INDOCRYPT 2000

First International Conference on Cryptology in India
Indian Statistical Institute, Calcutta, India
10–13 December 2000
http://www.isical.ac.in/~indocrypt

Programme

10 December, 2000

1030–1130 : **Tutorial I**

Number Theory and Cryptography
Prof. R. Balasubramaniam Inst. of Mathematical Sciences, Chennai

1130–1230 : **Tutorial II**

Complexity in Cryptography
Prof. K. Sikdar Indian Statistical Institute, Calcutta

1330–1415 : **Tutorial III**

Payment Systems and E-Cash and Related Authentication
Prof. C E Veni Madhavan Indian Institute of Science, Bangalore

1415–1500 : **Tutorial IV**

Sequences and Stream Cipher
Prof. Cunsheng Ding Hong Kong Univ. of Science and Technology

1500–1545 : **Tutorial V**

Differential Cryptanalysis
Prof. Eli Biham Technion–Israel Inst. Of Technology

1630–1730 : **Inauguration**

Dr. N. Vittal Chief Vigilance Commissioner, Govt. of India

Special Guest: *Dr. K. N. Gupta* Controller of Certifying Auth., Govt. of India

11 December, 2000

0930–1030 : **Invited Talk**

Cryptographic Protocols and Their Complexities
Prof. Adi Shamir M.I.T., USA

1100–1300 : **1. E-cash and Multi-party Computation**

An online, transferable E-cash payment system
R. Sai Anand, C. E. Veni Madhavan IISC Bangalore

Anonymity control in Multi-bank E-cash system
Ik Rae Jeong, Dong Hoon Lee Korea University

Efficient Asynchronous Secure Multiparty Distrilbuted Computation
K. Srinathan, C. Pandu Rangan IIT Madras

Tolerating Generalized Mobile Adversaries in Secure Multi-party Computation
K. Srinathan, C. Pandu Rangan IIT Madras

1400–1530 : **2. Stream Ciphers and Boolean Function**

The correlation of a Boolean function with its variable
Dingyi Pei, Wenliang Qin State Key Lab. Of Inf. Security, China

On choice of connection-polynomials for LFSR-based Stream Ciphers
K.Jambunathan ISI Calcutta

On resilient Boolean function with maximal possible nonlinearity
Yuriy V. Tarannikov Mech. and Math. Dept, Moscow State University, Russia

1600–1700 : **3. Cryptanalysis I**

Decimation attack of stream ciphers

Eric Filiol INRIA, France

Cryptanalysis of the A5/1 GSM Stream Cipher
Eli Biham, Dunkelman Orr Technion – Israel Inst. Of Technology , Israel

12 December, 2000

0930–1030 : Invited Talk

On the Selection of the Advanced Encryption Standard
Prof. Eli Biham Technion – Israel Inst. Of Technology , Israel

1100–1200 : 4. Elliptic Curve

Power Analysis Breaks Elliptic Curve Cryptosystem Even Secure Against the Timing Attack
Katsuyuki Okeya Hitachi Ltd., Japan, *Kouichi Sakurai* Kyushu Univ., Japan

Efficient Construction of Cryptographically Strong Elliptic Curves
Harald Baier, Johannes Buchmann Univ. of Tech. , Germany

1200–1300 : 5. Fast Arithmetic

High speed software multiplication in F2m
Lopez Julio Cesar Univ. of Valle, Colombia, *Ricardo Dahab* State Univ. of Campinas, Brazil

On Efficient Normal Basis Multiplication
Arash Reyhani-Masoleh, Anwar Hasan Univ. of Waterloo, Canada

1400–1530 : 6. Digital Signature

Codes identifying Bad Signatures in Batches
Jaroslaw Pastuszak Polish Academy of Sc. ,Poland, *Josef Pieprzyk, Jennifer Seberry* Univ. of Wollongong , Australia

Distributed Signcryption
Yi Mu, Vijay Varadharajan Univ. of Western Sydney, Australia

Fail-Stop Signature for Long Messages
Willy Susilo, Rei Safavi-Naini, Huaxiong Wang Univ. of Wollongong, Australia

1600–1730 : 7. Cryptographic Protocols

Symmetrically private information retrieval (Extended Abstract)
Sanjeev Kumar Mishra CISCO Systems Pvt. Ltd., India, *Palash Sarkar* Univ. of Waterloo, Canada

Two-Pass Authenticated Key Agreement Protocol with Key Confirmation
Kwangjo Kim, Bo-Yeon Song Inf. and Communications Univ., S. Korea

Anonymous Traceability Schemes with Unconditional Security
R Safavi-Naini, Y Wang Univ. of Wollongong , Australia

13 December, 2000

0930–1100 : 8. Cryptanalysis II

On Bias Estimation in Linear Cryptanalysis
Ali Aydin Selcuk University of Maryland, USA

On the Incomparability of Entropy and Marginal Guesswork in Brute-Force Attacks
John Pliam LASEC, EPFL, Switzerland

Improved Impossible Differentials on Twofish
Eli Biham, Vladimir Furman Technion – Israel Inst. Of Technology , Israel

1130–1300 : 9. Block Cipher and Public Key Cryptography

New Block Cipher DONUT Using Pairwise Perfect Decorrelation
Dong Hyeon Cheon, Sang Jin Lee, Jong In Lim CIST, Korea Univ., Korea, *Sang Jae Lee* Korea Info. Security Agency, Korea

Generating RSA Keys on a Handheld Using an Untrusted Server
D. Boneh, N. Modadugu, M. Kim Stanford Univ., USA

A Generalised Takagi-Cryptosystem with a module of form prqs
Seongan Lim, Seungjoo Kim, Hongsub Lee Korea info. Security Agency, Korea, *Ikkowan Yie* Inha Univ, Korea