

# ICISC 2005 Program

**Thursday December 1, 2005**

**Session 1: Key Management and Distributed Cryptography**      **Chaired by Nicolas T. Courtois**

- 10:00 - 10:20      **A Timed-Release Key Management Scheme for Backward Recovery**  
Maki Yoshida, Osaka University, Japan  
Shigeo Mitsunari, u10 Networks, Japan  
Toru Fujiwara, Osaka University, Japan
- 10:20 - 10:40      **Property-Based Broadcast Encryption for Multi-level Security Policies**  
André Adelsbach, Ulrich Huber, Ahmad-Reza Sadeghi, Ruhr-Universität Bochum, Germany
- 10:40 - 11:00      **Efficient Cryptographic Protocol Design Based on Distributed El Gamal Encryption**  
Felix Brandt, Stanford University, USA
- 11:00 - 11:20      **Break**

**Session 2: Authentication and Biometrics**      **Chaired by Jacques Patarin**

- 11:20 - 11:40      **An Enhanced Estimation Algorithm for Reconstructing Fingerprint Strip Image**  
Woong-Sik Kim, Weon-Hee Yoo, Inha University, Korea  
Jang-Hyun Park, KIPA(Korea IT Industry Promotion Agency), Korea  
Bok-Ki Kim, Kwangwoon University, Korea
- 11:40 - 12:00      **Trust Management for Resilient Wireless Sensor Networks**  
Junbeom Hur, Younho Lee, Seong-Min Hong, Hyunsoo Yoon, KAIST, Korea
- 12:00 - 12:20      **Efficient Authenticators with Application to Key Exchange**  
Shaoquan Jiang, Guang Gong, University of Waterloo, Canada
- 12:20 - 13:40      **Lunch**

**Invited talk I**      **Chaired by Jeong Hyun Yi**

- 13:40 - 14:30      **Invited talk 1: National Security, Forensics and Mobile Communications**  
David Naccache, Ecole Normale Supérieure, France
- 14:30 - 14:50      **Break**

**Session 3: Provable Security and Primitives**      **Chaired by Kouichi Sakurai**

- 14:50 - 15:10      **Improvements to Mitchell's Remote User Authentication Protocol**  
Vipul Goyal, Abhishek Jain, IT-BHU, India  
Jean Jacques Quisquater, Université Catholique de Louvain, Belgium
- 15:10 - 15:30      **Benes and Butterfly Schemes Revisited**  
Jacques Patarin, Audrey Montreuil, Versailles University, France
- 15:30 - 15:50      **Relative Doubling Attack Against Montgomery Ladder**  
Sung-Ming Yen, Lee-Chun Ko, National Central University, Taiwan  
SangJae Moon, Kyungpook National University, Korea  
JaeCheol Ha, Korea Nazarene University, Korea
- 15:50 - 16:10      **Improved Collision Attack on MD4 with Probability Almost 1**  
Yusuke Naito, Yu Sasaki, Noboru Kunihiro, Kazuo Ohta, University of Electro-Communications, Japan

**Finding Collision on 45-Step HAS-160**

Aaram Yun, NSRI, Korea

16:10 - 16:30 Soo Hak Sung, Paichai University, Korea

Sangwoo Park, NSRI, Korea

Donghoon Chang, Seokhie Hong, Hong-Su Cho, Korea University, Korea

16:30 - 16:50 **Break**

**Session 4: System/Network Security**

**Chaired by Heejo Lee**

**The Program Counter Security Model: Automatic Detection and Removal of Control-Flow Side Channel Attacks**

16:50 - 17:10 David Molnar, Matt Piotrowski, UC-Berkeley, USA

David Schultz, MIT, USA

David Wagner, UC-Berkeley, USA

**The Dilemma of Covert Channels Searching**

17:10 - 17:30 Changda Wang, Jiangsu University, China

Shiguang Ju, Carleton University, Canada

**A Probabilistic Approach to Estimate the Damage Propagation of Cyber Attacks**

17:30 - 17:50 Young-Gab Kim, Taek Lee, Hoh Peter In, Korea University, Korea

Yoon-Jung Chung, InJung Kim, ETRI, Korea

Doo-Kwon Baik, Korea University, Korea

**Foundations of Attack Trees**

17:50 - 18:10 Sjouke Mauw, Eindhoven University of Technology, The Netherlands

Martijn Oostdijk, Radboud University Nijmegen, The Netherlands

18:10 **Banquet**

**Friday December 2, 2005**

**Invited talk II**

**Chaired by Youjin Song**

10:00 - 10:50 **Invited talk 2: Information Security as Interdisciplinary Science Based on Ethics**

Shigeo Tsujii, Institute of Information Security, Japan

10:50 - 11:10 **Break**

**Session 5: Block/Stream Ciphers ( I )**

**Chaired by Sangwoo Park**

**An Algebraic Masking Method to Protect AES Against Power Attacks**

11:10 - 11:30 Nicolas T. Courtois, Axalto Crypto Research & Advanced Security, France

Louis Goubin, Versailles University, France

**Characterisations of Extended Resiliency and Extended Immunity of S-Boxes**

11:30 - 11:50 Josef Pieprzyk, Xian-Mo Zhang, Macquarie University, Australia

Jovan Dj. Golić, Telecom Italia, Italy

**Integral Cryptanalysis of Reduced FOX Block Cipher**

11:50 - 12:10 Wenling Wu, Wentao Zhang, Dengguo Feng, Chinese Academy of Sciences, China

**Hybrid Symmetric Encryption Using Known-Plaintext Attack-Secure Components**

12:10 - 12:30 Kazuhiko Minematsu, Yukiyasu Tsunoo, NEC Corporation, Japan

12:30 - 13:50 **Lunch**

**Session 6: Block/Stream Ciphers (II)****Chaired by Josef Pieprzyk**

- 13:50 - 14:10 **Cryptanalysis of Sinks**  
Nicolas T. Courtois, Axalto Smart Cards Crypto Research, France
- 14:10 - 14:30 **Weaknesses of COSvd (2,128) Stream Cipher**  
Bin Zhang, Chinese Academy of Sciences, China  
Hongjun Wu, Katholieke Universiteit Leuven, Belgium  
Dengguo Feng, Hong Wang, Chinese Academy of Sciences, China
- 14:30 - 14:50 **Expanding Weak PRF with Small Key Size**  
Kazuhiko Minematsu, Yukiyasu Tsunoo, NEC Corporation, Japan
- 14:50 - 15:10 **On Linear Systems of Equations with Distinct Variables and Small Block Size**  
Jacques Patarin, Versailles University, France
- 15:10 - 15:30 **Break**

**Session 7: Efficient Implementations****Chaired by Felix Brandt**

- 15:30 - 15:50 **An FPGA Implementation of CCM Mode Using AES**  
Emmanuel López-Trejo, Francisco Rodríguez-Henríquez, Arturo Díaz-Pérez, CINVESTAV-IPN, Mexico
- 15:50 - 16:10 **New Architecture for Multiplication in  $GF(2^m)$  And Comparisons with Normal and Polynomial Basis Multipliers for Elliptic Curve Cryptography**  
Soonhak Kwon, Sungkyunkwan University, Korea  
Taekyoung Kwon, Sejong University, Korea  
Young-Ho Park, Sejong Cyber University, Korea
- 16:10 - 16:30 **An Efficient Design of CCMP for Robust Security Network**  
Duhyun Bae, Gwanyeon Kim, Jiho Kim, Sehyun Park, Ohyoung Song, Chung-Ang University, Korea

**Session 8: Digital Rights Management****Chaired by Seokhie Hong**

- 16:30 - 16:50 **Software-based Copy Protection for Temporal Media during Dissemination and Playback**  
Gisle Grimen, Christian Mönch, Roger Midtstraum, Norwegian University of Science and Technology, Norway
- 16:50 - 17:10 **Ambiguity Attacks on the Ganic-Eskicioglu Robust DWT-SVD Image Watermarking Scheme**  
Grace C.-W.Ting, Swinburne University of Technology (Sarawak Campus), Malaysia
- 17:10 - 17:30 **Break**

**Session 9: Public Key Cryptography****Chaired by Taekyoung Kwon**

- 17:30 - 17:50 **Universal Custodian-Hiding Verifiable Encryption for Discrete Logarithms**  
Joseph K. Liu, University of Bristol, UK  
Patrick P. Tsang, Dartmouth College, USA  
Duncan S. Wong, Robert W. Zhu, City University of Hong Kong, China
- 17:50 - 18:10 **An Efficient Static Blind Ring Signature Scheme**  
Qianhong Wu, University of Wollongong, Australia  
Fanguo Zhang, Sun Yat-sen University, China  
Willy Susilo, Yi Mu, University of Wollongong, Australia
- 18:10 - 18:30 **Trading Time for Space: Towards an Efficient IBE Scheme with Short(er) Public Parameters in the Standard Model**  
Sanjit Chatterjee, Palash Sarkar, Indian Statistical Institute, India
- 18:30 - 18:50 **Yet Another Forward Secure Signature from Bilinear Pairings**  
Duc-Liem Vo, Kwangjo Kim, Information and Communication University, Korea
- 18:50 **Adjourn**