

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

*List of the Meetings and Participants
The Japan-team Visit to India, February 10-14, 2009*

***I. Kick-off Meeting,
Indian Statistical Institute, Kolkata, February 10, 2009***

Agenda of the meeting

1 5min	Opening Remarks by Japan-team Leader	- Hajime Watanabe (RCIS-AIST, Tokyo)
5min	Welcome Message	- Rajiv Sharma (DST, New Delhi)
5min	Welcome Message	- Bimal Roy (ISI, Kolkata)
5min	Opening Remarks by Indian-team Leader	- Sugata Gangopadhyay (IIT Roorkee)
2 10min	A Brief Overview on RCIS-AIST (including Q & A)	Kazukuni Kobara (RCIS-AIST, Tokyo)
3 10min	An Overview of the Project Goals and Realization Issues	Miodrag Mihaljevic (RCIS-AIST, Tokyo)
5min	Q & A	
4 up to 5min	introduction of Manabu Hagiwara, Seonghan Shin and Goutam Kumar Paul	Miodrag Mihaljevic (RCIS-AIST, Tokyo)
5 10min	“Code-Based PKC”	Manabu Hagiwara (RCIS-AIST, Tokyo)
5min	Q & A	
6 10min	“Authentication for RFID and Sensor Networks”	Seonghan Shin (RCIS-AIST, Tokyo)
5min	Q & A	
7 10min	“Cryptanalysis of RC4-like Stream Ciphers”	Goutam Kumar Paul (JU, Kolkata)
5min	Q & A	
8 10min	“Affine Equivalence of Boolean Functions”	Sugata Gangopadhyay (IIT, Roorkee)
5min	Q & A	
9 up to 30min	Round Table Discussion on the Project Realization Issues and the Achievements Dissemination	Moderator Miodrag Mihaljevic (RCIS-AIST, Tokyo)

PARTICIPANTS

The Japan participants of the meeting

- Dr. Hajime Watanabe, RCIS Deputy Director, Professor, Japan Team Project Leader
- Dr. Kazukuni Kobara, RCIS Principal Research Scientist, Professor
- Dr. Manabu Hagiwara, RCIS Research Scientist, Associated Professor
- Dr. Seonghan Shin, RCIS Research Scientist, Associated Professor
- Dr. Miodrag Mihaljevic, RCIS Invited Senior Research Scientist, Professor

The Indian participants of the meeting

1. Prof. Bimal Kumar Roy, Professor-in-Charge, Applied Statistics Unit, Indian Statistical Institute Kolkata.
2. Prof. Aditya Bagchi, Dean of Studies, Indian Statistical Institute Kolkata.
3. Dr. Rajiv Sharma, Advisor, International Division, Department of Science and Technology (DST) India.
4. Dr. Subhamoy Maitra, Associate Professor Applied Statistics Unit, Indian Statistical Institute Kolkata.
5. Dr. Sugata Gangopadhyay, Assistant Professor, Department of Mathematics, Indian Institute of Technology Roorkee, Indian Team Project Leader.
6. Mr. Goutam Kumar Paul, Lecturer, Department of Computer Science & Engineering, Jadavpur University, Kolkata.
7. Dr. Avishek Adhikari, Lecturer, Department of Pure Mathematics, University of Calcutta.
8. Ms. Sushmita Ruj, Research Scholar, Applied Statistics Unit, Indian Statistical Institute Kolkata.

II. Evening Meeting in Jadavpur University Kolkata, February 10, 2009

Agenda of the meeting: Discussions with the students.

PARTICIPANTS

The Japan participants of the meeting

- Dr. Hajime Watanabe, RCIS Deputy Director, Professor, Japan Team Project Leader
- Dr. Kazukuni Kobara, RCIS Principal Research Scientist, Professor
- Dr. Manabu Hagiwara, RCIS Research Scientist, Associated Professor
- Dr. Seonghan Shin, RCIS Research Scientist, Associated Professor
- Dr. Miodrag Mihaljevic, RCIS Invited Senior Research Scientist, Professor

The Indian participants of the meeting

1. Dr. Subhamoy Maitra, Associate Professor, Applied Statistics Unit, Indian Statistical Institute Kolkata.
2. Mr. Goutam Kumar Paul, Lecturer, Department of Computer Science & Engineering, Jadavpur University, Kolkata.
3. Dr. Sugata Gangopadhyay, Assistant Professor, Department of Mathematics, Indian Institute of Technology Roorkee, Indian Team Project Leader.
4. Dr. Ujjwal Maulik, Professor, Department of Computer Science & Engineering, Jadavpur University.
5. Mr. Amit K. Mistry, Graduate Student (Masters in Computer Science & Engineering), Jadavpur University.
6. Mr. Abhra Maity, Graduate Student (Masters in Computer Science & Engineering), Jadavpur University.

III. Morning meeting with the Director of IIT, Roorkee, February 12, 2009

Agenda of the meeting

- Welcome messages
- Brief presentation of the Project (Miodrag Mihaljevic)
- Brief presentation of RCIS-AIST (Kazukuni Kobara)
- Discussions

PARTICIPANTS

The Japan participants of the meeting

- Dr. Hajime Watanabe, RCIS Deputy Director, Professor, Japan Team Project Leader
- Dr. Kazukuni Kobara, RCIS Principal Research Scientist, Professor
- Dr. Manabu Hagiwara, RCIS Research Scientist, Associated Professor
- Dr. Seonghan Shin, RCIS Research Scientist, Associated Professor
- Dr. Miodrag Mihaljevic, RCIS Invited Senior Research Scientist, Professor

The Indian participants of the meeting

1. Prof. S. C. Saxena, Director, Indian Institute of Technology Roorkee.
2. Prof. Surendra Kumar, Dean, Finance and Planning, Indian Institute of Technology Roorkee.
3. Prof. Rama Bhargava, Head, Department of Mathematics, Indian Institute of Technology Roorkee.
4. Dr. Sugata Gangopadhyay, Assistant Professor, Department of Mathematics, Indian Institute of Technology Roorkee, Indian Team Project Leader.

Note on the important initiative: Director of IIT has proposed consideration of establishment of a Centre for Information Security within IIT (New Delhi location).

IV. Afternoon meeting with the Department members of IIT, Roorkee, February 12, 2009

Agenda of the meeting

- Welcome messages
- Brief presentation of the Project
- Brief presentation of RCIS-AIST (Kazukuni Kobara)
- Technical talk “Code-Based PKC” (Manabu Hagiwara)
- Discussions

PARTICIPANTS

The Japan participants of the meeting

- Dr. Hajime Watanabe, RCIS Deputy Director, Professor, Japan Team Project Leader
- Dr. Kazukuni Kobara, RCIS Principal Research Scientist, Professor
- Dr. Manabu Hagiwara, RCIS Research Scientist, Associated Professor
- Dr. Seonghan Shin, RCIS Research Scientist, Associated Professor
- Dr. Miodrag Mihaljevic, RCIS Invited Senior Research Scientist, Professor

The Indian participants of the meeting

1. Prof. Rama Bhargava, Head, Department of Mathematics, Indian Institute of Technology Roorkee.
2. Prof. G. S. Srivastava, Dean Academic Studies, Indian Institute of Technology Roorkee.
3. Prof. D. K. Mehra, Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee.
4. Prof. T. R. Gulati, Department of Mathematics, Indian Institute of Technology Roorkee.
5. Prof. V. K. Katiyar, Department of Mathematics, Indian Institute of Technology Roorkee.
6. Prof. R. C. Mittal, Department of Mathematics, Indian Institute of Technology Roorkee.
7. Prof. S. P. Sharma, Department of Mathematics, Indian Institute of Technology Roorkee.
8. Dr. G. S. Agarwal, Associate Professor, Department of Mathematics, Indian Institute of Technology Roorkee.
9. Dr. Aditi Gangopadhyay, Assistant Professor, Department of Mathematics, Indian Institute of Technology Roorkee.
10. Dr. Sandip Banerjee, Assistant Professor, Department of Mathematics, Indian Institute of Technology Roorkee.
11. Dr. Sugata Gangopadhyay, Assistant Professor, Department of Mathematics, Indian Institute of Technology Roorkee, Indian Team Project Leader.
12. Dr. Madhu Jain, Assistant Professor, Department of Mathematics, Indian Institute of Technology Roorkee.