan Li, Weizhi Meng, Lam-For Kwok, and Horace Ho Shing Ip</i>	
Iris Cancellable Template Generation Based on Indexing-First-One Hashing . . .	450
<i>Yen-Lung Lai, Zhe Jin, Bok-Min Goi, Tong-Yuen Chai, and Wun-She Yap</i>	

**Web Security**

Detecting Malicious URLs Using Lexical Analysis . . . . .	467
<i>Mohammad Saiful Islam Mamun, Mohammad Ahmad Rathore, Arash Habibi Lashkari, Natalia Stakhanova, and Ali A. Ghorbani</i>	
Gatekeeping Behavior Analysis for Information Credibility Assessment on Weibo. . . . .	483
<i>Bailin Xie, Yu Wang, Chao Chen, and Yang Xiang</i>	

**Data Mining for Security Application (Short Paper)**

Finding Anomalies in SCADA Logs Using Rare Sequential Pattern Mining . . .	499
<i>Anisur Rahman, Yue Xu, Kenneth Radke, and Ernest Foo</i>	

**Provable Security (Short Paper)**

Improved Security Proof for Modular Exponentiation Bits . . . . .	509
<i>Kewei Lv, Wenjie Qin, and Ke Wang</i>	

**Security Protocol (Short Paper)**

Secure Outsourced Bilinear Pairings Computation for Mobile Devices. . . . .	519
<i>Tomasz Hyla and Jerzy Pejaś</i>	
The Design and Implementation of Multi-dimensional Bloom Filter Storage Matrix . . . . .	530
<i>Fei Xu, Pinxin Liu, Jianfeng Yang, and Jing Xu</i>	

<b>Author Index</b> . . . . .	539
-------------------------------	-----

Network and System Security

10th International Conference, NSS 2016, Taipei,

Taiwan, September 28-30, 2016, Proceedings

Chen, J.; Piuri, V.; Su, C.; Yung, M. (Eds.)

2016, XIV, 540 p. 128 illus., Softcover

ISBN: 978-3-319-46297-4