

ISPEC 2008, 21-23 April, Crowne Plaza, Darling Harbour, Sydney, Australia
Program

21 April 2008

8:45-9:00 Opening

9:00-10:00: **Invited Speech (Chair: Yi Mu)**

Trust Enhanced Security
Vijay Varadharajan, Macquarie University, Australia

10:00-10:30: Tea Break

Authentication and Signatures (Chair, Marc Joye)

10:30-10:55: Verification of Integrity and Secrecy Properties of a Biometric
Authentication Protocol
Anongporn Salaiwarakul and Mark D. Ryan
University of Birmingham, UK

10:55-11:20: An On-line Secure E-passport Protocol
Vijayakrishnan Pasupathinathan and Josef Pieprzyk, Huaxiong Wang
Macquarie University, Australia;
Nanyang Technological University, Singapore

11:20-11:45: Secure Multi-Coupons for Federated Environments: Privacy-Preserving
and Customer-Friendly
Frederik Armknecht, Alberto Escalante, Hans Loehr, Mark Manulis,
Ahmad-Reza Sadeghi
Ruhr-University Bochum, Germany,
Universite Catholique de Louvain, Belgium

11:45-12:10: 1-out-of-n Oblivious Signatures
Raylin Tso and Takeshi Okamoto and Eiji Okamoto
University of Tsukuba, Japan

12:10-12:35 A formal study of the privacy concerns in biometric-based remote
authentication schemes
Qiang Tang and Julien Bringer and Herve Chabanne and David Pointcheval
University of Twente, Netherlands, Sagem Security;
Ecole Normale Superieure, France

12:35-2:00: Lunch break

Encryption (Chair: Tsuyoshi Takagi)

- 2:00-2:25: Private Query on Encrypted Data in Multi-User Settings
Feng Bao, Robert H. Deng, Xuhua Ding, Yanjiang Yang
Singapore Management University,
Institute for Infocomm Research, Singapore
- 2:25-2:50: Towards Tamper Resistant Code Encryption: Practice and Experience
Jan Cappaert, Bart Preneel, Bertrand Anckaert, Matias Madou
and Koen De Bosschere
Katholieke Universiteit Leuven, Belgium; Universiteit Gent, Belgium
- 2:50-3:15: A New Public Key Broadcast Encryption Using the Boneh-Boyen-Goh's HIBE Scheme
Jong Hwan Park and Dong Hoon Lee
Korea University, Korea
- 3:15-3:45: Tea Break

System Security (Chair: Jan Cappaert)

- 3:45-4:10: RSA Moduli with a Predetermined Portion: Techniques and Applications
Marc Joye
Thomson R&D, France
- 4:10-4:35: Variants of the Distinguished Point Method for Cryptanalytic Time Memory Trade-offs
Jin Hong, Kyung Chul Jeong, Eun Young Kwon, In-Sok Lee, and Daegun Ma
Seoul National University, Korea
- 4:35-5:00: Secure Cryptographic Precomputation with Insecure Memory
Patrick P. Tsang and Sean W. Smith
Dartmouth College, USA

22 April 2008

9:00-10:00: Invited Speech (Chair: Liqun Chen)

Scalable Authentication Techniques Compatible With
Modern Multimedia Coding Standards
Robert H. Deng, Singapore Management University, Singapore

10:00-10:30: Tea Break

Network Security (Chair: C. Pandu rangan)

- 10:30-10:55: Securing Peer-to-peer Distributions for Mobile Devices
Andre Osterhues, Ahmad-Reza Sadeghi, Marko Wolf,

Christian Stueble, N. Asokan
Horst Goertz Institute for IT Security, Ruhr-University Bochum, Germany

10:55-11:20: Unified Rate Limiting in Broadband Access Networks for Defeating Internet Worms and DDoS Attacks

Keun Park, Dongwon Seo, Jaewon Yoo, Heejo Lee, Hyogon Kim
Korea University, Korea

11:20-11:45: Combating Spam and Denial-of-Service Attacks with Trusted Puzzle Solvers

Patrick P. Tsang and Sean W. Smith
Dartmouth College, USA

11:45-12:10: PROBE: A Process Behavior-based Host Intrusion Prevention System

Minjin Kwon, Kyoochang Jeong, Heejo Lee
Korea University, Korea

12:10-12:35: Towards the World-Wide Quantum Network

Quoc-Cuong Le and Patrick Bellot
Ecole Nationale Supérieure des Télécommunications (ENST), Paris, France

12:35-2:00: Lunch Break

Access Control (Chair : Vijay Varadharajan)

2:00-2:25: Synthesising Monitors from High-level Policies for the Safe Execution of Untrusted Software

Andrew Brown, Mark Ryan
University of Birmingham, UK

2:25-2:50: Mediator-Free Secure Policy Interoperation in Multi-Domain Environments

Xingang Wang, Dengguo Feng, Zhen Xu, Honggang Hu
Chinese Academy of Sciences, China

RFID Security (Chair: Robert Deng)

2:50-3:15: Privacy of Recent RFID Authentication Protocols

Khaled Ouafi, Raphael C.-W. Phan
Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland;
Loughborough University, UK

3:15-3:40: A New Hash-based RFID Mutual Authentication Protocol Providing Enhanced User Privacy Protection

Jihwan Lim, Heekuck Oh, Sangin Kim
Hanyang University, Korea

3:40-4:10: Tea Break

Pairing and Elliptic curve (Chair: Willy Susilo)

4:10-4:35: An Efficient Countermeasure against Side Channel Attacks for Pairing

Computation

Masaaki Shirase, Tsuyoshi Takagi, Eiji Okamoto

Future University-Hakodate, Japan; University of Tsukuba, Japan

4:35-5:00: Efficient Arithmetic on Subfield Elliptic Curves over Small Finite Fields of Odd Characteristic

Keisuke Hakuta and Hisayoshi Sato and Tsuyoshi Takagi

Hitachi, Ltd, Japan; Future University, Japan

6:00-10:00: Dinner Cruise

23 April 2008

Secret Computation I (Chair: Svein Johan Knapskog)

9:00-9:25: Secure Computation of the Vector Dominance Problem

Jin Yuan, Qingsong Ye, Huaxiong Wang, Josef Pieprzyk

Macquarie University, Australia;

Nanyang Technological University, Singapore

9:25-9:50: Rational Secret Sharing with Repeated Games

Maleka S., Amjed Shareef, C. Pandu Rangan

IIT MADRAS, India

9:50-10:20: Tea Break

Secret Computaton II (Chair: Svein Johan Knapskog)

10:20-10:45: Distributed Private Matching and Set Operations

Qingsong Ye and Huaxiong Wang and Josef Pieprzyk

Macquarie University, Australina;

Nanyang Technological University, Singapore

10:45-11:10: Computational Soundness of Non-Malleable Commitments

David Galindo, Flavio D. Garcia, and Peter van Rossum

University of Malaga, Spain;

Radboud University Nijmegen, Netherlands

Ciphers and Hash Functions (Chair: Josef Pieprzyk)

11:10-11:35: Square Attack on Reduced-Round Zodiac Cipher

Wen Ji and Lei Hu

Graduate School of Chinese Academy of Sciences, China

11:35-12:00: Analysis of zipper as a hash function

Pin Lin, Wenling Wu, Chuankun Wu, Tian Qiu

Chinese Academy of Science, China

12:00-12:25: On the importance of the key separation principle for different modes of operation
Danilo Gligoroski and Suzana Andova and Svein Johan Knapskog
Q2S, NTNU, Norway; TUE, Netherlands

12:25-12:35: Closing

12:35-2:00: Lunch