**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

Meeting with IIT Director,
Roorkee, Feb. 12, 1009

# Partner Institutions

**JAPAN**

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

**INDIA**

- Department of Mathematics, Indian Institute of Technology (IIT), Roorkee
- Applied Statistics Unit, Indian Statistical Institute (ISI), Kolkata
- Department of Computer Science & Engineering, Jadavpur University (JA), 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
- Goutam Paul, M.Sc., 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

# 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.

Thank You Very Much for the Attention,

and

QUESTIONS Please!