

Advanced Program

Recent update: Oct. 2nd 2004

The IWAP 2004 conference room is SPR-Hall

1st Day : Oct. 3, 2004 (Sunday)

15:00-15:30 Registration

15:30-16:30 **Invited Talk 1**

Chair: **Kwangjo Kim** (ICU, Korea)

PKI for supporting cross-border e-Commerce

Kwok-Yan Lam (Tsinghua Univ., China)

16:30-16:50 Coffee Break

16:50-18:30 **Regular papers**

Chair: **Tsuyoshi Takagi** (TUD, Germany)

Cryptanalysis of TTS and Tame-Like Multivariable Signature Schemes

Jintai Ding, Zhijun Yin (Univ. of Cincinnati, USA)

Limitation of Immediate Key Revocation in Identity-Based Schemes

Yumiko Hanaoka (NTT DoCoMo, Japan), *Goichiro Hanaoka*

(Univ. of Tokyo, Japan), *Junji Shikata* (Yokohama National Univ., Japan),

Hideki Imai (Univ. of Tokyo, Japan)

Unified Certificate Verification Protocol

Kasun De Zoysa (University of Colombo School of Computing, Sri Lanka)

Collaborative Admission Control in the Office

Jong-Phil Yang, Kyung-Hyune Rhee (Pukyong National Univ., Korea)

19:00-20:00 **Opening Cocktail Party**

2nd Day : Oct. 4, 2004 (Monday)

09:00-10:00 **Invited Talk 2**

Chair: **Ryoichi Sasaki** (Tokyo Denki Univ., Japan)

Building trust relationship between PKIs : Focus on Certificate Policy

Junghee Kim (KISA, Korea)

10:00-10:20 Coffee Break

10:20-12:00 **Regular papers**

Chair: **Chi-Sung Laih** (Nat'l Cheng Kung Univ., Taiwan)

Evaluation of Total Cost in Hysteresis Signature Systems

Yusuke Ueda, Ryoichi Sasaki (Tokyo Denki Univ., Japan),

Hiroshi Yoshiura (Univ. of Electro-Communications, Japan),

Seiichi Susaki, Kunihiko Miyazaki (Hitachi, Japan)

User-side Forward-dating Attack on Time-stamping Protocol

Shin'ichiro Matsuo, Hiroaki Oguro (NTT DATA Corporation, Japan)

Towards a Flexible Intra-Trustcenter Management Protocol

Vangelis Karatsiolis, Marcus Lippert, Alexander Wiesmaier, Anna Pitaev, Markus Ruppert, Johannes Buchmann (Darmstadt Univ. of Technology, Germany)

Extensible Personal Authentication Framework using Biometrics and PKI

Koji Okada, Tatsuro Ikeda, Hidehisa Takamizawa, Toshiaki Saisho (TOSHIBA Solutions Corporation, Japan)

12:00-14:00 Lunch

14:00-15:00 **Invited Talk 3** Chair: *Hideki Imai (Univ. of Tokyo, Japan)*

Post-quantum signatures

Johannes Buchmann (Darmstadt Univ. of Technology, Germany)

15:00-16:00 **Poster Paper Session**

Proposal on Bio-PKI in which DNA Personal Identifier is embedded in Public Key

Yukio Itakura, Shigeo Tsujii (Chuo Univ., Japan)

A New Certificate Validation Scheme for Simplifying Digital Signature Verification on Verifier

*Yeon Hee Choi (Korea Polytechnic Univ., Korea),
Mi Og Park, Moon Seog Jun (Soongsil Univ., Korea)*

Action Research for PKI Interoperability

Yo Ishigaki, Yasushi Matsumoto (SECOM, Tokyo)

Design and Implementation of a RFC3161-Compliant Time-Stamping Service

*Chung-Huang Yang, Chih-Ching Yeh (National Kaohsiung Normal Univ., Taiwan),
Fang-Dar Chu (Chunghua Telecom, Taiwan)*

Payment PKI based on EMV and Efficient IC Card Authentication Mechanism

Sang-Heon Song, Jong-Hu Lee, Jae-Cheol Ryou (Chungnam National Univ., Korea)

16:00-17:30 **Panel A**

Killer Application of PKI

Chairperson: Kwangjo Kim (ICU, Korea)

17:30-18:30 **Invited Talk 4** Chair: *Jae-cheol Ryou (Chungnam Nat'l Univ., Korea)*

Current topics on Mobile PKI

Toshiaki Tanaka (KDDI Lab., Japan)

19:00-21:00 **Welcome Banquet**

3rd Day : Oct. 5, 2004 (Tuesday)

09:00-10:00	Invited Talk 5 Chair: Kouichi Sakurai (Kyushu Univ., Japan) Various certificates and their applications in PKI <i>Chi-Sung Laih</i> (National Cheng Kung Univ., Taiwan)
10:00-10:20	Coffee Break
10:20-11:50	Panel B On long-term security of public-key technology Chairperson: Tsuyoshi Takagi (TUD, Germany)
11:50-12:10	Coffee Break
12:10-13:00	Recent Results A new attack against SFLASH <i>Jintai Ding</i> (Univ. of Cincinnati, USA) Aryabhata Remainder Theorem: Relevance to public-key crypto-algorithms <i>T.R.N. Rao</i> (Univ. of Louisiana at Lafayette, USA) <i>Chung-Huang Yang</i> (National Kaohsiung Normal Univ., Taiwan) A Study on Confidentiality of Biometrics Information on Biometrics Authentication Process in BioPKI <i>Yoshifumi Ueshige</i> (Institute of Systems & Information Technologies/Kyushu, Japan) Enhancing security of Security-Mediated PKI by one-time ID <i>Satoshi Koga, Kenji Imamoto</i> (Kyushu Univ., Japan) Security in Personal Area Network <i>Jong-Phil Yang</i> (Pukyong National Univ., Korea)
13:00	Workshop closing – "The 4th IWAP (2005)" announcement