

Final Program of PKC2001

Tutorial, invited talks and regular sessions (presentation time : 25 min.) will be conducted at Halla Hall.
Reception, Banquet and Lunch will be served at Lotus Hall.

February 12 (Monday) 2001

16:00 ~ Registration

20:00 ~ 22:00 Special Tutorial for Braid Cryptosystems [Chair : Jongin Lim]

Day 1 : February 13 (Tuesday) 2001

08:00 ~ Registration

09:00 ~ 09:10 Opening Address [Kwangjo Kim]

09:10 ~ 10:00 Invited Talk 1 [Session Chair : Yuliang Zheng]

“Provably-Secure Public-Key Cryptosystems”, Mihir Bellare (*UC San Diego, USA*)

10:00 ~ 10:30 Coffee Break

10:30 ~ 12:10 Session 1. Provably Secure Encryption [Session Chair : Arjen K. Lenstra]

“On the Security of a Williams Based Public Key Encryption Scheme”, Siguna Müller (*U. of Klagenfurt, Austria*)

“Semantically Secure McEliece Public-Key Cryptosystems-Conversions for McEliece PKC-”, Kazukuni Kobara, Hideki Imai (*U. of Tokyo, Japan*)

“IND-CCA Public Key Schemes Equivalent to Factoring $n=pq$ ”, Kaoru Kurosawa, Wakaha Ogata, Toshihiko Matsuo, Shuichi Makishima (*Tokyo Inst. of Tech., Japan*)

“A Generalisation, a Simplification and some Applications of Paillier’s Probabilistic Public- Key System”
Ivan Damgård, Mads Jurik (*U. of Aarhus, Denmark*)

12:10 ~ 13:30 Lunch Break

13:30 ~ 15:10 Session 2. Public Key Primitives [Session Chair : Sung Jun Park]

“A New Aspect for Security Notions : Secure Randomness in Public-Key Encryption Schemes”, Takeshi Koshihara (*Fujitsu, Japan*)

“Identification, Signature and Signcryption Using High Order Residues Modulo an RSA Composite”, Yuliang Zheng (*Monash U., Australia*)

“On the Security of Lenstra’s Variant of DSA without Long Inversions”, Arjen K. Lenstra (*Citibank, USA*), Igor E. Shparlinski (*Macquarie U., Australia*)

“Fast Irreducibility and Subgroup Membership Testing in XTR”, Arjen K. Lenstra (*Citibank, USA*), Eric R. Verheul (*PricewaterhouseCoopers, Netherlands*)

15:10 ~ 15:40 Coffee Break

15:40 ~ 17:45 Session 3. New Notions and Proactive Security [Session Chair : Takashi Mano]

“The Gap-Problems: a New Class of Problems for the Security of Cryptographic Schemes”, Tatsuki Okamoto (*NTT, Japan*), David Pointcheval (*ENS, France*)

“Marking: A Privacy Protecting Approach Against Blackmailing”, Dennis Kügler, Holger Vogt (*Darmstadt U. of Tech., Germany*)

“Adaptive Security for the Additive-Sharing Based Proactive RSA”, Yair Frankel (*Ecash Tech. USA*), Philip D. MacKenzie (*Bell Labs, USA*), Moti Yung (*CertCo, USA*)

“Robust Forward-Secure Digital Signature Schemes with Proactive Security”, Wen-Guey Tzeng, Zhi-Jia Tzeng (*Nat. Chiao Tung U., Taiwan*)

“Equitability in Retroactive Data Confiscation versus Proactive Key Escrow”, Yvo Desmedt (*Florida State U., USA*), Mike Burmester (*Royal Holloway U. of London, UK*), Jennifer Seberry (*U. of Wollongong, Australia*)

18:30 Reception

Day 2 : February 14 (Wednesday) 2001

09:00 ~ 09:50 Invited Talk 2 [Session Chair : Ki-Yoong Hong]

“Towards National PKI in Korea”, Jun-Cheol Yang (*MIC, Korea*)

09:50 ~ 10:20 Coffee Break

10:20 ~ 12:25 Session 4. Public Key Infrastructure [Session Chair : Yvo Desmedt]

"Efficient Revocation in Group Signatures", Emmanuel Bresson, Jacques Stern (*ENS, France*)

"A Public Key Traitor Tracing Scheme with Revocation Using Dynamic Shares",

Wen-Guey Tzeng, Zhi-Jia Tzeng (*Nat. Chiao Tung U., Taiwan*)

"Efficient Asymmetric Self-Enforcement Scheme with Public Traceability",

Hirofumi Komaki, Yuji Watanabe, Goichiro Hanaoka, Hideki Imai, (*U. of Tokyo, Japan*)

"A PVSS as Hard as Discrete Log and Shareholder Separability",

Adam Young (*Columbia U., USA*), Moti Yung (*CertCo, USA*)

"One Round Threshold Discrete-Log Key Generation without Private Channels",

Pierre-Alain Fouque, Jacques Stern (*ENS, France*)

12:25 ~ 14:00 Lunch Break

14:00 ~ 15:40 Session 5. Cryptanalysis [Session Chair : Susanne Wetzel]

"Cryptanalysis of Two Sparse Polynomial Based Public Key Cryptosystems", Feng Bao, Robert H. Deng

(*Kent Ridge Digital Labs, Singapore*), Willi Geiselmann (*U. of Karlsruhe, Germany*), Claus Schnorr

(*Frankfurt U., Germany*), Rainer Steinwandt (*U. of Karlsruhe, Germany*), Hongjun Wu (*Kent Ridge Digital Labs, Singapore*)

"Cryptanalysis of PKP : A new approach", Éliane Jaulmes, Antoine Joux (*DCSSI, France*)

"Cryptanalysis of a Digital Signature Scheme on ID-Based Key-Sharing Infrastructures", Hongjun Wu, Feng Bao, Robert H. Deng (*Kent Ridge Digital Labs, Singapore*)

"Loopholes in Two Public Key Cryptosystems Using the Modular Group", Rainer Steinwandt (*U. of Karlsruhe, Germany*)

15:40 ~ 16:10 Coffee Break

16:10 ~ 17:50 Session 6. Digital Signatures and Cryptographic Protocols [Session Chair : Moti Yung]

"Secure Server-Aided Signature Generation", Markus Jakobsson, Susanne Wetzel (*Bell Labs, USA*)

"Efficient Long-term Validation of Digital Signatures",

Arne Ansper, Ahto Buldas, Meelis Roos, Jan Willemson (*Cybernetica, Estonia*)

"Remarks on Mix-network Based on Permutation Networks", Masayuki Abe, Fumitaka Hoshino (*NTT, Japan*)

"New Key Recovery in WAKE protocol", Chong Hee Kim, Pil Joong Lee (*POSTECH, Korea*)

18:30 Banquet

Day 3 : February 15 (Thursday) 2001

09:00 ~ 09:50 Invited Talk 3 [Session Chair : Tatsuaki Okamoto]

"An Outline of ETC System in Japan – Security ensured in interconnectable and interoperable ETC System", Ko Itoh (Organization for Road System Enhancement, Japan)

09:50 ~ 10:20 Coffee Break

10:20 ~ 12:00 Session 7. Implementation [Session Chair : Kyung Hyune Rhee]

"Redundant Representation of Finite Fields", Willi Geiselmann, Harald Lukhaub (*U. of Karlsruhe, Germany*)

"Compact Encoding of Non-adjacent Forms with Applications to Elliptic Curve Cryptography",

Marc Joye, Christophe Tymen (*Gemplus, France*)

"Efficient Implementation of Elliptic Curve Cryptosystems on the TI MSP430x33x Family of Microcontrollers",

Jorge Guajardo (*WPI, USA*), Rainer Blümel, Uwe Krieger (*Cryptovision, Germany*), Christof Paar (*WPI, USA*)

"A Novel Systolic Architecture for an Efficient RSA Implementation",

Nikos K. Moshopoulos, K.Z. Pekmestzi (*Nat. Tech. U. of Athens, Greece*)

12:00 ~ 13:00 Lunch Break

13:00 Adjourn

13:30 ~ Guided Tour