



National Workshop on Cryptology 2004

An annual event of Cryptology Research Society of India



Venue: AMRITA Vishwa Vidyapeetham, Amritapuri, Kollam, Kerala. Date: 10 to 12 September, 2004.

Programme Schedule

Day 1 (10th Sept. 2004)

9:00 AM – 10:30 AM	Inaugural Session	
	<i>Welcome Address</i>	<i>Sri. Indra Mohan, Vice President, ARL, Amrita Vishwa Vidyapeetham.</i>
	<i>Presidential Address</i>	<i>Prof. Bimal Roy, Professor, ISI Kolkatta</i>
	<i>Chief Guest</i>	<i>Dr. N. Sitaram (Director, CAIR)</i>
	<i>Keynote Address</i>	<i>Rear Admiral .S. Balachandran (Director General, WESEE)</i>
	<i>Talk by</i>	<i>Shri. K.A. Menon (Executive Director, Dhanalakshmi Bank Limited)</i>
	<i>Vote of Thanks</i>	<i>Dr. K.B .M. Namboodiripad, Dean, Amrita Vishwa Vidyapeetham, Amritapuri Campus.</i>
10:30 AM – 11:30 AM	Basic Concepts Regarding Stream Ciphers as Finite State Machines <i>Dr Jovan Golic, Scientist, Telecom Italia, Italy</i>	
11:30 AM – 11:50 AM	Tea break	
Session 1		
Session Chair: Dr Veni Madhavan		
11:50 AM – 12:20 PM	Stream Cipher Cryptography-A Practitioner's Perspective <i>Dr N Krishnan, Retd. Director, Joint Cipher Bureau, Ministry of Defence</i>	
12:20 PM – 12:40 PM	Software Implementation of a Crypto Layer using Elliptic Curve Cryptography <i>Sharavan Kumar, B R Ivan, S D Dhodapkar (RCnD, BARC)</i>	
12:40 PM – 01:00 PM	Non Trivial Solutions to Cubic Sieve Congruence $X^3 = Y^2 * Z \text{ Mod } P$ <i>S Maitra, Y V Subha Rao, (ISI, Calcutta)</i> <i>P Stancia (Auburn University)</i> <i>S Gangopadyaya (Dept. of IT, Lund University)</i>	
01:00 PM – 01:20 PM	A Deniable One-Way-Function-Based Identification Scheme <i>Bri Ratna</i> <i>Lecturer in Computer Science</i> <i>Amritapuri Campus, Amrita Vishwa Vidyapeetham</i>	
01:20 PM – 02:20 PM	Lunch break	
Session 2		
Session Chair: Prof. Dr Bimal Roy		
02:20 PM – 02:50 PM	Theoretical & Practical Aspects of Integer Factoring <i>Prof. Veni Madhavan, Professor, Computer Science and Automation, Indian Institute of Science</i>	
02:50 PM – 03:10 PM	Landau Ramanujan Keyed Hash Function for Message Authentication <i>A Suganya, N Vijaya Rangan (SETS, Chennai)</i>	
03:10 PM – 03:30 PM	A New Online Extended Visual Cryptography Scheme for STS Access Structure <i>Sucheta Chakrabarti, S K Pal (SAG, DRDO)</i>	
03:30 PM – 03:50 PM	Implementation and Performance Analysis of Image Authentication Technique	

	A Shanmugham, Uma Maheshawari (PSG Tech, Coimbatore)
03:50 PM – 04:10 PM	Tea break
Session 3	
Session Chair: Dr Sharad Sane	
04:10 PM – 04:40 PM	Efficient Computation of Tate Pairing Prof Dr Rana Barua, Professor, ISI Kolkotta
04:40 PM – 05:00 PM	A New Audio Secret Sharing Scheme S Krishnan, Dr V Sadasivam (Manomanium, Sundaranar University)
05:00 PM – 05:20 PM	Cryptography Using Lorenz Dynamics B R Ivan, S D Dhodapkar (RCnD, BARC) Q V Lawande (TPD, BARC)
05:20 PM – 05:40 PM	Cryptography Technique for Surveillance and Detection of Counterfeit Currency Dr M V N K Prasad, Milind, A Saxena (IDRBT)
05:40 PM – 06:00 PM	Short Comings in an existing DSA Integrated Key Agreement Protocol Abhishek Agarwal, Anee Das (DA-IICT)

Day 2 (11th Sept. 2004)

Session 1	
Session Chair: Prof. Dr Bimal Roy	
08:30 AM – 09:30 AM	Analysis of Stream Ciphers and Types of Stream Ciphers Dr Jovan Golic, Scientist, Telecom Italia, Italy
09:30 AM – 10:00 AM	Algebraic Attacks On Stream Ciphers Dr S S Bedi, SAG, DRDO
10:00 AM – 10:20 AM	High Speed and Secure Data Transmission Using Encrypted Text over Internet. B S Shajee Mohan, Vinod George (LBS College Engg., Kerala)
10:20 AM – 10:40 AM	Implementation of Routing Algorithm for Time Scheduling in Quantum Cryptography G Rama, E Lakshmi (VIT, Vellore)
10:40 AM – 11:00 AM	Tea break
Session 2	
Session Chair: Dr S S Bedi	
11:00 AM – 11:20 AM	Stream Ciphers Using Chaotic System Dhandapany K, Sriram B, Sundar Singh, J Sundareshan, Dr V Prithviraj (Pondicherry Engg College)
11:20 AM – 11:40 AM	Primitive Polynomial Testing Methodology R Vijayasathy, N Vijaya Rangan (SETS, Chennai)
Session 3	
Session Chair: Dr Veni Madhavan	
11:40 AM – 12:10 PM	General access Structure for B/W Visual cryptography Prof. Bimal Roy, Professor, ISI Kolkotta
12 :10 PM – 12:30 PM	Implementation of part of Qudratic Seive Algorithm in Programmable h/w Hari Babu P, Shoba P M (CDAC)
12:30 PM – 12:50 PM	Anonymous Trapdoor Primitive in Public Key Encryption Scheme Chandrabhushan (ISI, Calcutta)
12:50 PM – 01:10 PM	Fast VLSI Architectures for Implementing ECC Bri Rehna Lecturer in Electronics Amritapuri Campus Amrita Vishwa Vidhyapeetham
01:10 PM – 02:10 PM	Lunch break

Session 4	
Session Chair: Dr Saxena	
02:10 PM – 02:40 PM	IDRBT CA and Banking Applications Dr V P Gulati, Director, IDRBT
02:40 PM – 03:00 PM	An Efficient Multi Signature Scheme for E-Service Maniklal Das, A Saxena, V P Gulati (IDRBT)
03:00 PM – 03:20 PM	Intrusion Prevention Modeling and Simulation for Fast Detection DDoS Attacks M W David (Cubic Corporation) J Mitra (MDI) K Sakurai (Kyusin University)
03:20 PM – 03:40 PM	Multi Party Secure Key Exchange Algorithm Using Neural Cryptography Dr G K Patra, V Anil Kumar, R P Thangavelu (CSIR Center for Math Modeling, B'lore)
03:40 PM – 04:00 PM	Tea Break
Session 5	
Session Chair: Dr Sethu Madhavan	
04:00 PM – 04:20 PM	Performance Analysis of Network Security Protocol in Cluster Environment P R Srinivasan, V Vadehi, L Karthik (MIT Campus, Anna University)
04:20 PM – 04:40 PM	Water Marking by Bit Decomposition in Wavelet Domain Md Mansoor Roomi, B Yagameena, R Sridevi, P Hemalatha (Tyagarajar College of Engg, Madurai)
04:40 PM – 05:00 PM	IRIS Code generation and Authentication S Athinarayanan (Sethu Institute of Technology)

Day 3 (12th Sept. 2004)

Session 1	
Session Chair: Dr N Krishnan	
09:00 AM – 10:00 AM	Correlation and Algebraic Attacks Dr Jovan Golic, Scientist, Telecom Italia, Italy
10:00 AM – 10:30 AM	Orthogonal Arrays & Their Applications to Combination Locks Dr Sharad Sane, Professor, University of Mumbai
10:30 AM – 10:50 AM	Authenticated Multi-parity key agreement A provably secure Tree based scheme using pairing Ratna Dutta, Rana Barua, Palash Sarkar (Applied Statistics Unit, Calcutta)
10:50 AM – 11:10 AM	Encryption of Ground Control Point Library Data Managalamani, A Bhaskar, Mittal (NRSA)
11:10 AM – 11:30 AM	Mandatory Access Control Using Bell-lapadula Security Model for General Purpose Operating System Kernel N Sethu Subrahmanian Research Associate Amrita Research Labs Amritapuri Campus Amrita Vishwa Vidyapeetham
11:30 AM – 11:50 AM	Tea break
Session 2	
Session Chair: Shri. Suresh Kumar R	
11:50 AM – 12:00	Demo by SETS
12:00 – 12:20 PM	Secure Speech Layer Radha Lecturer in Computer Science Amritapuri Campus

	<i>Amrita Vishwa Vidyapeetham</i>
12:20 PM – 01:30 PM	Lunch
01:30 PM – 01:50 PM	Onion Routing <i>Rajesh G Nair,</i> <i>Research Associate</i> <i>Amrita Research Labs</i> <i>Amritapuri Campus</i> <i>Amrita Vishwa Vidyapeetham</i>
01:50 PM – 02:10 PM	Quad Trees Based Image Authentication <i>Latha Parameshwaran (AITEC, Ettimadai)</i> <i>Dr K Anbumani (Karunya Institute)</i>
02:10 PM – 02:30 PM	Securing Critical IT Infra Structure <i>N Rajendran, Pushap Kamal, Debabrata Nayak (IDRBT)</i> <i>Dr Albert Rabera (St. Joseph College)</i>
02:30 PM – 02:50 PM	Steganography in Audio Formats <i>Shanmuga Sundaram N, Suraj R (AITEC, Ettimadai)</i>
02:50 PM – 03:10 PM	New Observation on the Security of Rijndael Crypto System <i>Dipanwita Roy Chowdry, Debdeep Mukhopadhyay (IIT, Karagpur)</i>
03:10 PM – 03:30 PM	Tea break
03:30 PM - 04:00 PM	Feedback
04:00 PM	Valedictory Session Chief Guest: Dr. Govindarajan, BARC

Subject to Change