Program

Sunday, February 7, 2010

18:30–20:00 Registration
19:00–20:00 Welcome Reception

Monday, February 8, 2010

9:00–9:30 Registration (Coffee & Juice)
9:30–9:40 Welcome Remarks

Session 1: Stream Ciphers and Block Ciphers (Chair: Jin Hong)

9:40–10:05 Cryptanalysis of the DECT Standard Cipher
Karsten Nohl, Erik Tews, and Ralf-Philipp Weinmann
10:05–10:30 Improving the Generalized Feistel
Tomoyasu Suzaki and Kazuhiko Minematsu
10:30–10:55 Nonlinear Equivalence of Stream Ciphers
Sondre Rønjom and Carlos Cid

10:55–11:20 **Coffee Break**

Invited Talk I (Chair: Seokhie Hong)

11:20–12:10 The Survey of Cryptanalysis on Hash Functions
Xiaoyun Wang

12:10–13:50 **Lunch**

Session 2: RFID and Implementations (Chair: Carlos Cid)

13:50–14:15 Lightweight Privacy Preserving Authentication for RFID Based on a Stream Cipher
Olivier Billet, Jonathan Etrog, and Henri Gilbert
14:15–14:40 Fast Software AES Encryption
Dag Arne Osvik, Joppe W. Bos, Deian Stefan, and David Canright

14:40–15:05 **Coffee Break**

Session 3: Hash Functions I (Chair: Jongsung Kim)

15:05–15:30 Attacking the Knudsen-Preneel Compression Functions
Onur Özen, Thomas Shrimpton, and Martijn Stam

15:30–15:55 Finding Preimages of Tiger Up to 23 Steps
Lei Wang and Yu Sasaki

15:55–16:20 Cryptanalysis of ESSENCE
María Naya-Plasencia, Andrea Röck, Jean-Philippe Aumasson, Yann Laigle-Chapuy, Gaëtan Leurent, Willi Meier, and Thomas Peyrin

17:00–18:30 **Social Event (Nanta)**

Tuesday, February 9, 2010

9:00–9:30 Registration (Coffee & Juice)

Session 4: Theory (Chair: Thomas Shrimpton)

9:30–9:55 Domain Extension for Enhanced Target Collision-Resistant Hash Functions
Ilya Mironov

9:55–10:20 Security Analysis of the Mode of JH Hash Function
Rishiraj Bhattacharyya, Avradip Mandal, and Mridul Nandi

10:20–10:45 Enhanced Security Notions for Dedicated-Key Hash Functions: Definitions and Relationships
Mohammad Reza Reyhanitabar, Willy Susilo, and Yi Mu

10:45–11:10 **Coffee Break**

Session 5: Message Authentication Codes (Chair: Bart Preneel)

11:10–11:35 A Unified Method for Improving PRF Bounds for a Class of Blockcipher based MACs
Mridul Nandi

11:35–12:00 How to Thwart Birthday Attacks against MACs via Small Randomness
Kazuhiko Minematsu

12:00–12:25 Constructing Rate-1 MACs from Related-Key Unpredictable Block Ciphers: PGV Model Revisited
Liting Zhang, Wenling Wu, Peng Wang, Lei Zhang, Shuang Wu, and Bo Liang

12:25–14:05 **Lunch**

Session 6: Hash Functions II (Chair: Yu Sasaki)

14:05–14:30 Higher Order Differential Attack on Step-Reduced Variants of *Luffa* v1
Dai Watanabe, Yasuo Hatano, Tsuyoshi Yamada, and Toshinobu Kaneko

14:30–14:55 Rebound Attack on Reduced-Round Versions of JH
Vincent Rijmen, Deniz Toz, and Kerem Varıcı

Session 7: Hash Functions III (Short Presentation) (Chair: Yu Sasaki)

14:55–15:10 Pseudo-cryptanalysis of the Original Blue Midnight Wish
Søren S. Thomsen

15:10–15:25 Differential and Invertibility Properties of BLAKE
Jean-Philippe Aumasson, Jian Guo, Simon Knellwolf, Krystian Matusiewicz, and Willi Meier

15:25–16:00 **Coffee Break**

16:00–17:30 **Rump Session** (Chair: Orr Dunkelman)

18:00–20:30 **Gala Dinner & Social Event (Samcheonggak)**

Wednesday, February 10, 2010

9:00–9:30 Registration (Coffee & Juice)

Invited Talk II (Chair: Tetsu Iwata)

9:30–10:20 A Provable-Security Perspective on the Development of Hash Functions
Thomas Shrimpton

10:20–10:50 **Coffee Break**

Session 8: Cryptanalysis (Chair: Taizo Shirai)

10:50–11:15 Rotational Cryptanalysis of ARX
Dmitry Khovratovich and Ivica Nikolić

11:15–11:40 Another Look at Complementation Properties
Charles Bouillaguet, Orr Dunkelman, Gaëtan Leurent, and Pierre-Alain Fouque

11:40–12:05 Super-Sbox Cryptanalysis: Improved Attacks for AES-like Permutations
Henri Gilbert and Thomas Peyrin

12:05–12:10 **Closing Remarks**

12:10–13:50 **Lunch**