December 13, 2012

Program of Keynote Speeches

Date: Thursday, 13 Dec. 2012
Room: 2F A.B Lecture Hall
Time: 09:30~10:30 am

Chair: **Prof. Ching-Nung Yang**, National Dong Hwa University, Taiwan
Speaker: **Prof. L. Harn**, University of Missouri-Kansas City, USA
Title: Secret Sharing and Its Applications
Abstract: Secret sharing was first proposed in 1979 by Shamir and Blakley separately. Secret sharing has become a very important cryptographic tool used in multi-party computing, e-voting, distributed computing, etc. In this talk, I will outline new research problems and solutions when secret reconstruction is performed in asynchronous channels. It will include rational secret sharing, secure secret reconstruction, multi-secret sharing, cheater detection and identification. In addition, new applications using secret sharing to support secure group communication, secure multicast transmission will also be addressed.

Time: 10:30~11:30 am

Chair: **Prof. Ruay-Shiung Chang**, National Dong Hwa University, Taiwan
Speaker: **Prof. C.-C. Jay Kuo**, University of Southern California, USA
Title: Depth-Assisted Intelligent Video
Abstract: Intelligent video, including video understanding, indexing and retrieval, is a very challenging computer vision problem and a good application candidate of cloud computing. When a scene is captured by a single camera, the 3D world space is projected to a 2D image space. A significant amount of information is lost during the projection process. There is a recent trend to put more emphasis on acquiring the depth information so as to simplify the video processing and understanding tasks. The depth information can be obtained by a depth camera, a stereo camera or some depth-inference algorithms. These are very hot topics due to the popularity of the Microsoft Kinetic and the emergence of 3D video contents such as 3D movies and 3DTV. In this talk, I will give an overview talk on the usefulness of the depth information in several video analysis problems and future research opportunities and challenges.

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

Date: Thursday, 13 Dec. 2012

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

Workshop on Computer Architecture, Embedded Systems, SoC, and VLSI/EDA

Date: Thursday, 13 Dec. 2012

Room: 3F 315.316.317

Session: Computer Architecture and Embedded Systems (4:30~6:00 pm)

Chair: **Prof. Shyue-Ming Tang**, National Defense University, Taiwan

1051 On the Variants of Tagged Geometric History Length Branch Predictors

Yeong-Chang Maa and Mao-Hsu Yen

1147 Hardware Acceleration Design for Embedded Operating System Scheduling

Jian-He Liao, Jer-Min Jou, Cheng-Hung Hsieh, and Ding-Yuan Lin

1148 A Distributed Run-Time Dynamic Data Manager for Multi-core System Parallel Execution

Wen-Hsien Chang, Jer-Min Jou, Cheng-Hung Hsieh, and Ding-Yuan Lin

1156 Design of a Dynamic Parallel Execution Architecture for Multi-Core Systems

Shiang Huang, Jer-Min Jou, Cheng-Hung Hsieh, and Ding-Yuan Lin

---

Date: Thursday, 13 Dec. 2012

Room: 3F 308.309

Session: VLSI Design and Digital Signal Processing (4:30~6:00 pm)

Chair: **Prof. Shun-Wen Cheng**, Far East University, Taiwan

1063 Energy-Aware Compiler Optimization for VLIW-DSP Cores

Yung-Cheng Ma, Tse-An Liu, and Wen-Shih Chao

1067 A Multiplier-Free Noise Trapped Touch Algorithm for Low Cost 4x4 Matrix Panel Design

Yu-Hsaing Yu, Qi-Wen Wang, and Tsung-Ying Sun

1160 A Novel Defragmemtable Memory Allocating Schema for MMU-less Embedded System

Yu-Hsaing Yu, Jing-Zhong Wang, and Tsung-Ying Sun

1100 Asynchronous Ring Network Mechanism with A Fair Arbitration Strategy for Network on Chip

Jih-Ching Chiu, Kai-Ming Yang, and Chen-Ang Wong

1203 High-Performance 128-bit Comparator Based on Conditional Carry-Select Scheme
Shun-Wen Cheng, Jhen-Yuan Li, and Wei-Chi Chen

Workshop on Software Engineering and Programming Languages

Date: Thursday, 13 Dec. 2012

Room: 3F 308.309

Session: Novel Compilation Techniques (1:00~2:30 pm)

Chair: **Prof. Peng-Sheng Chen**, National Chung Cheng University, Taiwan

1123 Low Power Compiler Optimization for Pipelining Scaling
Jen-Chieh Chang, Cheng-Yu Lee, Chia-Jung Chen, and Rong-Guey Chang

1179 Accurate Instruction-Level Alias Analysis for ARM Executable Code
Tat-Wai Chong and Peng-Sheng Chen

1022 A Translation Framework for Automatic Translation of Annotated LLVM IR into OpenCL Kernel Function
Chen-Ting Chang, Yu-Sheng Chen, I-Wei Wu, and Jyh-Jiun Shann

1119 An Editing System Converting a UML State Diagram to a PLC Program
Yung-Liang Chang, Chin-Feng Fan, and Swu Yih

Session: Web Services and Software Engineering (2:45~4:15 pm)

Chair: **Prof. Jiann-I Pan**, Tzu-Chi University, Taiwan

1038 An Effective Flood Forecasting System Based on Web Services
Ya-Hui Chang, Pei-Shan Wu, Yu-Te Liu, and Shang-Pin Ma

1107 A Two-leveled Web Service Path Re-planning Technique
Shih-Chien Chou and Chih-Yang Chiang

1048 A Flexible and Re-configurable Service Platform for Multi-user Mobile Games
Yu-Sheng Cheng, Chun-Feng Liao, and Don-Lin Yang

1009 A Simulation Environment for Studying the Interaction Process between a Human and an Embedded Control System
Chin-Feng Fan, Cheng-Tao Chiang, and Albert Yih