Division of Electrical Engineering and Computer Science	Research field	Information Security	Lab. ID EC28
Laboratory web site	http://iseclab.ec.t.kanazawa-u.ac.jp/en/index.html		

Research subjects

Information security has increased its importance as the fundamental technology of information society. A key technology of information security is crytography and it includes encryption for secrecy, digital signature for guaranteeing the content of message and its author, and authentication for guaranteeing the legitimacy of user accessing system. Secure information society can be built by constructing secure authentication and cryptographic protocols such as electronic commerce, electronic election, electronic auction etc. in the network.
a) Fundamental cryptographic techniques: Encryption, digital signature, user authentication, pseudorandom number etc.
b) Secure protocol/cryptographic protocol: Cryptocurrency, blockchain technology, electronic payment, electronic auction, application of game theory to cryptography etc.
c) Other protection or authentication techniques: Privacy protection, digital contents protection, software protection, behavior authentication, etc.
d) Security in new fields: Security for IoT and Edgecomputing, Quantum computing and Post-quantum cryptography

Master/Doctor course: Education policy, curriculum, typical activity in the laboratory

Students acquire knowledge and techniques from book reading and seminar for explaining academic papers or reporting research status.
Each student is supervised by professor(s) of the lab and conducts his/her own thesis.
Research results are presented in the major domestic security meetings or symposiums and international conferences. Then based on the comments obtained after the presentation, papers are revised and published in a journal .

Daily life in the laboratory, etc.

At least one PC is available for each student.
Our laboratory often joins softball tournament organized during summer together with members of other laboratory.
Juice and nacks are prepared for taking a rest in the laboratory

Message or comments by the laboratory faculty staffs

Information security needs not only the knowledge and techniques of cryptography, IT security and other research field, e.g. computer science, computer engineering, information and communication engineering, but also management, law and society system, moral and psychology and so on. It is recommended to seek a solution from a wide viewpoint.
We have an experience to welcome students from other domestic universities and also foreign students.
A Ph.D course student has experienced internship in security section of major company as a part of training program for innovative talents. After finishing the bachelar or master degree courses, graduates have been working in companies for communication or software. Also some graduate works in university.

Recent Master theses in these 3 years (+ more if appropriate)

year.month	Thesis title (including English translation of Japanese thesis title)
2017.3	A Study on Constructions of Rational Proofs and Consensus Protocols
2017.3	Construction and Evaluation of Systems Enhancing Privacy and Usability
2017.3	A Study on the Authentication Using Wireless LAN Information
2017.3	Implementation and Evaluation of Cryptographic Library for ARM Cortex-M0 Microcontrollers
2016.3	Construction and Implementation of a Simple and Secure Web Single Sign-On Scheme
2016.3	A Study on Cryptographic Technologies with Usability and Incentives
2015.3	An Improvement of Resistance to Shoulder Surfing on Pattern Lock
2015.3	A method to prohibit the identity theft which abuses stolen cookies
2015.3	A Study of Constructing Fully Homomorphic Encryption
2015.3	A Study on the Method Distinguishing Users by Location Information

Recent Doctoral theses in these 3 years (+ more if appropriate)

year.month	Thesis title (including English translation of Japanese thesis title)
2016.9	A Study on the Secure Online Examination System

Laboratory mail address: Masahiro Mambo <mambo *at* ec.t. ****> ****: kanazawa-u.ac.jp