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

Kick-Off Meeting

India, Kolkata,

Indian Statistical Institute

February 10, 2009

Moderator: Miodrag Mihaljevic

Partner Institutions

J A P A N

- Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Tokyo

I N D I A

- Department of Mathematics, Indian Institute of Technology (IIT), Roorkee
- Applied Statistics Unit, Indian Statistical Institute (ISI), Kolkata
- Department of Computer Science & Engineering, Jadavpur University (JU), Kolkata

RCIS - AIST

- Dr. Hajime Watanabe, Deputy Director, Project Leader, Professor
- Dr. Kazukuni Kobara, Principal Research Scientist, Professor
- Dr. Manabu Hagiwara, Research Scientist, Associate Professor
- Dr. SeongHan Shin, Research Scientist, Associate Professor
- Dr. Miodrag Mihaljevic, Invited Senior Research Scientist, Professor

Indian Team

- Dr. Sugata Gangopadhyay, Assistant Professor, IIT Roorkee, Project Leader
- Dr. Subhamoy Maitra, Associate Professor, ISI Kolkata
- Mr. Goutam Paul, M.S., Lecturer, Jadavpur University, Kolkata
- Dr. Deepak Dalai, Visiting Faculty, IIT Roorkee
- Manish Garg, M.Sc., Research Scholar, IIT Roorkee
- Ankita, M.Sc., Research Scholar, IIT Roorkee

AGENDA of the Visit

Visit Day / Date	Time	Activity	Indian-side Host (Name, Title, Institution)
First Day, February 09	Morning Night	Departure from Tokyo, Narita (11:30) Arrival to Kolkata (20:35)	
Second Day, February 10	Morning 10-11 A.M Morning/ Afternoon 11:15 – 14:30 Evening 17-18	Visit to Indian Statistical Institute, Kolkata (ISI) **Project Kick-Off Meeting at ISI** Visit to Jadavpur University, Kolkata (JU)	- Bimal Roy, Professor, ISI - Subhamoy Maitra Associate Professor, ISI -Sugata Gangopadhyay, Assistant Professor, IIT -Goutam Kumar Paul, Lecturer, JU
Third Day, February 11	Morning Evening / Night	- Flight Kolkata – New Delhi - Ground transportation from New Delhi to Roorkee (5 hours) - Arrival to Roorkee	Sugata Gangopadhyay, Assistant Professor, IIT
Fourth Day, February 12	Morning/Afternoon	- Visit to Indian Institute of Technology Roorkee (IIT) - Meeting with IIT Director -Meeting with Math. Department Members	Sugata Gangopadhyay, Assistant Professor, IIT
Fifth Day, February 13	Morning Evening	- Ground Transportation from Roorkee to New Delhi (5 hours) - “Red Fort” visit: Heritages of India (as an additional stimulation for Japan-India joint efforts)	Sugata Gangopadhyay, Assistant Professor, IIT
Sixth Day, February 14		Departure from New Delhi to Tokyo (7:45 A.M.)	

AGENDA of the Kick-Off Meeting

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

Project:

“Security Evaluation and Design of Components and Cryptographic Primitives for RFID and Sensor Networks”

An Overview of the Project Goals and Realization Issues

Miodrag Mihaljevic

The Motivation and Goals

- The main motivation for this project is **aggregation of certain expert powers between Japan and India in order to cope with the challenges of information security** when only low complexity cryptographic techniques can be implemented with a particular focus towards RFID (Radio Frequency Identification) and sensor networks/systems.
- Particularly the research focus will be related towards techniques which require **simple hardware and minimize additional power consumption**.
- The project goals include **security evaluation and design of dedicated cryptographic components** and primitives within the specified scenarios.

A Specific Feature of the Project

- A main specific feature of this project is that it focuses on **the design and security evaluation** of the low complexity cryptographic primitives **employing the results and approaches developed in coding theory** (particularly related to the channels with deletion, insertion and substitution errors and wire-tap channel coding) and combinatorial designs.

Particular Goals of the Project

- security evaluation of a number of approaches related to coding theory and combinatorial designs as a background for developing low complexity stream ciphers and authentication protocols as well as to provide more insights into certain existing schemes;
- design of certain components and particularly dedicated Boolean functions for certain low complexity cryptographic primitives;
- developing of low-complexity stream ciphers and authentication protocols for RFID and sensor networks;
- developing schemes for the keys pre-distribution in sensor networks;
- developing architectural elements for privacy protection in RFID and sensor networks employing low-complexity cryptographic primitives.

Basic Joint Activities

- **Mutual Visits**
- Visits of Indian-team members to Tokyo in total duration of 360 days
- Visits of Japan-team members to India in total duration of 180 days

- **Workshops**
- 2009 Workshop in Tokyo
- 2010 Workshop in India
- 2011 Workshop in Tokyo

Missions of the Joint Activities

- **Mutual visits** will be mainly dedicated to:
- **Joint work on particular research problems**
- **Search towards novel research directions** based on combining complementary research skills

- **Workshops** will be mainly dedicated to:
- **Plenary presentations and discussions** of the achieved results and prospective research topics
- **Dissemination** of the project research results to the public research community

Expected Outcomes (1)

- **Added Value** to the on going research activities at the both side
- Papers inspired and supported by the entire project activities
- **Joint Papers**
- Resulting from joint research activities mainly performed during mutual visits of the team members

Expected Outcomes (2)

- The expected outcome of the project is a number of advanced results relevant for cryptographic techniques in highly restricted implementation scenarios obtained via an extensive international collaboration.
- A particular expected novelty and common feature of these advanced cryptographic primitives for the authentication, privacy and secrecy is that they employ results and approaches from the coding theory and the combinatorial designs.

AGENDA of the Kick-Off Meeting

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

Brief Introduction of Three Project Members

- Dr. Manabu Hagiwara, Research Scientist, Associate Professor
- Dr. Seonghan Shin, Research Scientist
- Goutam Kumar Paul, Lecturer

AGENDA of the Kick-Off Meeting

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

Round Table Discussion on the Project Realization Issues and the Achievements Dissemination

Moderator

Miodrag Mihaljevic

Main Topics of the Discussion

- Project Home-Page
- Schedule of the Main Joint Activities
- Collaboration with Two Related Japan-India Projects
- Dissemination of the Project Achievements
- Other Relevant Issues

Schedule of the Main Joint Activities

- Visits of Indian-team members to RCIS-AIST, Tokyo
- Visits of Japan-team members to ISI Kolkata and IIT Roorkee
- Workshops

Collaboration with Two Related Japan-India Projects

- "Analysis of Cryptographic Algorithms and Evaluation on Enhancing Network Security Based on Mathematical Science"
- Prof. Sakurai and Prof. Bimal Roy

- "Security proofs and multidisciplinary evaluation for dynamic hierarchical key assignment schemes"
- Prof. Kanta Matsuura, The University of Tokyo, and Prof. Anish Mathuria, Dhirubhai Ambani Institute of ICT

Dissemination of the Project Achievements

- **Workshops and Workshops' Records**
- **Dedicated Publications** (if we have intentions in this direction, we should preliminary act well in advance)

Thank You Very Much for the Attention,

and

QUESTIONS Please!