

Workshop on Cryptography and Information Security

Date: Thursday, 13 Dec. 2012

Room: 3F 305.306.307

Session: Authentication (1:00~2:30 pm)

Chair: **Prof. Raylin Tso**, National Chengchi University, Taiwan

- 1005 A Secure ECC-based RFID Authentication Scheme Using Hybrid Protocols
Yi-Pin Liao and Chih-Ming Hsiao
- 1007 A Dynamic Approach to Hash-Based Privacy-Preserving RFID Protocols
Chih-Yuan Lee, Hsin-Lung Wu, and Jen-Chun Chang
- 1117 Deniable Authentication Protocols with Confidentiality and Anonymous Fair Protections
Shin-Jia Hwang, Yun-Hao Sung, and Jen-Fu Chi
- 1122 A Novel Authentication Scheme Based on Torus Automorphism for Smart Card
Chin-Chen Chang, Qian Mao, and Hsiao-Ling Wu

Session: Cheater Detection, Cryptanalysis, and Communication Security (2:45~4:15 pm)

Chair: **Prof. Wei-Bin Lee**, Feng Chia University, Taiwan

- 1011 An Extension of Harn-Lin's Cheater Detection and Identification
Lein Harn and Changlu Lin
- 1025 Cryptanalysis on User Authentication Scheme with Anonymity
Yung-Cheng Lee
- 1139 Cryptanalysis of a Provably Secure Certificateless Short Signature Scheme
Yu-Chi Chen, Raylin Tso, and Gwoboa Horng
- 1159 Controlled Quantum Secure Direct Communication based on Single Photons
Wei-Lin Chang, Fang-Jhu Lin, Guo-Jyun Zeng, and Yao-Hsin Chou

Session: Intrusion Detection and Prevention (4:30~6:00 pm)

Chair: **Prof. Chia-Mei Chen**, National Sun Yat-Sen University, Taiwan

- 1006 Impact of Identifier-Locator Split Mechanism on DDoS Attacks
Ying Liu, Jianqiang Tang, and Hongke Zhang
- 1045 Detecting Web-Based Botnet with Fast-flux Domain
Chia-Mei Chen, Ming-Zong Huang, and Ya-Hui Ou
- 1090 Improvements of Attack-Defense Trees for Threat Analysis
Ping Wang and Jia-Chi Liu
- 1094 Design and Implementation of a Linux Kernel Based Intrusion Prevention

System in Gigabit Network Using Commodity Hardware

Li-Chi Feng, Chao-Wei Huang, and Jian-Kai Wang

1115 Performance Evaluation on Permission-Based Detection for Android Malware

Chun-Ying Huang, Yi-Ting Tsai, and Chung-Han Hsu

Room: 3F 315.316.317

Session: Steganography, Data Hiding, and Watermarking (1:00~2:30 pm)

Chair: **Prof. Wei-Jen Wang**, National Central University, Taiwan

1096 Image Steganography Using Gradient Adjacent Prediction in Side-Match Vector Quantization

Shiau-Rung Tsui, Cheng-Ta Huang, and Wei-Jen Wang

1113 A Data Hiding Scheme based on Square Formula Fully Exploiting Modification Directions

Wen-Chung Kuo

1132 Digital Watermarking Based on JND Model and QR Code Features

Hsi-Chieh Lee, Chang-Ru Dong, and Tzu-Miao Lin

1135 Multi-Dimensional and Multi-Level Histogram-Shifting-Imitated Reversible Data Hiding Scheme

Zhi-Hui Wang, Chin-Chen Chang, Ming-Li Li, and Shi-Yu Cui

Session: Server Security, Security Auditing, and Secret Image Sharing (2:45~4:15 pm)

Chair: **Prof. Wen-Chung Kuo**, National Yunlin University of Science and Technology, Taiwan

1087 Theoretical Analysis and Realistic Implementation of Secure Servers Switching System

Yu-Hong Chen, Kuang-Tse Chen, and Lei Wang

1101 Design and Implementation of a Self-Growth Security Baseline Database for Automatic Security Auditing

Chien-Ting Kuo, He-Ming Ruan, Shih-Jen Chen, and Chin-Laung Lei

1152 Enhancing Cloud-based Servers by GPU/CPU Virtualization Management

Tin-Yu Wu, Wei-Tsong Lee, Chien-Yu Duan, and Tain-Wen Suen

1209 A Threshold Secret Image Sharing with Essential Shadow Images

Ching-Nung Yang and Chih-Cheng Wu