

Division of Electrical, Information and Communication Engineering	Research field	Information Security	Lab. ID EI19
Laboratory web site	http://iseclab.ec.t.kanazawa-u.ac.jp/en/index.html		
Research subjects			
<p>Information security has increased its importance as the fundamental technology of information society. A key technology of information security is cryptography 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.</p> <p>a) Fundamental cryptographic techniques: Encryption, digital signature, user authentication, pseudorandom number etc.</p> <p>b) Secure protocol/cryptographic protocol: Cryptocurrency, blockchain technology, smart contract privacy, electronic payment, electronic auction etc.</p> <p>c) Other protection or authentication techniques: Privacy protection, digital contents protection, software protection, behavior authentication, etc.</p> <p>d) Security in new fields: Security for IoT and Edgecomputing, AI security and privacy, Quantum computing and Post-quantum cryptography.</p>			
Master/Doctor course: Education policy, curriculum, typical activity in the laboratory			
<p>Students acquire knowledge and techniques from book reading and seminar for explaining academic papers or reporting research status.</p> <p>Each student is supervised by professor(s) of the lab and conducts his/her own thesis.</p> <p>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 .</p>			
Daily life in the laboratory, etc.			
<p>At least one PC is available for each student.</p> <p>Our laboratory has joined softball tournament of the Division and also enjoyed various sports like futsal, table tennis, jogging, cycling and so on.</p> <p>Juice and nacks are prepared for taking a rest in the laboratory</p>			
Message or comments by the laboratory faculty staffs			
<p>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.</p> <p>We have an experience to welcome students from other domestic universities and also foreign students.</p> <p>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 bachelor or master degree courses, graduates have been working in companies for communication or software. Also some graduate works in university.</p>			
Laboratory mail address	Masahiro Mambo <mambo *at* ec.t. ****> ****: kanazawa-u.ac.jp		