Division of Electrical Engineering and	Research	Information Security	Lab. ID
Laboratory web site	http://isecla	ah ec t kanazawa-u ac in /en /index html	E020
Research subjects	<u>11(1).//130018</u>		
Information security has increased its technology of information security is o guaranteeing the content of message	importance crytography a and its autho	as the fundamental technology of information socie and it includes encryption for secrecy, digital signat or, and authentication for guaranteeing the legitimac	ty. A key ure for sy of user
accessing system. Secure information cryptographic protocols such as elect a) Fundamental cryptographic techniq number etc.	society can ronic comme ues: Encrypt	be built by constructing secure authentication and erce, electronic election, electronic auction etc. in the ion, digital signature, user authentication, pseudorar	ne network. 1dom
b) Secure protocol/cryptographic prot electronic payment, electronic auction	tocol: Crypto 1 etc.	currency, blockchain technology, smart contract pr	ivacy,
protection, behavior authentication d) Security in new fields: Security for	techniques: 1 C. IoT and Edge	ecomputing AI security and privacy Quantum com	ware
Post-quantum cryptography.			
Master/Doctor course: Education poli	cv curricului	m typical activity in the laboratory	
Students acquire knowledge and tech	niques from I	pook reading and seminar for explaining academic p	apers or
reporting research status.			
Each student is supervised by profess Research results are presented in the conferences. Then based on the comr iournal	or(s) of the major dome nents obtain	lab and conducts his/her own thesis. stic security meetings or symposiums and internation ed after the presentation, papers are revised and po	onal ublished in a
Daily life in the laboratory, etc.			
At least one PC is available for each s	student.		
Our laboratory has joined softball tour	nament of th	ne Division and also enjoyed various sports like futs	al, table
tennis, jogging, cycling and so on.			
Juice and nacks are prepared for takin	ng a rest in t	he laboratory	
Message or comments by the laborate	orv faculty st	affs	
Information security needs not only the	e knowledge	and techniques of cryptography. IT security and ot	her
research field, e.g. computer science,	computer en	gineering, information and communication engineeri	ng, but also
management, law and society system, a wide viewpoint.	moral and p	sychology and so on. It is recommended to seek a s	olution from
We have an experience to welcome st A Ph D course student has experience	udents from ed internship	other domestic universities and also foreign studen	its. Training
program for innovative talents. After f	inishing the b	pachelar or master degree courses, graduates have	been
working in companies for communicati	on or softwa	re. Also some graduate works in university.	
Recent Master theses in these 3 year	s (+ more if a	appropriate)	
year.month Thesis title (including Eng	glish translati	on of Japanese thesis title)	
2021.3 How to Make Machine Le	arning Resis	tant against Adversarial Examples	
2021.3 On Verifiable Functions a	nd their App	lications	
2021.3 A Study on White-Box C	ryptography		
2021.3 A Study on the Redactab	le Blockchai	n	
2021.3 On the Privacy Risk of W	eb Access H	listory	
2020.3 A Study on the Techniqu	es for IoT Sy	/stem Security	
2020.3 Analysis of Data Backup	Methods Co	ntributing to Cybersecurity	
2020.3 Location-Related Privacy	/ Risk Analys	is of Web Access History	
2019.3 Security and Privacy Tec	hnieuqs in C	loud-Edge Computing Environments	
2019.3 A Study on the Incentive	Design for F	airness in Blockchains	
2019.3 A Study on the Approxim	ation of Pro	Dability Distributions in Cryptographic Primitives	
2019.3 A Study on the Implement	itation of Cry	ptographic Primitives for IoI	
2019.3 On the Privacy Risk Eval	Detection M	sonal Data ethod against Adversarial Examples	
		against Auversariai Examples	

- ---

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
2015.3 Recent Doc [.]	A Study on the Method Distinguishing Users by Location Information coral theses in these 3 years (+ more if appropriate)
2015.3 Recent Doc [.] year.month	A Study on the Method Distinguishing Users by Location Information coral theses in these 3 years (+ more if appropriate) Thesis title (including English translation of Japanese thesis title)
2015.3 Recent Doc year.month 2021.9	A Study on the Method Distinguishing Users by Location Information coral theses in these 3 years (+ more if appropriate) Thesis title (including English translation of Japanese thesis title) Design and Implementation of the Efficient and Secure Content Distribution Scheme in Named Data Networking
2015.3 Recent Doc year.month 2021.9 2020.9	A Study on the Method Distinguishing Users by Location Information coral theses in these 3 years (+ more if appropriate) Thesis title (including English translation of Japanese thesis title) Design and Implementation of the Efficient and Secure Content Distribution Scheme in Named Data Networking A Study on the Preservation of Name Privacy in Named Data Networking
2015.3 Recent Doc year.month 2021.9 2020.9 2019.9	A Study on the Method Distinguishing Users by Location Information coral theses in these 3 years (+ more if appropriate) Thesis title (including English translation of Japanese thesis title) Design and Implementation of the Efficient and Secure Content Distribution Scheme in Named Data Networking A Study on the Preservation of Name Privacy in Named Data Networking A Study on the Personal Privacy Preservation in Set-Valued Database Publishing
2015.3 Recent Doc year.month 2021.9 2020.9 2019.9 2019.9	A Study on the Method Distinguishing Users by Location Information coral theses in these 3 years (+ more if appropriate) Thesis title (including English translation of Japanese thesis title) Design and Implementation of the Efficient and Secure Content Distribution Scheme in Named Data Networking A Study on the Preservation of Name Privacy in Named Data Networking A Study on the Personal Privacy Preservation in Set-Valued Database Publishing Trust Establishment for Fog Computing Service in Vehicular Network
2015.3 Recent Doc year.month 2021.9 2020.9 2019.9 2019.9 2016.9	A Study on the Method Distinguishing Users by Location Information coral theses in these 3 years (+ more if appropriate) Thesis title (including English translation of Japanese thesis title) Design and Implementation of the Efficient and Secure Content Distribution Scheme in Named Data Networking A Study on the Preservation of Name Privacy in Named Data Networking A Study on the Personal Privacy Preservation in Set-Valued Database Publishing Trust Establishment for Fog Computing Service in Vehicular Network A Study on the Secure Online Examination System