

**The 12th Australasian Conference on Information Security and Privacy (ACISP)
at Southbank Convention Centre, Townsville, Australia
2-4 July, 2007**

PROGRAM

Monday, 2nd July, 2007

| | |
|------------------------------------|---|
| 08:00 – 09:00 | Registration |
| 09:00 – 09:15 | Welcome Address |
| 10:15 – 10:45 | Morning Tea |
| Session 1: 09:15 – 10:30 | STREAM CIPHERS <i>Chair : Jovan Golic</i> <ul style="list-style-type: none">• An Analysis of the Hermes8 Stream Ciphers Steve Babbage, Carlos Cid, Norbert Pramstaller, Havard Raddum• On the Security of the LILI Family of Stream Ciphers Against Algebraic Attacks Sultan Al-Hinai, Leonie Simpson, Matt Henricksen, Ed Dawson• Strengthening NLS against Crossword Puzzle Attack Debojyoti Bhattacharya, Debdeep Mukhopadhyay, Dipanwita RoyChowdhury |
| 10:30 – 11:00 | Morning Tea |
| Session 2: 11:00 – 12:00 | SECRET SHARING SCHEME <i>Chair : Ron Steinfeld</i> <ul style="list-style-type: none">• Flaws in Some Secret Sharing Schemes against Cheating Toshinori Araki and Satoshi Obana• Efficient (k, n) Threshold Secret Sharing Schemes Secure against Cheating from $n - 1$ Cheaters Toshinori Araki |
| 12:00 – 13:30 | Lunch |
| Session 3: 13:30 – 15:10 | HASHING <i>Chair : Rei Safavi-Naini</i> <ul style="list-style-type: none">• A New Strategy for Finding a Differential Path of SHA1 Jun Yajima, Yu Sasaki, Yusuke Naito, Terutoshi Iwasaki, Takeshi Shimoyama, Noboru Kunihiro, Kazuo Ohta• Preimage Attack on the Parallel FFT-Hashing Function Donghoon Chang, Moti Yung, Jaechul Sung, Seokhie Hong, Sangjin Lee• Second Preimages for Iterated Hash Functions and their Implications on MACs Mario Lamberger and Norbert Pramstaller and Vincent Rijmen• On Building Hash Functions From Multivariate Quadratic Equations Olivier Billet, Thomas Peyrin and Matt J.B. Robshaw |
| 15:10 -15:40 | Afternoon Tea |
| Session 4: 15:40 – 16:30 | BIOMETRICS <i>Chair : Hossein Ghodosi</i> <ul style="list-style-type: none">• An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication Julien Bringer, Hervé Chabanne, Malika Izabachène, David Pointcheval, Qiang Tang, Sébastien Zimmer• Soft generation of secure biometric keys Jovan Golic and Madalina Baltatu |
| 16:30 – 18:00 | ACISP General Meeting |

Tuesday, 3rd July, 2007

09:00 – 10:00

INVITED SPEAKER

Chair : *Josef pieprzyk*

- **Constructing Cryptographic Curves**
Professor Andreas Enge
École Polytechnique, France

10:00 – 10:30

Morning Tea

Session 5:

10:30 – 11:45

CRYPTANALYSIS

Chair : *Yvo Desmedt*

- **Related-Key Amplified Boomerang Attacks on the Full-Round Eagle-64 and Eagle-128**
Kitae Jeong, Changhoon Lee, Jaechul Sung, Seokhie Hong, Jongin Lim
- **Analysis of the SMS4 block cipher**
Fen Liu, Wen Ji, Lei Hu, Jintai Ding, Shuwang Lv, Andrei Pyshkin, Ralf-Philipp Weinmann
- **Forgery Attack to an Asymptotically Optimal Traitor Tracing Scheme**
Yongdong Wu, Feng Bao, and Robert H. Deng

Session 6-1:

11:45 – 12:10

PUBLIC KEY CRYPTOGRAPHY

Chair : *Jennifer Seberry*

- **TCHo: a Hardware-Oriented Trapdoor Cipher**
Jean-Philippe Aumasson, Matthieu Finiasz, Willi Meier, Serge Vaudenay

12:10 – 13:30

Lunch Break

Session 6-2

13:30 – 15:10

PUBLIC KEY CRYPTOGRAPHY

Chair : *Jennifer Seberry*

- **Anonymity on Paillier's Trap-door Permutation**
Ryotaro Hayashi and Keisuke Tanaka
- **Generic Certificateless Key Encapsulation Mechanism**
Qiong Huang and Duncan S. Wong
- **Double-Size Bipartite Modular Multiplication**
Masayuki Yoshino, Katsuyuki Okeya, Camille Vuillaume
- **Affine Precomputation with Sole Inversion in Elliptic Curve Cryptography**
Erik Dahmen and Katsuyuki Okeya and Daniel Schepers

15:10 – 15:40

Afternoon Tea

Session 6-3:

15:40 – 16:30

PUBLIC KEY CRYPTOGRAPHY

Chair : *Huaxiong Wang*

- **Construction of Threshold (Hybrid) Encryption in the Random Oracle Model: How to Construct Threshold Tag-KEM from Weakly Secure Threshold KEM**
Takeru Ishihara, Hiroshi Aono, Sadayuki Hongo, and Junji Shikata
- **Efficient Chosen-Ciphertext Secure Identity-Based Encryption with Wildcards**
James Birkett and Alexander Dent and Gregory Neven and Jacob Schuldt

18:45 – 19:15

Pre Conference Drinks

19:15 – 22:00

Conference Dinner

Invited Speaker

- **Professor Andreas Enge** obtained his PhD in mathematics at the University of Augsburg in 2000. He is currently vice-head of the joint research team TANC - Algorithmic Number Theory for Cryptology between INRIA and École polytechnique, and teaches informatics at all levels at École polytechnique. Andreas has published widely on algebraic curves and cryptology, including a book entitled Elliptic Curves and their Application to Cryptography.

Wednesday, 4th July, 2007

Session 7-1:

09:00 – 10:15

AUTHENTICATION

Chair : Ed Dawson

- **Combining Prediction Hashing and MDS Codes for Efficient Multicast Stream Authentication**

Christophe Tartary and Huaxiong Wang

- **Certificateless Signature Revisited**

Xinyi Huang, Yi Mu, Willy Susilo, Duncan Wong, Wei Wu

- **Identity-Committable Signatures and Their Extension to Group-Oriented Ring Signatures**

Cheng-Kang Chu and Wen-Guey Tzeng

10:15 – 10:45

Morning Tea

Session7-2:

10:45 – 12:25

AUTHENTICATION

Chair : Willy Susilo

- **Hash-and-sign with Weak Hashing Made Secure**

Sylvain Pasini and Serge Vaudenay

- **"Sandwich" is Indeed Secure: How to Authenticate a Message with Just One Hashing**

Kan Yasuda

- **Threshold Anonymous Group Identification and Zero-Knowledge Proof**

Akihiro Yamamura, Takashi Kurokawa, Junji Nakazato

- **Noninteractive Manual Channel Message Authentication Based On eTCR Hash functions**

Mohammad Reza Reyhanitabar, Shuhong Wang, Reihaneh Safavi-Naini

12:25 – 13:30

Lunch

Session 8:

13:30 – 14:45

E-COMMERCE

Chair : Colin Boyd

- **A practical system for globally revoking the unlinkable pseudonyms of unknown users**

Stefan Brands and Liesje Demuyne and Bart De Decker

- **Efficient and Secure Comparison for On-Line Auctions**

Ivan Damgård, Martin Geisler, Mikkel Krøigård

- **Practical Compact E-Cash**

Man Ho Au and Willy Susilo and Yi Mu

Session 9:

43:45 – 15:35

SECURITY

Chair : Yi Mu

- **Use of Dempster-Shafer Theory and Bayesian Inferencing for Fraud Detection in Mobile Communication Networks**

Suvasini Panigrahi, Amlan Kundu, Shamik Sural and A. K. Majumdar

- **On Proactive Perfectly Secure Message Transmission**

Kannan Srinathan, Prasad Raghavendra, Pandu Rangan Chandrasekaran

15:30 – 16:30

Closing Drinks