Crypto and Security Project of Strategic Japanese-Indian Cooperative Program on Multidisciplinary Research Field, which combines Information and Communications Technology with Other Fields

Supported by Japan Science and Technology Agency & Department of Science and Technology of the Government of India

HP@ http://itslab.csce.kyushu-u.ac.jp/JIP/index.html

Kanta MATSUURA, Univ. of Tokyo
Takashi NISHIDE, Kouichi SAKURAI, Kyushu Univ.
Hajime WATANABE, AIST

RESEARCH TEAMS

Team #	Name	Affiliation
1	Prof. Kouichi SAKURAI	Kyushu University
2	Prof. Kanta MATSUURA	Tokyo University
3	Dr. Hajime WATANABE	AIST*

*: National Institute of Advanced Industrial Science and Technology

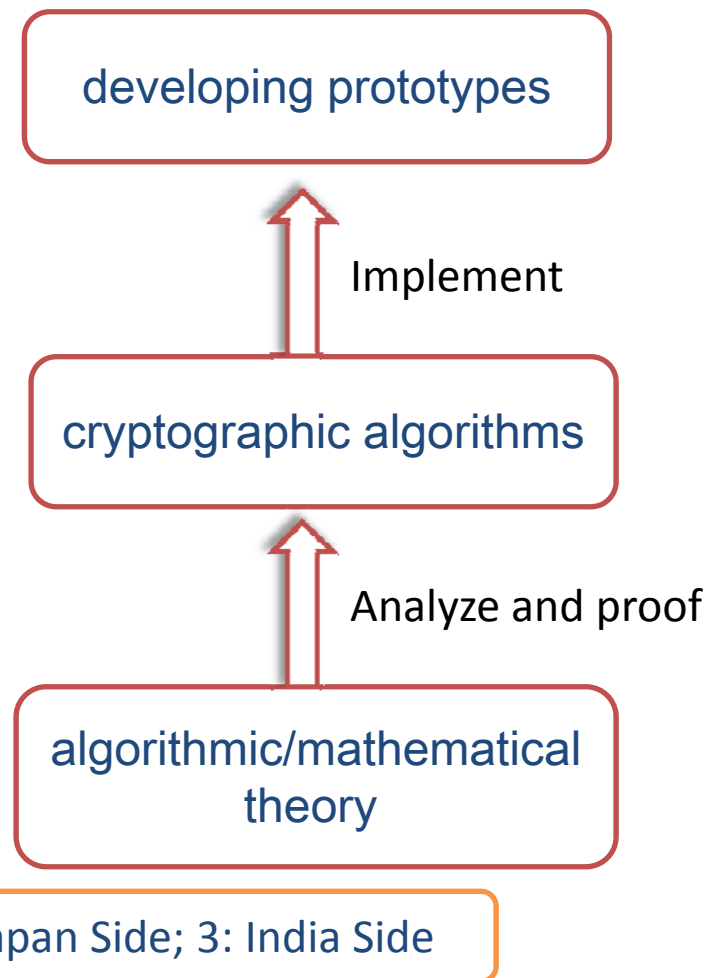| Team #	Name	Affiliation
1	Prof. Bimal ROY	Indian Statistical Institute
2	Prof. Anish MATHURIA	DA-IICT*
3	Dr. Sugata GANGOPADHYAY	India Institute of Technology

*: Dhirubhai Ambani Institute of Infomation and Communication Technology

Analysis of Cryptographic Algorithms and Evaluation on Enhancing Network Security Based on Mathematical Science
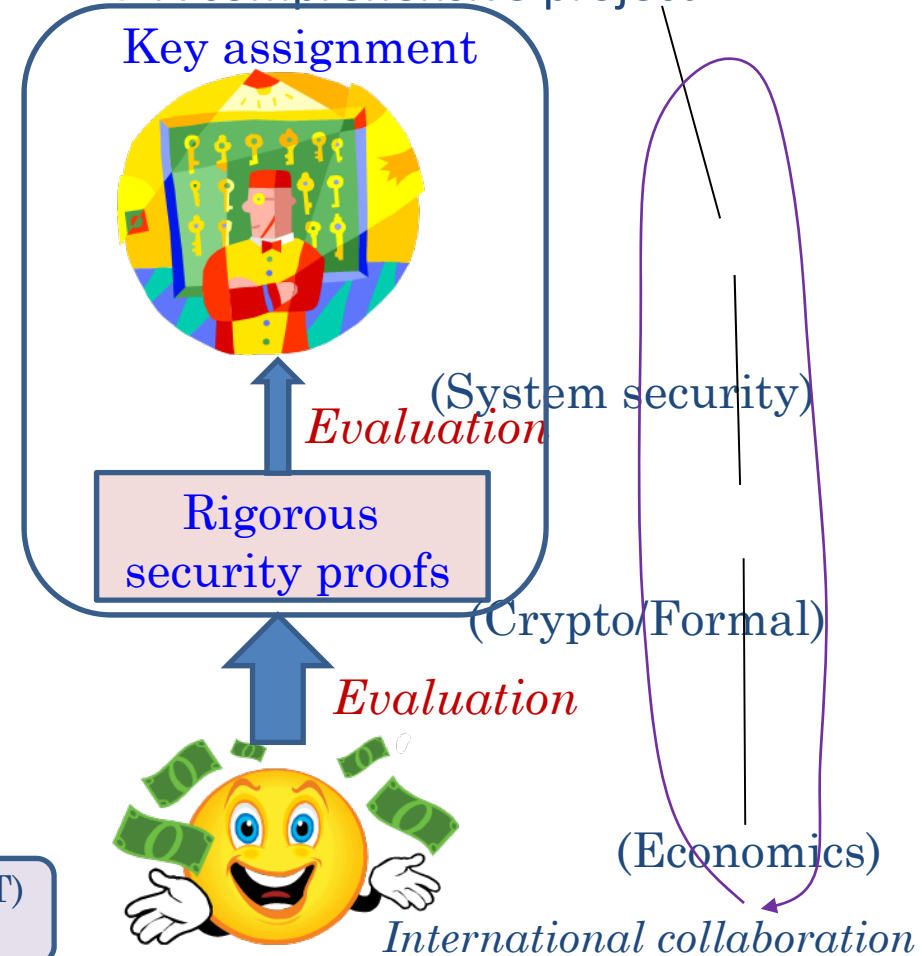
The main objects:

1. To design cryptographic algorithms, and implementation with prototype;

2. To gather information on network incident data and model them; and

3. To analyze and prove the security of cryptographic algorithms with algorithmic/mathematical theory.

developing prototypes

↑ Implement

cryptographic algorithms

↑ Analyze and proof

algorithmic/mathematical theory

1,2: Japan Side; 3: India Side

National Institute of Advanced Industrial Science and Technology
AIST

ISIT

KDDI

Security proofs and multidisciplinary evaluation for dynamic hierarchical key assignment schemes

○ The main objectives:

- (1) to develop and apply a proof model for reasoning about the security of dynamic schemes; and

- (2) to evaluate the proposed model in a multidisciplinary way.

○ The sub topics include

(3) provable security in general.

- (1) and (3) are different in terms of technology but can be evaluated in a similar manner in terms of economic impacts and implications.

(1) Anish Mathuria (Dhirubhai Ambani Institute of ICT)
(2),(3) Kanta Matsuura (The University of Tokyo)

○ A comprehensive project

Key assignment

(System security)

Evaluation

Rigorous security proofs

(Crypto/Formal)

Evaluation

(Economics)

International collaboration

- Develop highly secure functionalities in RFID and sensor network where only limited computation abilities are available

- Develop and implement highly efficient functionalities with simple hardware and low electronic power consumption

3H: High Efficiency; High Performance; High Safety

Limited computation ability

RFID/ Sensor Network

National Institute of Advanced Industrial Science and Technology
AIST

ISIT

KDDI
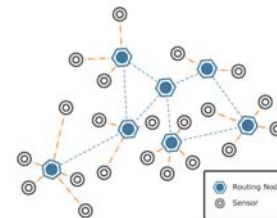
Joint Workshop Announcement

- 1st workshop held on 12th December, 2009, India

- Total 11 reports from: *Prof. Kazukuni Kobara, Dr.Avishek Adhikari,Dr. Rishiraj Bhattacharyya, Dr. Naveen Chaudhary, Dr. Yang Cui, Dr. Takashi Nishide, Dr. Junichi Takeuch, Dr. Jacob Schuldt, Dr. Subhamoy Maitr, Dr. Sugata Gangopadhyay, Dr. Miodrag Mihaljevic.*

- Main topics: *Multi-Secret Sharing Scheme, Hash Function, Code-Based Public-Key Cryptosystems, Undeniable Signature, etc.*

- 2nd workshop held in 2010 ,Japan

Call for Participation

National Institute of Advanced Industrial Science and Technology
AIST

ISIT

KDDI

STATISTICAL INDIAN INSTITUTE
UNITY IN DIVERSITY

UNIVERSITY OF CALCUTTA
ADVANCEMENT OF LEARNING

1ˢᵗ Workshop Program in India

- 9.30 -10.00 *Inauguration*

- 10.00- 10.30 *Tea*

- 10.30-11.00 *Constructions of some Multi-Secret Sharing Schemes by* Avishek Adhikari

- 11.30-12.00 *Hash Function Combiners by* Rishiraj Bhattacharyya

- 12.00-12.30 *Topic To be Decided by* Naveen Chaudhary

- 12.00 -12.30 *Tea*

- 12.30-13.00 *Some Hot Topics on Code-Based Public-Key Cryptosystems by* Prof. Kazukuni Kobara

- 13.00-13.30 *Efficient Constructions of Deterministic Encryption from Hybrid Encryption and Code-Based PKE by* Yang Cui

- 13.30-14.30 *LUNCH*

- 14.30- 15.00 *Multiparty Computation for Interval, Equality, and Comparison Without Bit-Decomposition Protocol by* Takashi Nishide

- 15.00- 15.30 *On Botnet Detection using Sparse Structure Learning by* Junichi Takeuchi

- 15.30- 16.00 *Undeniable Signatures with Delegatable Verification by* Jacob Schuldt

- 16.00-16.30 *Tea*

- 16.30-17.00 *Topic To Be Decided by* Subhamoy Maitra

- 17.00-17.30 *Third-order nonlinearities of a subclass of Kasami functions by* Sugata Gangopadhyay

- 17.30-18.00 *Secret Key Recovery of Keystream Generator LILI-128 Based on a Novel Weakness of the Employed Boolean Function by* Miodrag Mihaljevic

Thank you for your attention