2009 – 2011 Cooperative Research Project:
“Security Evaluation and Design of Components and Cryptographic Primitives for RFID and Sensor Networks”

The Japan-team Visit to India, April 13-15, 2009

The First Spring Working Meeting

Venue: Indian Statistical Institute, Kolkata

Agenda of the Visit

- **Main Goal**: “Technical Discussions on Future Joint Research Activities and Regarding the 2009 Visits of India-team Members to Tokyo”
- **Lectures** on Certain Topic Candidates for joint Research Activities Related to Crypto&Coding
- **Short Technical Talks**
- **Round-table Discussions**
- Establishing **Program of the Visit and Research Directions** for Indian-team Members Visits to Japan

PARTICIPANTS

The Japan participants of the meetings

- Dr. Miodrag Mihaljevic, RCIS Invited Senior Research Scientist, Professor
- Dr. Seonghan Shin, RCIS Research Scientist, Associated Professor

The Indian participants of the meetings

1. Dr. Sugata Gangopadhyay, Assistant Professor, Department of Mathematics, Indian Institute of Technology Roorkee, Indian Team Project Leader.
2. Dr. Subhamoy Maitra, Associate Professor Applied Statistics Unit, Indian Statistical Institute Kolkata
3. Mr. Goutam Kumar Paul, Lecturer, Department of Computer Science & Engineering, Jadavpur University, Kolkata.
4. Dr. Deepak Kumar Dalai, Lecturer, School of Mathematics National Institute of Science Education and Research Bhubaneswar

List of Delivered Lectures

Lecture 1:
M. Mihaljevic, “**Towards Low Complexity and Highly Secure Cryptographic Primitives Which Involve Pure Randomness and Dedicated Coding: On Algebraic Representation and Security Evaluation of Certain Stream Ciphers which Involve Randomness”**

Lecture 2:
M. Mihaljevic, “**Wire-Tap Channel System and Dedicated Coding”**

Lecture 3:
S. Shin, **“Linear-Code Based Public-Key Cryptosystem”**

Lecture 4:
S. Maitra, **“Simulating A Large Pseudo-Random Permutation Using Several Smaller Ones”**

Lecture 5:
G. Paul, **“Fast and Effcient Key Recovery from RC4 Permutation after KSA”**