

A decorative graphic consisting of a black crosshair centered over a blue square, a red square, and a yellow square. The squares are partially overlapping and have a slight gradient.

Brief Overview on RCIS-AIIST

Kaz Kobara

Research Center for Information Security,
AIIST



Introduction to AIST

- Several *AIST on the globe
 - JAIST
 - KAIST
 - NAIST
 - AIST
- They are independent orgs each other have no relation except they perform research



Introduction to AIST

- KAIST
 - Korea Advanced Institute of Science and Technology
 - Univ. in Korea
- JAIST/NAIST
 - Japan/NARA Advanced Institute of Science and Technology
 - Univ. with graduate school curriculum
- AIST
 - National Institute of Advanced Industrial Science and Technology

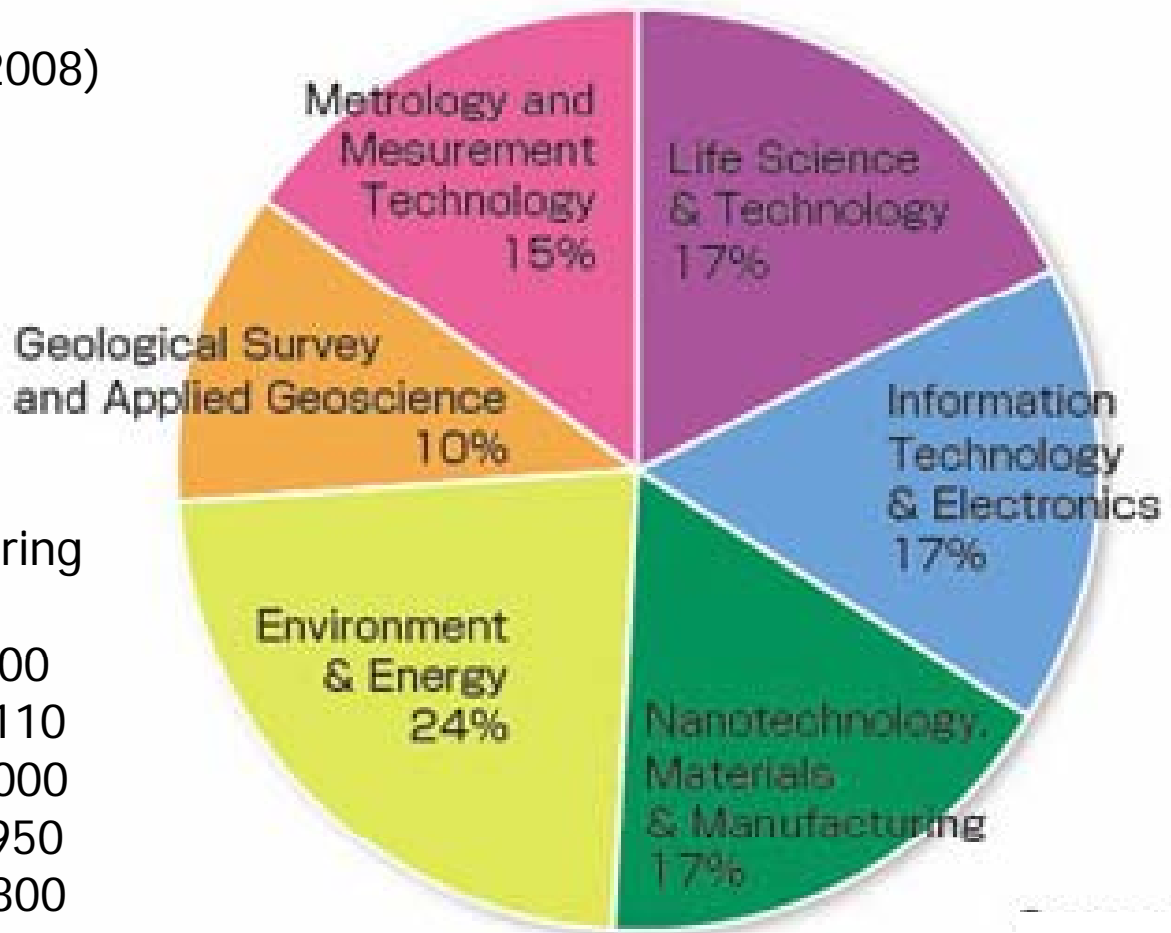
Research Field and Composition of Research Staff

of Employees (as of April 2008)

- Researchers 2,408
 - Tenured [2,031]
 - Fixed-term [377]
- Administrative staffs 695
- Total 3,103

of Visiting Researchers (during FY 2007)

- Postdoctoral researchers 500
- From private companies 1,110
- From universities 2,000
- From corporation etc 950
- From overseas 800



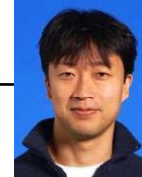
What's RCIS

- ❑ **Research Center for Information Security**
- ❑ One of the research centers/units in AIST
- ❑ Founded in April 2005 (7 year project)
- ❑ Location: Akihabara, Tokyo
- ❑ Members: **Biggest Information Security Research Group in JAPAN**
 - ❑ Research-related Personnel 52 (full-time: 25)
 - ❑ Admin Staff 6

Organization of RCIS



Director: Hideki Imai (Chuo Univ.)



**Principal Research Scientist:
Kazukuni Kobara**



**Deputy Director:
Akinori Yonezawa
(Univ. of Tokyo)
Hajime Watanabe**



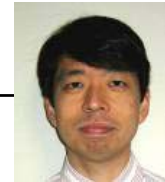
**Res Team for
Security Fundamentals
Leader: Akira Otsuka**



**Advisor:
Tsutomu Matsumoto
(Yokohama NU.)
Takeshi Nanya (Univ. of Tokyo)**



**Res Team for Physical Analysis
Leader: Kentaro Imafuku**



**Res Team for Hardware Security
Leader: Akashi Satoh**



**Res Team for Software Security
Leader: Etsuya Shibayama**

Full-time researchers	25
Part-time researchers	4
Invited Senior Research Scientists	5
Postdoctoral Fellows	6
Technical Staffs	6
Visiting Researchers	5
Internships	1

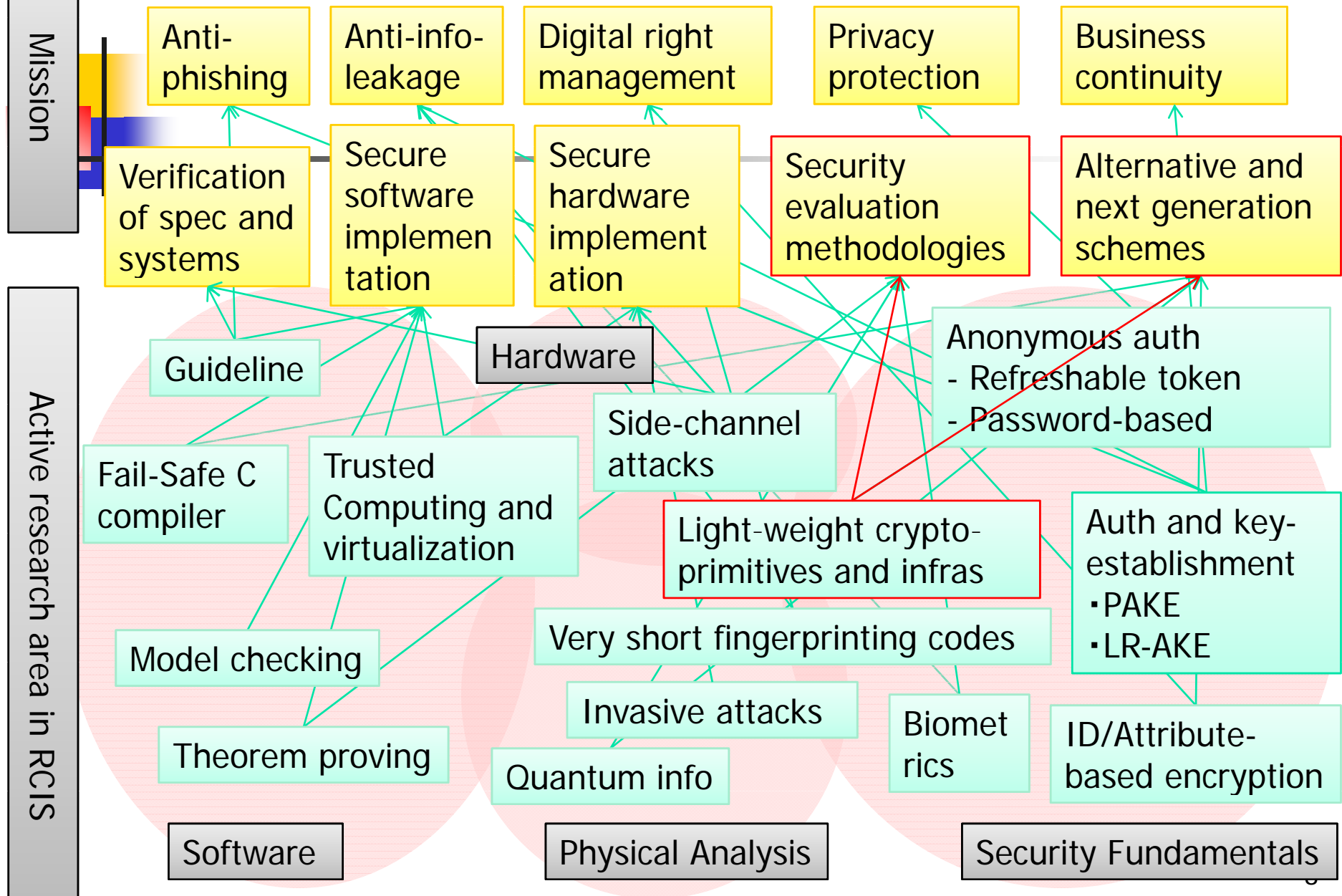
52 researchers, 6 administrative staffs, 58 in total

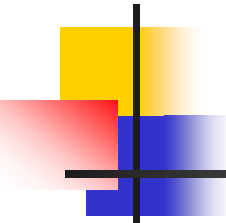
Research Fields of Each Team



- **Security Fundamentals (RTSF)**
 - Cryptographic primitives and protocols
 - Biometrics
- **Physical Analysis (RTPA)**
 - Cryptosystems based on physical assumption, such as quantum mechanics, radio waves and TRMs
- **Hardware Security (RTHW)**
 - Side channel attacks and fault-base analysis
 - Side-channel Attack Standard Evaluation Board (SASEBO)
- **Software Security (RTSS)**
 - Secure programming and compilers
 - WEB security
 - Formal verification

Contribution to make the IT society more secure and usable

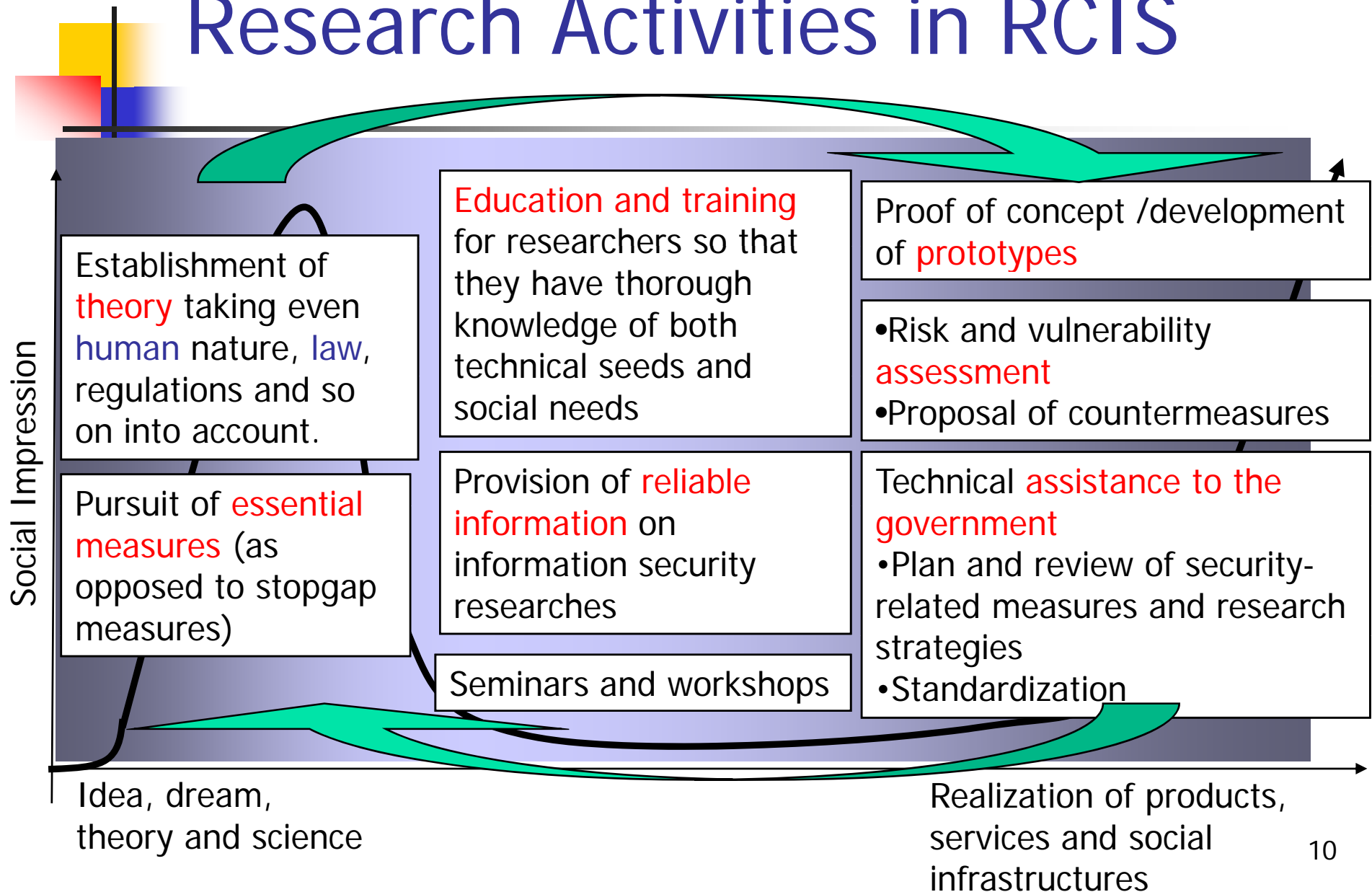




Light-weight crypto-primitives and infrastructures

- Security evaluation of a number of approaches related to **coding theory**
- **Low-complexity** stream ciphers and authentication protocols for RFID, SN and PAN
- **Privacy protection** in RFID, SN and PAN employing low-complexity cryptographic primitives

Research Activities in RCIS



Cooperation with International Organizations



Ratio of Nationality (as of Oct. 2008)

