ASIACRYPT 2004

Dec. 5~9, 2004, Jeju Island, Korea

Call for Participation

http://www.iris.re.kr/ac04

Conference Information

The Asiacrypt conferences are series of annual international conferences on high quality research in cryptology. Asiacrypt 2004 is organized by the IACR (International Association for Cryptologic Research) in cooperation with KIISC (Korea Institute of Information Security & Cryptology) and IRIS (International Research center for Information Security) at ICU (Information Communications University) and financially supported by MIC (Ministry of Information and Communication), Korea. Asiacrypt 2004 will be held during December 5~9, 2004 at Shilla Jeju Hotel in Jeju Island, Korea. Anyone interested in the latest developments in cryptology and its applications to information security is encouraged to attend Asiacrypt 2004.

Location & Travel Information

Jeju is a beautiful island located in the south sea of the Korean peninsula which is highlighted with its rich tourism. It is also called “Honeymoon Island,” since it is a favorite honeymoon place. The Shilla Jeju hotel is a beautiful place located at Jungmun resort area on the south coastline of Jeju Island. It takes about 50 minutes to get to the hotel by airport limousine or taxi from Jeju International Airport. Local flight connections from Incheon International airport and other major cities to Jeju airport are frequent and convenient.

Other Information

Average temperature of Jeju Island in December is expected to be 5 to 10 degree Celsius. Please bring warm sweaters and good windbreakers. The unit of Korean currency is Won (indicated as KW). Coin denominations are KW 10, 50, 100, and 500 and bank notes are KW 1,000, 5,000, and 10,000. One US dollar is equivalent to about 1,200 Korean Won, although the exchange rate is subject to change with market fluctuations. In electricity, most buildings have outlets for 220 volts only. Any visitors with confirmed outbound tickets may stay in Korea up to 30 days without visas except some restricted countries. We are preparing more information on accommodation, tour, social program, *etc*. for your enjoyable and memorable stay in Jeju. For more information, check the conference web site http://www.iris.re.kr/ac04/.

General Chair

Professor **Kwangjo Kim**
School of Engineering, ICU
103-6 Munji-dong Yuseong-gu, Daejeon,
305-714,Korea
Tel : +82-42-866-6118
Fax : +82-42-866-6273
E-mail kkj@icu.ac.kr
HP: +82-11-9414-1386

Program Chair

Professor **Pil Joong Lee**
Dept. of E.E., POSTECH
San 31 Hyoja-dong Nam-gu, Pohang,
790-784, Korea
Tel : +82-54-279-2232, +82-2-526-5585
Fax : +82-54-279-2903
E-mail pjl@postech.ac.kr
HP: +82-16-533-3232

Preliminary Program

Monday December 6, 2004

08:50~09:00	**Opening Remarks**

Session 1 : Block Ciphers

09:00~09:25	**On Feistel Ciphers using Optimal Diffusion Mappings across Multiple Rounds** Taizo Shirai and Bart Preneel
09:25~09:50	**Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC** Phillip Rogaway
09:50~10:15	**Eliminating Random Permutation Oracles in the Even-Mansour Cipher** Craig Gentry and Zulfikar Ramzan
10:15~10:40	**Coffee Break**

Session 2 : Public Key Encryption

10:40~11:05	**Towards Plaintext-Aware Public-Key Encryption without Random Oracles** Mihir Bellare and Adriana Palacio
11:05~11:30	**OAEP 3-Round: A Generic and Secure Asymmetric Encryption Padding** Duong Hieu Phan and David Pointcheval

Invited Talk I

11:30~12:30	**Stream Ciphers: Dead or Alive?** Adi Shamir
12:30~14:00	**Lunch**

Session 3 : Number Theory and Algebra

14:00~14:25	**On the Generalized Linear Equivalence of Functions over Finite Fields** Luca Breveglieri, Alessandra Cherubini, and Marco Macchetti
14:25~14:50	**Sieving Using Bucket Sort** Kazumaro Aoki and Hiroki Ueda

14:50~15:15 **Right-Invariance: A Property for Probabilistic Analysis of Cryptography based on Infinite Groups**
Eonkyung Lee

15:15~15:40 **Coffee Break**

Session 4 : Secure Computation

15:40~16:05 **Practical Two-Party Computation based on the Conditional Gate**
Berry Schoenmakers and Pim Tuyls

16:05~16:30 **Privacy in Non-Private Environments**
Markus Bläser, Andreas Jakoby, Maciej Liśkiewicz, and Bodo Manthey

16:30~16:55 **Asynchronous Proactive Cryptosystems Without Agreement**
Bartosz Przydatek and Reto Strobl

16:55~17:20 **Lattice-Based Threshold-Changeability for Standard Shamir Secret-Sharing Schemes**
Ron Steinfeld, Huaxiong Wang, and Josef Pieprzyk

Tuesday December 7, 2004

Session 5 : Hash Functions

09:00~09:25 **Masking Based Domain Extenders for UOWHFs: Bounds and Constructions**
Palash Sarkar

09:25~09:50 **Higher Order Universal One-Way Hash Functions**
Deukjo Hong, Bart Preneel, and Sangjin Lee

09:50~10:15 **The MD2 Hash Function is Not One-Way**
Frédéric Muller

10:15~10:40 **Coffee Break**

Session 6 : Key Management

10:40~11:05 **New Approaches to Password Authenticated Key Exchange based on RSA**
Muxiang Zhang

11:05~11:30 **Constant-Round Authenticated Group Key Exchange for Dynamic Groups**
Hyun-Jeong Kim, Su-Mi Lee, and Dong Hoon Lee

11:30~11:55 **A Public-Key Black-Box Traitor Tracing Scheme with Sublinear Ciphertext Size against Self-Defensive Pirates**
Tatsuyuki Matsushita and Hideki Imai

11:55~13:30	**Lunch** **Free Afternoon**

Rump Session

19:00~	**Rump Session**

Wednesday December 8, 2004

Session 7 : Identification

09:00~09:25	**Batching Schnorr Identification Scheme with Applications to Privacy-Preserving Authorization and Low-Bandwidth Communication Devices** Rosario Gennaro, Darren Leigh, Ravi Sundaram, and William Yerazunis
09:25~09:50	**Secret Handshakes from CA-Oblivious Encryption** Claude Castelluccia, Stanislaw Jarecki, and Gene Tsudik
09:50~10:15	***k*-Times Anonymous Authentication** Isamu Teranishi, Jun Furukawa, and Kazue Sako
10:15~10:40	**Coffee Break**

Session 8 : XL-algorithms

10:40~11:05	**The XL-Algorithm and a Conjecture from Commutative Algebra** Claus Diem
11:05~11:30	**Comparison between XL and Gröbner Basis Algorithms** Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita

Session 9 : Digital Signatures

11:30~11:55	**Generic Homomorphic Undeniable Signatures** Jean Monnerat and Serge Vaudenay
11:55~12:20	**Efficient and Provably Secure Trapdoor-free Group Signature Schemes from Bilinear Pairings** Lan Nguyen and Rei Safavi-Naini
12:20~14:00	**Lunch**

Session 10 : Public Key Cryptanalysis

14:00~14:25	**On the Security of MOR Public Key Cryptosystem** In-Sok Lee, Woo-Hwan Kim, Daesung Kwon, Sangil Nahm, Nam-Seok Kwak, and Yoo-Jin Baek
14:25~14:50	**Cryptanalyzing the Polynomial-Reconstruction based Public-Key System Under Optimal Parameter Choice** Aggelos Kiayias and Moti Yung

14:50~15:15	**Colluding Attacks to a Payment Protocol and Two Signature Exchange Schemes** Feng Bao
15:15~15:45	**Coffee Break**

Invited Talk II

15:45~16:45	**Information Security in Korea IT839 strategy** Ho-Ick Suk
17:00~18:00	**IACR Membership Meeting**
18:30~	**Banquet**

Thursday December 9, 2004

Session 11 : Symmetric Key Cryptanalysis

09:00~09:25	**How Far Can We Go Beyond Linear Cryptanalysis?** Thomas Baignères, Pascal Junod, and Serge Vaudenay
09:25~09:50	**The Davies-Murphy Power Attack** Sébastien Kunz-Jacques, Frédéric Muller, and Frédéric Valette
09:50~10:15	**Time-Memory Trade-Off Attacks on Multiplications and *T*-functions** Joydip Mitra and Palash Sarkar
10:15~10:40	**Cryptanalysis of Bluetooth Keystream Generator Two-level E0** Yi Lu and Serge Vaudenay
10:40~11:05	**Coffee Break**

Session 12 : Protocols

11:05~11:30	**On Provably Secure Time-Stamping Schemes** Ahto Buldas and Märt Saarepera
11:30~11:55	**Strong Conditional Oblivious Transfer and Computing on Intervals** Ian F. Blake and Vladimir Kolesnikov
11:55~12:20	**Improved Setup Assumptions for 3-Round Resettable Zero Knowledge** Giovanni Di Crescenzo, Giuseppe Persiano, and Ivan Visconti
12:20~14:00	**Lunch**
14:00~	**Conference Adjourns**