

KOREA UNIVERSITY SCHOOL OF CYBER SECURITY

KOREA
UNIVERSITY
SCHOOL OF
CYBERSECURITY



CONTENTS

KOREA UNIVERSITY SCHOOL OF CYBERSECURITY

School of Cybersecurity

02 Introduction

04 Greetings from the Dean

06 Organization

08 History

09 Awards

10 Professors

Full-time Professors

Invited Professors

Specially Appointed Professors

16 Degree Programs

Undergraduate Programs

a. Div. of Smart Security

b. Dept. of Cyber Defense

Graduate Programs

School of Cybersecurity

a. Dept. of Information Security

b. Dept. of Financial Security

c. Dept. of Cyber Security

d. Dept. of Digital Forensics

e. Dept. of Convergence Security

Korea University Graduate School

a. Dept. of Cyber Security

18 Laboratories

a. Privacy Enhancing Technologies Lab.

b. Financial Security Policy Lab.

c. Network and Security Research Lab.

d. Digital Forensic Research Lab.

e. Wireless Network Lab.

f. Security Assessment aNd Engineering Lab.

g. Cyber Law & Policy Lab.

h. Signal Processing and Advanced Intelligence Lab.

i. Cryptographic Algorithm Lab.

j. Cryptographic Protocol Lab.

k. Risk Management Lab.

l. Artificial Intelligence Lab.

m. Embedded Security Lab.

n. Formal Methods Lab.

o. Computer Systems Security Lab.

p. Hardware Security Lab.

q. Hacking and Countermeasure Research Lab.

Institute of Cybersecurity & Privacy

24 Introduction

26 Organization

28 History

30 Research Centers

a. Army RMF Research Center

b. Global Intelligence Center

c. Digital Forensics Research Center

d. Blockchain Security Research Center

e. Center for Cyber Resilience Research

f. Center for Cyber Security Policy

g. Cryptology Research Center

h. Research Coordination Headquarters

i. Cyber Warfare Technology Research Center

j. KU-Samsung SDS Joint Security Research Center

Introduction

As Korea's leading institution in research and education in information security, the School of Cybersecurity provides a range of undergraduate and graduate education and training courses to cultivate world-leading experts. Our graduates dedicate themselves to maintaining the safety of our information society and safeguarding the nation and organizations against cyber threats.

International Center for Converging Technology Building

**Founded in 2000
as the world's first
information
security school**

SCHOOL OF CYBERSECURITY

Greetings from the Dean

Founded as the world's first graduate school on information security in 2000, the School of Cybersecurity (SCS) has continued to push its boundaries to position itself as the cradle of cybersecurity experts in Korea over the past 20 years. Today, under the guidance of 17 full-time professors devoted to the discipline of cybersecurity, it produces about 100 master and doctorate recipients annually. As of 2020, it has cultivated over 1,500 master and doctorate holders specialized in information security, thereby contributing to Korea's advancement in cybersecurity.

In the face of emerging cyber threats, the SCS has strived to develop technologies and nurture a workforce with skills and abilities matched to society's needs. At its inception, cryptography was of the utmost priority in its research. Since then, however, the SCS has continued to scale up its scope and reach of education and research into all fields of cybersecurity, including digital forensics, privacy policy, cyber law, embedded security, financial security, security engineering, system security, blockchain, and artificial intelligence security. Coupled with these endeavors, various departments under the graduate program have been introduced to lead the nation's research and education on information security.

With the aim of building a cybersecurity community serving the world, the SCS has set out to produce communications experts that possess both outstanding technical skills and a strong sense of responsibility. It is devoted to studying creative ways to solve social problems such as privacy protection while paving the ground for academic-industry-research partnership. To this end, it is working on building an online education system, holding an international cybersecurity challenge competition, and developing and distributing cybersecurity ethics-related programs and open-source materials.

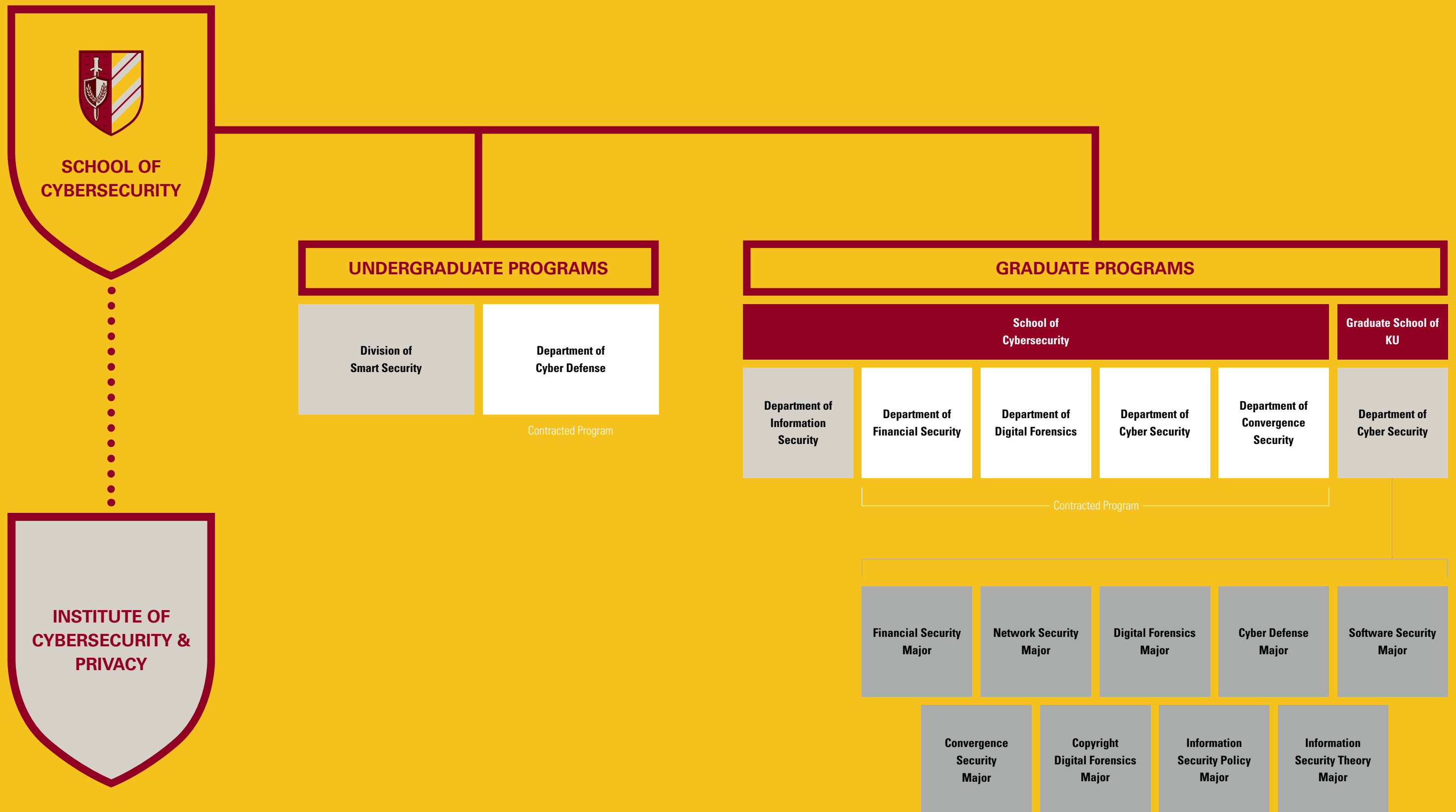
The SCS will not sit on its laurels, but rather continue to innovate to respond to the rapidly changing smart technology environment and ever-evolving cyber threats. It has already begun to challenge the status quo. Selected by the Ministry of Education in 2020 as a research and education group on smart city security for the Brain Korea (BK) 21 FOUR, the SCS is currently preparing to emerge as an educational institution specialized in smart security for smart cities, which are being heralded as the future of cities supported by cutting-edge smart technologies. Going forward, the SCS will continue its innovation and transformation journey at the forefront of the cybersecurity field, thereby growing into a world-renowned cybersecurity education and research institution beyond Korea and Asia.

Thank you.



Professor **Lee Sang-jin**
Dean of the School of Cybersecurity

Organization



History

2000. 03.	Established the Information Security Technology Collaboration Program (master's/doctoral program in the Graduate School)
2000. 09.	Gained approval of the Graduate School of Information Security as a professional graduate school
2001. 03.	Founded the Graduate School of Information Security (45 in master's/doctoral program)
2001. 03.	Inaugurated Lim Jong-in as First Dean
2001. 08.	Increased admission quota for the general graduate program (to 75 in master's/doctoral program)
2006. 05.	Selected for 2nd Phase BK21 Project Group (Ubiquitous information Security Agency)
2006. 09.	Integrated with the Dept. of Industrial Systems & Information Engineering of the Graduate School, renamed the Graduate School of Information Management and Security, and adjusted the admission quota (115 in total: 83 in master's, 32 in doctoral program)
2007. 03.	Recruited students together for the Graduate School of Information Management and Security (91 in master's/doctoral program, incl. extra quota)
2009. 03.	Established the Dept. of Financial Security (Employment contract program, Ministry of Knowledge Economy; 15 in master's program)
2009. 12.	Selected as 2nd Phase BK21 3rd-Year Best Project Group (for 3 years in a row from 2007)
2010. 03.	Established the Dept. of Information Security (51 for master's, 22 for doctoral program) Changed the affiliation of industrial system and management engineering majors of Dept. of Information & Industrial Engineering into Graduate School (quota reduction by 30 in master's and 10 in doctoral program)
2010. 03.	Established the Dept. of Cyber Security (Retraining program, Ministry of Knowledge Economy Cyber Safety Center/KEPCO KDN; 25 in master's program)
2010. 09.	Selected for 2nd Phase BK21 4th-Year Best Project Group (Convergence 2 Panel)
2011. 03.	Renamed to the School of Cybersecurity and changed admission quota (45 in master's, 23 in doctoral program)
2011. 09.	Established the Dept. of Public Security Policy (Retraining program, Ministry of Knowledge Economy; 30 in master's program)
2012. 03.	Established the Dept. of Cyber Defense, Division of Information Security (30 in bachelor's program)
2012. 03.	Changed admission quota of Dept. of Information Security (40 in master's, 28 in doctoral program)
2012. 09.	Established the Dept. of Digital Forensics (Retraining program, National Police Agency) (25 in master's program)
2013. 03.	Established the Dept. of KB Financial Security (Retraining program, KB Kookmin Bank, 25 in master's program)
2013. 09.	Established the Dept. of Cyber Defense, Graduate School (Master's/Doctoral program)
2013. 09.	Changed admission quota of the Dept. of Information Security, School of Cybersecurity (53 in master's, 31 doctoral program)
2013. 09.	Selected for BK21 PLUS Project Group (IT Convergence Security Agency)
2014. 03.	Established the Samsung Information Security Major, Dept. of Information Security (employment contract program, Samsung SDS, 10 in master's program)
2014. 03.	Established the Financial Security Policy Major, Dept. of Financial Security (retraining program, 25 in master's program)
2014. 03.	Changed admission quota of Dept. of Information Security (57 in master's, 29 in doctoral program)
2014. 09.	Established the Dept. of Cyber Security (retraining program, ROK Cyber Command; 30 in master's, 10 in doctoral program)
2015. 03.	Established the Dept. of Big Data Application and Security (retraining program, 20 in master's program)
2018. 03.	Established the Dept. of Convergence Security (retraining program, 20 in master's, 10 in doctoral program)
2018. 09.	Established the Dept. of Blockchain (retraining program, 30 in master's, 10 in doctoral program)
2020. 03.	Renamed the Dept. of Cyber Defense, Graduate School into Dept. of Cyber Security
2020. 04.	Received approval for the Division of Smart Security by the Ministry of Education (30 in bachelor's program)
2020. 10.	Selected for the BK21 FOUR Research Group (Smart City Security Education & Research)
2021. 03.	Received 30 new entrants in the Division of Smart Security

Awards

2009. 12.	Digital Forensic Research Center (DFRC) won Grand Champion at the Digital Forensics Challenge (DFRC)
2010. 12.	Won Grand Champion at DC3's Digital Forensics Challenge (DFRC)
2013. 08.	Won the DFRWS Forensics Challenge, an international academic conference
2015. 05.	Won the Bronze Prize at the world's largest ACM-ICPC (Association for Computing Machinery-International Collegiate Programming Contest)
2015. 08.	Won DEFCON CTF 2015, one of the world's largest hacking contests
2015. 11.	Won Trend Micro CTF 2015 (Japan) international attack & defense contest
2015. 12.	Won HITCON CTF 2015 (Taiwan) international attack & defense contest
2016. 01.	Won SECCON CTF 2015 (Japan) international attack & defense contest
2016. 01.	Won Holyshield 2016
2016. 05.	Won 1st Place at CODEGATE international collegiate hackathon conference
2016. 06.	Won XCTF 2016
2016. 08.	Won DEFCON 2016
2016. 10.	Won at the University Division in the Crypto Analysis Contest
2016. 10.	Won HDCON 2016
2016. 11.	Won Grand Prize both at General Division and Technology Competition in 2016 Korea Whitehat Contest
2016. 12.	Won HITCON CTF 2016 (Taiwan) 2 times in a row
2017. 01.	Won SECCON (Japan) international attack & defense contest
2017. 04.	Ranked runner-up at General Division of CODEGATE 2018
2017. 07.	Ranked runner-up in CODE BLUE 2017
2017. 07.	Came in fourth in DEFCON
2017. 10.	Won KASPERSKY Industrial CTF (China) international attack & defense contest
2017. 11.	Ranked 1st in the Attack Team Division in Cyber Conflict Exercise 2017
2017. 11.	Won the National Security Research Institute (NSR) CCE
2017. 12.	Won HITCON CTF 2017 (Taiwan) international attack & defense contest 3 times in a row
2017. 12.	Won the White Hacker League 2017
2018. 02.	Won SECCON (Japan) international attack & defense contest
2018. 04.	Won the General Division of Codegate 2018
2018. 08.	Won DEFCON CTF 2018, the world's largest hacking contest
2018. 08.	CYKOR, Cyber Defense Dept. club, won Samsung Capture The Flag SCTF.
2018. 10.	Won 1st Prize at the 17th Hwarangdae Collegiate Forum on National Security
2018. 11.	Won POC2018 Belluminar hacking competition
2019. 03.	Won at the General Division in CODEGATE 2019
2019. 09.	Ranked 3rd place at the General Division in 2019 Cyber Operations Contest
2019. 10.	Won 2019 CODE BLUE CTF
2019. 11.	Received a prize in the 2019 BTS (Beyond Technology, STEAM education) Hackathon
2019. 11.	Won 1st Prize in 2019 Open SW Mini-Hackathon
2019. 11.	Won the POC2019 Belluminar hacking competition
2020. 09.	Won at the College Student Division in CODEGATE 2020
2021. 10.	Won 1st Prize at the 20th Hwarangdae Collegiate Forum on National Security

Professors

Full-time Professors



Jong In Lim

Career

2001-Present	Professor of School of Cybersecurity, Korea University
2015	Special Advisor to the President for National Security
2010	Chairman, Korea Institute of Information Security and Cryptology
2001-2014	Dean of School of Cybersecurity, Korea University
1986-Present	Professor, Korea University
1986	Ph.D., Department of Mathematics, Korea University

Research Area

National Cyber Security, Cyber Defense, Privacy, Digital Forensics Policy, Convergence Security Policy



Dong Hoon Lee

Career

2001-Present	Professor of School of Cybersecurity, Korea University
2018	President of Korea Institute of Information Security & Cryptology
2015-2017	Dean of School of Cybersecurity, Korea University
1993-Present	Professor, Korea University
1992	Ph.D., Computer Engineering, University of Oklahoma

Research Area

Automotive Vehicle Security, Sensor Network Security, Efficient and Applicable Digital Signature and Encryption Scheme, Proof Technique of Cryptographic Protocols, Key Management



Jin Young Choi

Career

2015-Present	Professor of School of Cybersecurity, Korea University
2013-Present	Director, Secure Software Research Center
1996-Present	Professor, Korea University
1993	Ph.D., Computer and Information Science, University of Pennsylvania

Research Area

Secure Software Engineering, Formal Methods



Sangjin Lee

Career

2001-Present	Professor of School of Cybersecurity, Korea University
2017-Present	Dean of School of Cybersecurity, Korea University
2013-2017	President, Digital Forensics Society of Korea
1999-Present	Professor, Korea University
1989-1999	Senior Researcher, Electronics and Telecommunications Research Institute (ETRI)
1994	Ph.D., Mathematics, Korea University

Research Area

Digital Forensics Techniques and Procedure, Incident Analysis, Development of Digital Forensics Tools, Reverse Engineering of Embedded Devices, Steganography



Wonjun Lee

Career

2015-Present	Professor of School of Cybersecurity, Korea University
2010-Present	Director, Future Network Center(FNC), Korea University
2008-2013	Director, WCU Future Network Optimization Technology Center, Korea University
2002-Present	Professor, Korea University
1999	Ph.D., Computer Science and Engineering, University of Minnesota, Minneapolis, USA

Research Area

Wireless & Mobile Networking Protocol, RF-Powered Networking, Security & Privacy in Wireless Communications, Machine Learning for Networking



Seokhie Hong

Career

2021-Present	Vice Dean of School of Cybersecurity, Korea University
2005-Present	Professor of School of Cyber Security, Korea University
2001	Ph.D, Mathematics, Korea University

Research Area

Research and Design of Public-Key Cryptosystems on Side channel attacks(Power Analysis, Fault Injection Analysis), Design and Analysis of Efficient Cryptosystems(Software and Hardware), Design and Cryptanalysis of Block Cipher, Security Analysis of Stream Cipher, Design and Cryptanalysis of Hash Function, Post Quantum Cryptography



Seong-Jun Oh

Career

2015-Present	Professor of School of Cybersecurity, Korea University
2007-Present	Professor, Korea University
2003-2007	Staff Engineer, Qualcomm CDMA Technologies, San Diego CA USA
2000-2003	Senior Engineer, Ericsson Wireless Communications, San Diego CA USA
2000	Ph.D., EECS(Systems), University of Michigan, Ann Arbor

Research Area

Wireless Communication System Design and Performance Evaluation, Machine Learning and Artificial Intelligence



Ik Rae Jeong

Career

2008-Present	Professor of School of Cybersecurity, Korea University
2006-2008	Researcher, Electronics and Telecommunications Research Institute (ETRI)
2004	Ph.D., Information Security, Korea University

Research Area

Cryptographic protocol, Biometric security, Blockchain security



Huy Kang Kim

Career

2010-Present	Professor of School of Cybersecurity, Korea University
2004-2010	Head of Information Security Department/Technical Director of NCSOFT
2009	Ph.D., Industrial and System Engineering, KAIST
2007	AI Spera, Co-founder
1999	Founder, A3 Security Consulting

Research Area

Automobile Security, Online Game Security, Fraud Detection System,
Cyber Threat Intelligence, Data-Driven Security



Seungjoo Kim

Career

2011-Present	Professor of School of Cybersecurity, Korea University
2018-2020	Member of Presidential Committee on the 4th Industrial Revolution
2018-2019	Visiting Professor of Korea Military Academy
2004-2011	Associate Professor of Sungkyunkwan University
1998-2004	Director, KISA(Korea Internet & Security Agency)
1999	Ph.D., Information Eng., Sungkyunkwan University

Research Area

Security/Privacy by Design, Security Engineering, Security Requirements Engineering,
Secure Architecture Design, Secure Code Development,
Automated Risk-Based Security Testing and Verification, Security Evaluation and Assertion,
Secure Update, Supply Chain Security, Blockchain & Crypto Engineering



Kyungho Lee

Career

2011-Present	Professor of School of Cybersecurity, Korea University
2020-Present	Vice Chairman of Korea Institute of Information Security & Cryptology
2017-2019	Head of Korea University Data Hub
2009	Ph.D. in Information Security Engineering, Korea University
2007-2008	NAVER CISO, CPO

Research Area

Risk Management, Information Security Consulting, ISMS, Security & Privacy Policy,
Information protection and privacy policies, Information asset valuation,
Information security risk management, PIA, BIA, Information protection and privacy policies,
Data analysis and dysfunction detection, Cyber Warfare C&C, Cyber Warfare Threat Assessment



Ji Won Yoon

Career

2012-Present	Associate Professor of School of Cybersecurity, Korea University
2011-2012	Research Scientist, IBM Research Lab, Ireland
2009-2011	Research Fellow, Statistics Department, Trinity College Dublin
2008-2009	PostDoc, Pattern Analysis and Machine Learning lab, Robotics Group, University of Oxford, UK
2005-2008	Ph.D., Statistical Signal Processing, University of Cambridge, UK

Research Area

Covert channel design and detection, Multiple Drone Tracking,
Audio and Image Signals Analysis, Side Channel Analysis for Cryptanalysis,
Statistical Signal Processing, Bayesian Monte Carlo, Fundamental of Machine Learning



Hun-Yeong Kwon

Career

2015-Present	Professor of School of Cybersecurity, Korea University
2008-2015	Professor in Law at Kwangwoon Univ. Seoul, Korea
2019	President, the Cybercommunication Academic Societ
2017-2018	President, the Korea Society of Internet Ethics
2005	Ph.D., Law, Yonsei University, Seoul, Korea

Research Area

Information Security Law, Information and Communications Law and Policy,
Internet Law, Privacy Law, Cyber Security Policy



Junghee Lee

Career

2019-Present	Associate Professor of School of Cybersecurity, Korea University
2014-2019	Assistant Professor, University of Texas at San Antonio
2003-2008	Engineer, Samsung Electronics
2013	Ph.D., Georgia Institute of Technology

Research Area

Security of Hardware, Storage, Memory and Internet-of-Things



Sangkyun Lee

Career

2020-Present	Assistant Professor of School of Cybersecurity, Korea University
2017-2019	Assistant Professor, Computer Science, Hanyang University ERICA
2011-2016	Project Leader, Collaborative Research Center SFB 876, TU Dortmund University, Germany
2011	Ph.D. Computer Sciences, University of Wisconsin-Madison, USA

Research Area

AI Attack & Defense, Bigdata Machine Learning Algorithm,
Model Discovery and Compression in High-Dimensional Model Spaces



Youngjoo Shin

Career

2020-Present	Assistant Professor of School of Cybersecurity, Korea University
2017-2020	Assistant Professor of School of Computer and Information Engineering, Kwangwoon University, Seoul, Korea
2008-2017	Senior Researcher, National Security Research Institute (NSR), Daejeon, Korea
2014	Ph.D, Computer Science, KAIST, Daejeon, Korea

Research Area

System Security on OS and Hypervisor-based Virtualization, CPU Microarchitectural Attacks and Mitigation,
Security Analysis of Carrier-grade Network Devices, Network Security, Cloud Computing Security



Jungheum Park

Career

2021-Present	Assistant Professor of School of Cybersecurity, Korea University
2015-2019	Guest Researcher, National Institute of Standards and Technology, US
2014	Ph.D., Information Security, Korea University

Research Area

Digital Forensics, Cybercrime Response, Cybersecurity Incident Response

Invited
Professors

Chan Ok Kang

Career

2013-Present	Invited Professor of School of Cybersecurity, Korea University
2020	Ph.D., Political Science and Economics, International Political Science, Korea University
2009-2011	Reserve Officer's Training Corps Commander, Korea University
2008	Commander of UN Interim Peacekeeping Force in Lebanon
2007	C-3 Chief, ROK-US Combined Special Forces Command in Korea

Research Area

International Politics, Security, Military Strategy, Operational Arts



Seokjung Hwang

Career

2017-Present	Invited Professor of School of Cybersecurity, Korea University
2011	Defense Security Commander, Ministry of National Defense (Brigadier General)
2000	M.S. C4I, Graduate School of Information Communication, Ajou University

Research Area

Theory of National Intelligence, History of War, Weapon Systems Theory

Specially
Appointed
Professors

Hyoung Joong Kim

Career

2020-Present	Specially Appointed Professor of School of Cybersecurity, Korea University
2006-2020	Professor of School of Cybersecurity, Korea University
2002-Present	Co-Founder and Technical Program Chair for International Workshop on Digital-Forensics and Watermarking
1989	Ph.D., Control and Instrumentation Engineering, Seoul National University

Research Area

Image Forensics, Biometrics Authentication, Big Data Analysis, Data Hiding, Information Theory, Steganography, Signal Processing



In Seok Kim

Career

2011-Present	Specially Appointed Professor of School of Cybersecurity, Korea University
2014-2020	Professor (non-tenured) of School of Cybersecurity, Korea University
1999-2011	Former Vice Director, IT at Financial Supervisory Service
2008	Ph.D., Information Security, Korea University

Research Area

Electronic Financial Security, Electronic Financial Law, Electric Financial AUDIT



Hee Han

Career

2018-Present	Specially Appointed Professor of School of Cybersecurity, Korea University
2018-2020	Professor (non-tenured) of School of Cybersecurity, Korea University
2009-2018	Professor, Seoul Media Institute of Technology (SMIT), Seoul, Korea
2006	Head, T2TRC Motorola Lab
2000-2005	Brigade Commander, Defense Intelligence Command
1990-1999	Senior Researcher, Korea Institute of Defense Analysis
1989	Ph.D., EE, Yonsei University, Seoul, Korea

Research Area

Signal Processing/Speech Recognition, Creativity/Innovation, Cyber Security Strategy



JoonSang Yoo

Career

2009-Present	Specially Appointed Professor of School of Cybersecurity, Korea University
2014-Present	Chairman of the board of K-BoB Security Forum
2010-Present	President of Korea Information Technology Research Institute
1981-1996	The 11th, 12th, 13th and 14th Member of the National Assembly

Research Area

Cybersecurity Professional Education, Cybersecurity Leadership Training



Sung-joo Choi

Career

2020-Present	Specially Appointed Professor of School of Cybersecurity, Korea University
2016-2018	Ambassador to Poland
2013-2016	Member of UNSG's Advisory Board on Disarmament Matters
2013	Head of the Preparatory Secretariat for the Seoul Conference on Cyberspace
2013-2015	Ambassador for International Security
2009-2012	Ambassador to Algeria

Research Area

International Cyber Norms, International Cyber Security



Kunwon Yang

Career

2020-Present	Specially Appointed Professor of School of Cybersecurity, Korea University
2016-2019	Director, Cyber Investigation Division, KNPA (Korean National Police Agency)
2010-2016	Assistant Director/Head, Digital Forensics Lab. INTERPOL
	Counsellor, Korean Embassy in Vietnam
1994-2009	Director, Cyber Terror Response Center, KNPA
	Chief, Cyber Crime Investigation Unit, KNPA

Research Area

Digital Evidence Law, Cyber Crime, Digital Forensics

Degree Programs

Undergraduate Programs

a. Division of Smart Security

Newly created in 2021, the Division of Smart Security aims to cultivate talents who will grow into engineers and researchers in the field of security with skills and abilities essential in the smart era. The Division boasts outstanding faculty members from the areas of core technologies needed in a smart society, such as software, cybersecurity, and artificial intelligence. It provides a variety of high-quality educational programs to nurture cybersecurity engineers with basic knowledge and technical skills of software and artificial intelligence required by academia and industry as well as government agencies and large companies in the smart era.

b. Department of Cyber Defense (Contracted program)

The Department of Cyber Defense is an employment contract-type undergraduate program co-founded by Korea University and the Ministry of Defense. It aims to cultivate top cybersecurity officers who can safeguard the nation from cyber terrors and cyber wars. Students are funded full scholarships (tuition fees) for four years provided with grants for additional military service, and after graduation, they work in cyber defense as an officer for seven years. To cultivate the best cyber security officers, the Department offers the best faculty, the best facilities, the best curriculum, and various benefits.

School of Cybersecurity

a. Department of Information Security

The Department of Information Security is devoted to cultivating outstanding information security experts who combine in-depth theoretical knowledge and practical skills and carrying out a wide range of research on information security technologies and policies required by public and private sectors. To live up to the goals, purposefully designed master's and doctoral education programs are offered covering all fields of information security from information security technology and policy, physical security, cybersecurity, convergence security, and cryptography to digital forensics and artificial intelligence security. After graduation, students land in different fields, working for national research institutes such as the Korea Institute of Human Resources Development in Science & Technology (KIRD), the Korea Internet & Security Agency, and the Financial Security Agency, in high-tech IT companies like Samsung and LG, AhnLab, in other firms specialized in cyber security, or in law and accounting firms.

b. Department of Financial Security (Contracted program)

The Department of Financial Security was established in 2009 to provide security solutions to the financial field, which takes utmost priority in the era of the digital economy in order to protect the national economy and everyday lives. It has produced a number of experts specialized in financial security policies and technologies as a whole, who serve as essential workforce to safeguard financial information and electronic financial transactions. It is currently operated as a customized program to retrain and reskill the incumbent workforce in the financial industry, such as financial supervisory institutions and financial firms, into top financial security specialists equipped with theoretical knowledge and practical skills.

c. Department of Cyber Security (Contracted program)

Founded in 2010, the Department of Cyber Security is a program contracted to retrain and reskill the incumbent public officers from the energy sector into chief information security officers with leadership skills to manage a dedicated cyber security organization. It offers targeted intensive training programs on risk management, security control, response to cyberattacks, and smart grid security, which are essential to protect the infrastructure of the energy sector from cyber threats. By striving to move away from a theory-centered toward field-oriented customized program, it aims to cultivate chief information security officers who can contribute to advancing the national level of cyber security and infrastructure protection.

d. Department of Digital Forensics (Contracted program)

As digital evidence has been crucial to criminal investigations, the demand for digital forensics professionals has been increasing. Against the backdrop, the Department of Digital Forensics was founded in 2012 based on an agreement with the National Police Agency on improving the digital forensic expertise of investigative agencies. As a targeted master course, it retrain and reskills police officers from the National Police Agency through criminal law and forensic computer science classes. Setting out an ambition to cultivate skilled digital forensic experts, it provides systematic and specialized education on all fields of the digital forensics covering IT policy and technology.

e. Department of Convergence Security (Contracted program)

In today's convergence environment where companies are evolving into various forms, new cyber security threats are rapidly emerging. Under these circumstances, the Department of Convergence Security has been established as a retraining and reskilling program operated based on agreements with different industries. It is designed to help these industries secure an outstanding workforce who can effectively respond to new and emerging security risks. It provides the incumbent workforce of different companies with the latest knowledge on convergence security combining various security fields such as cyber security, physical security, IT security, and OT security, so that they can grow into world-class experts in convergence security.

Korea University Graduate School

a. Department of Cyber Security

With the arrival of the Fourth Industrial Revolution and in a hyper-connected intelligent information society, cyber security issues are on the rise. Affiliated with the KU Graduate School, the Department of Cyber Security aims to cultivate outstanding global talents with abilities to creatively solve various security problems facing public and private sectors as well as national defense and the international community. The full-time professors from the School of Cybersecurity provide the Department's students with lectures and research supervision in policy, theory, and applied fields. The Department is divided into nine majors: Financial Security, Network Security, Digital Forensics, Cyber Defense, Software Security, Convergence Security, Copyright Digital Forensics, Information Security Policy, and Information Security Theory. Among these, the Copyright Digital Forensics major has been selected as the supervisory organization of the Copyright-Specialized Digital Forensic Workforce Training Project by the Ministry of Culture, Sports and Tourism and the Korea Copyright Protection Agency. It has strived to foster experts for the area since 2020.



Laboratories

SCHOOL OF
CYBERSECURITY

Privacy Enhancing Technologies Lab.	Financial Security Policy Lab.	Network and Security Research Lab.
Digital Forensic Research Lab.	Wireless Network Lab.	Security Assessment aNd Engineering Lab.
Cyber Law & Policy Lab.	Signal Processing and Advanced Intelligence Lab.	Cryptographic Algorithm Lab.
Cryptographic Protocol Lab.	Risk Management Lab.	Artificial intelligence Lab.
Embedded Security Lab.	Formal Methods Lab.	Computer Systems Security Lab.
Hardware Security Lab.	Hacking and Counterneasure Research Lab.	

a. Privacy Enhancing Technologies Lab.
(Prof. Ik Rae Jeong)

Established in 2008 to live up to the increasing demand for privacy protection in a ubiquitous environment, the PET Lab conducts diverse research on privacy related technologies.

Research Area

- Lightweight Authentication and Key Exchange Protocol Analysis
- Database Security
- Biometric Security
- Block Chain Technology and Security

Products and Services Offered

- Order-preserving Encryption

b. Financial Security Policy Lab.
(Prof. In Seok Kim)

The FSP Lab was established to help financial firms better respond to increasing financial security incidents and rigorous regulatory standards. It focuses on providing them with services for security compliance, IT auditing, and vulnerability assessment and developing effective policies and strategies to strengthen financial security.

Research Area

- Financial Security Technique & Development
- Financial Security Law & Policy
- Corporate Audit Methodology
- Electronic Transaction Vulnerability Check
- Fraud Detection System
- Fintech Security

Products and Services Offered

- Consulting Method Regarding Financial IT Auditing
- Evaluation IT Management Status
- Electronic Finance related Legal Advice

c. Network and Security Research Lab.
(Prof. Wonjun Lee)

Founded in 2002, NetLab is devoted to research on various network technologies and network security. It studies protocol design, test bed implementation, standardization, performance analysis and optimization, network security, and user privacy in various wired and wireless network environments.

Research Area

- RF-Powered Computing and Networking for the Internet of Things
- Security and Privacy in Wireless Communications, Mobile Computing and Networked Systems
- Beyond 4G/5G Network Technologies for Mobile Telecommunications
- Optimization Techniques for Mobile Wireless Communication and Networking
- Design, Implementation, and Analysis of Next-Generation Communication Network Protocols

Products and Services Offered

- RF-Powered Networking
- Collision-based Authentication Scheme in Backscatter Networks
- Backscatter-based RF Sensing
- RF-Powered System Prototyping

d. Digital Forensic Research Lab.
(Prof. Sangjin Lee, Prof. Jungheum Park)

Established in 2003 as Korea's first digital forensic laboratory in university, the DFR Lab studies and develops effective techniques and procedures for the collection, preservation, interpretation, analysis, and representation of potential digital evidence in response to cybercrimes and cybersecurity incidents.

Research Area

- Techniques and Procedures for Digital Forensics
- Search and Collection of Potential Digital Evidence
- Multi-source Data Integration and Correlation Analysis
- Development of Digital Forensic Infrastructures
- Filesystem Data Analysis
- Application Data Analysis
- Digital Forensics in IoT world
- Digital Forensic Tool Development
- Operating System Artifact Analysis
- Cloud Data Analysis
- Counter Anti-Forensics
- Digital Forensic Tool Testing

Products and Services Offered

- Collection and Analysis of Digital Evidence
- Digital Forensics Consulting
- Data Wiping
- Data Leakage Analysis
- Deleted/Damaged Data Recovery

e. Wireless Network Lab.
(Prof. Seong-jun Oh)

The Wireless Network Lab, founded in 2008 to study wireless network technologies in earnest, has been conducting research on evaluation and performance analysis of the 4th and 5th generation wireless communication systems. It is currently studying how to apply machine learning and artificial intelligence technologies to wireless networks.

Research Area

- Spectral Efficiency Improvement for Next-Generation Wireless Communication Systems
- New Spectrum Sharing Mechanism
- Satellite-Terrestrial interference
- New network structure
- Small-Cell
- Physical Layer Security
- Detection of covert communication using machine learning
- Emerging technologies for 6G wireless communications
- Machine Learning in general

f. Security Assessment aNd Engineering Lab.
(Prof. Seungjoo Kim)

Established in 2011, the SANE Lab's research interest lies primarily in developing trustworthy software and hardware development methodology and related base technologies. It conducts security development lifecycle (SDL), security microkernel development research, and security testing and evaluation on cutting-edge equipment such as smart TVs, drones, and military weapon systems in the era of the Fourth Industrial Revolution.

Research Area

- Security/Privacy by Design
- Security Engineering(a.k.a. SDL)
- Security Requirements Engineering
- Secure Architecture and Design
- Secure Code Development
- Automated Risk-Based Security Testing and Verification
- Security Evaluation and Assertion : Common Criteria, CMVP, SSE-CMM, RMF A&A, etc.
- Secure Update
- Supply Chain Security
- Blockchain & Crypto Engineering

Products and Services Offered

- Toolchain for High-assurance S/W and H/W
- Security Development Lifecycle (SDL) Process Establishment Consulting
- Consulting on the security evaluation & certification including CMVP, CC, RMF, etc.

g. Cyber Law & Policy Lab.
(Prof. Hun-Yeong Kwon)

The Cyber Law Policy Lab was established to conduct research based on theories and practices on the norms governing cyberspace. In addition to policy research in various fields such as cyber security, e-government, information disclosure, personal information and privacy, and intellectual property rights, it participates in drafting, enacting, and amending related laws.

Research Area

- Cyberlaw
- Information Security Law and Policy
- Security Policy on e-Government
- Data Protection and Privacy Policy
- Digital Copyrights
- Policy on the Security of Converging Technologies
- Digital Forensics Law & Policy
- Cybercrime/Cyberterrorism
- Cyber Ethics & Digital Citizenship
- Cyber security policy

Products and Services Offered

- Research on Cyber/Information Security Law and Policy
- Cyber/Information Security-related Legal Advice

h. Signal Processing and Advanced Intelligence Lab.
(Prof. Ji Won Yoon)

The Lab's primary research interest lies in analyzing and decoding various signals such as electromagnetic waves using statistical signal processing and artificial intelligence technology. Based on mathematics and statistics (statistical signal processing), it reaches beyond existing research topics to study areas such as security technology development and hidden channel design and detection involving biomedical engineering.

Research Area

- AI Security
- Privacy Preserving Data and Signal Analysis
- Intelligence Research
- Signal and Information Processing for Cyber Security
- Audio and Image Signals Analysis
- Statistical Signal Processing

Products and Services Offered

- Location Tracking through Electromagnetic Signal Analysis
- Long-term Prediction based on Time Series

i. Cryptographic Algorithm Lab.
(Prof. Seokhie Hong)

The Cryptographic Algorithm Lab was established to study the public key cryptography widely used in user authentication, signing, and key exchange and to analyze symmetric key cryptographic algorithms, such as block cryptography, operation mode, stream cryptography, hash functions, and MAC. It has recently performed specialized research on the design and implementation of public key cryptographic algorithms and side-channel analysis for public key and symmetric key algorithms.

Research Area

- Design and Cryptanalysis of Block Cipher
- Security Analysis of Stream Analysis
- Design and Cryptanalysis of Hash Function
- Design and Analysis of Efficient S/W, H/W Cryptosystems
- Design of Cryptosystem on Side-Channel Analysis
- Post Quantum Cryptography

Products and Services Offered

- KLIB Cryptography Library
- Side-Channel Analysis
- Development/Analysis of Block Ciphers

j. Cryptographic Protocol Lab.
(Prof. Dong Hoon Lee)

The Cryptographic Protocol Lab aims to design an efficient and secure protocol suitable for various environments. To achieve this goal, it studies models to prove the safety of cryptography theories and adoptable applications, public key cryptography, digital signatures, authentication, and zero-knowledge proofs, as well as primitives for designing cryptographic schemes.

Research Area

- Efficient and Applicable Digital Signature and Encryption Scheme
- Proof Technique for Cryptographic Protocols
- Multi Signature
- Authentication and Key Agreement
- Zero-Knowledge Proof
- Fuzzy Extractor
- Lattice-based Cryptography
- Functional Encryption

Products and Services Offered

- Contents Distribution Method and System according to Contents Access Control of User Device
- Designing Secure and Efficient Cryptosystems
- Security Analysis of Cryptographic Protocol

k. Risk Management Lab.
(Prof. Kyung Ho Lee)

The Risk Management Lab primarily studies risk assessment and management, information protection consulting, information protection management systems (ISMS, PIMS), information and privacy protection policies, information asset valuation, and privacy impact assessment (PIA). It also conducts various studies to apply risk assessment and management methodology to different and specific environments and targets, including financial security, cyber warfare, IoT, and medical data.

Research Area
•Personal Information Management Technology Conforming to GDPR in IoT Environment
•Blockchain-based Medical Data Exchange System Integrity Technology and Dynamic Consent System Platform
•IoT Security Policy and Technology
•Information Security Consulting
•Information Security & Privacy Policy
•Information Security Management System (ISMS)
•Business Impact Analysis (BIA)
•Privacy Impact Assessment (PIA)
•Risk Analysis and Assessment
•Fintech Security Policy and Risk management
•Personal Information Management Technology
•Security Economic Analysis
•Financial Fraud Detection System
•Cyber Warfare Command &Control
•Cyber Warfare Threat Assessment
Products and Services Offered
•Financial Fraud Detection System
•Study on Information Security Management System
•Mobile Malware Detection Solution

l. Artificial Intelligence Lab.
(Prof. Sangkyun Lee)

The AI Lab is devoted to in-depth research on machine learning algorithms as well as effective applications of artificial intelligence to various fields. It also studies the compression of artificial intelligence models, their robustness against data noise or external attacks, explainable artificial intelligence (XAI), and cybersecurity technologies using artificial intelligence.

Research Area
•Normalization for Effective Learning of Complex AI Models such as Deep Neural Networks
•Big data-based Efficient Learning Algorithm
•Adversarial Attacks against AI, Detection of Attacks, and Defense
•Compression of Complex AI Models
•Applications of Computer Vision
•Time-Series Prediction Models
Products and Services Offered
•Exploring the Model Structure through Normalization
•Big data-based Efficient Learning Algorithm
•Adversarial Attacks against AI, Detection of Attacks, and Defense
•Miniaturization Technique through Compression of Complex AI models

m. Embedded Security Lab.
(Prof. Dong Hoon Lee)

As IT convergence is gaining momentum, embedded systems are increasing faster than ever. The Lab studies the security of embedded systems as well as other specific topics such as autonomous vehicles and connected car security, system software security, obfuscation and reverse engineering, and biometric authentication security based on information protection theory and technology.

Research Area
•Vehicular-IT Security
•Smart Device Security
•Smart Phone Security
•Smart Grid Security
•Sensor Network Security
•Designing & Implementing Crypto System
Products and Services Offered
•Identifying ECU using analysis of electrical signals
•Vehicle Smart-key identification
•Lightweight Cryptographic Library
•Themida Deobfuscation

n. Formal Methods Lab.
(Prof. Jin-Young Choi)

With the aim of developing systems that assure reliability and correctness based on formal methods (formal specification, formal verification), the Formal Methods Lab researches the theories of formal logics and formal methods, security software development methodology, secure coding, coding standards, protocols and requirements verification, and international standard certification processes.

o. Computer Systems Security Lab.
(Prof. Youngjoo Shin)

Founded in 2020, the primary research topic of the Lab involves technologies that offer solutions to various security problems found in computer systems. It studies core base technologies to detect and analyze system software vulnerabilities and counter cyberattacks on computer systems.

Research Area
•Formal Methods
•Secure Software Engineering
•Secure Coding
•Secure Software Development Life Cycle (Secure SDLC)
Products and Services Offered
•Software Security, Reliability and Safety Assurance Technologies

p. Hardware Security Lab.
(Prof. Junghee Lee)

The Hardware Security Lab was founded to study a range of security technologies related to different types of hardware, such as a dedicated hardware like ASIC, processors, memory, and storage. It also studies technologies to improve the security or efficiency of software by using hardware or design secure hardware.

Research Area
•System Security on OS and Hypervisor-based Virtualization
•CPU Micro-architectural Attacks and Mitigation
•Security Analysis of Carrier-grade Network Devices
•Network Security
•Cloud Computing Security
Products and Services Offered
•CPU Microarchitecture Vulnerability Analysis and Attack Detection Technology
•Network Device Security Vulnerability Analysis Technology

q. Hacking and Countermeasure Research Lab.
(Prof. Huy Kang Kim)

Established for data-driven security research, the Lab studies technologies to detect online game fraud, automobile intrusion, and abnormal financial transactions utilizing its own online game service, online payment, and vehicle driving and attack data, as well as cyber threat intelligence and visualization.

Research Area
•Online Game Security
•Automobile Security
•Fraud Detection System
•Cyber Threat Intelligence
•Security Visualization
Products and Services Offered
•Online Game Bot Detection, GFG analysis
•User Behavior Analysis
•Cyber Genome
•Intrusion Detection System for Automotive
•Fraud Detection System
•Mobile App Vulnerability Analysis



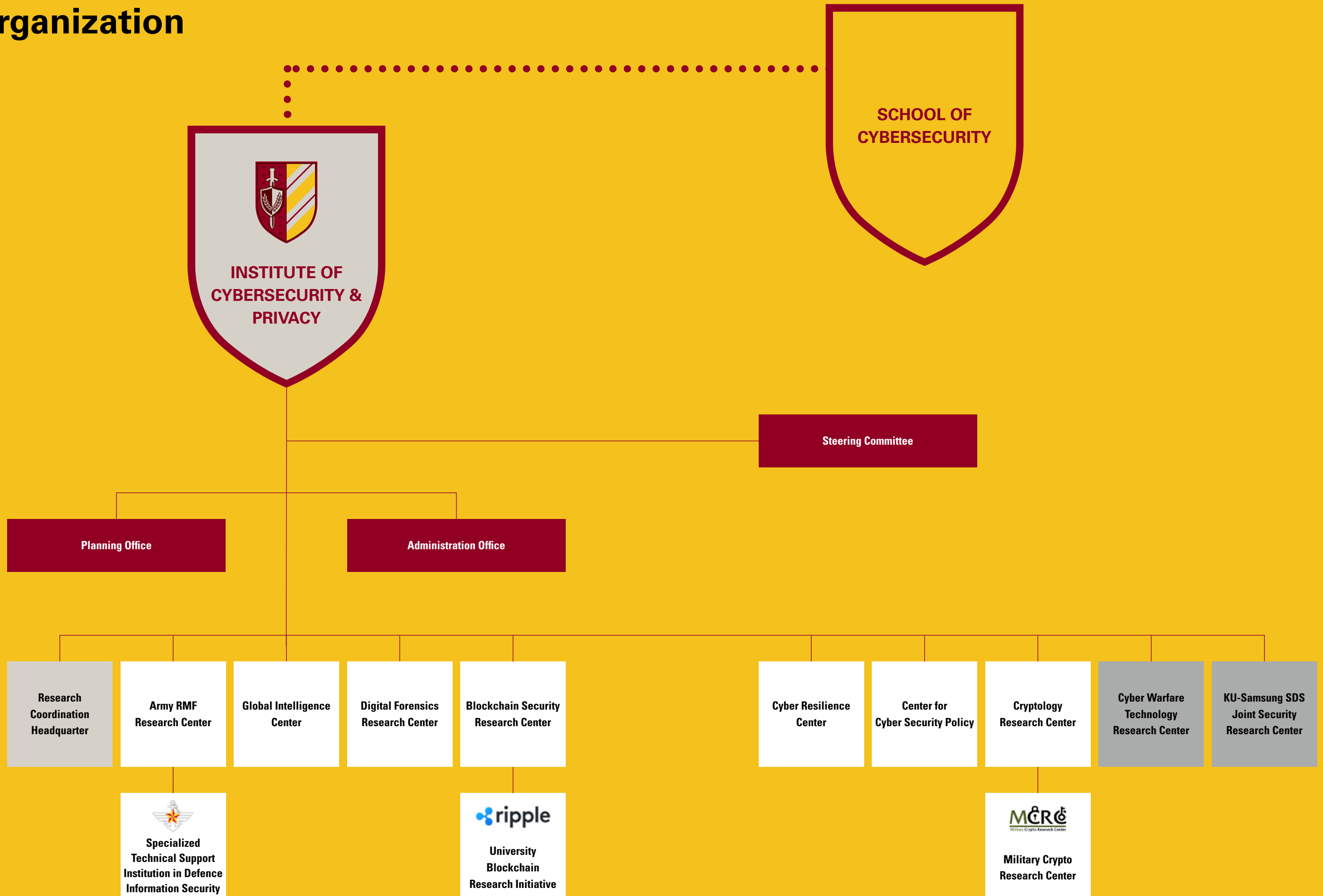
INSTITUTE OF CYBERSECURITY & PRIVACY

Introduction

Affiliated with the School of Cybersecurity, the Institute of Cybersecurity & Privacy aims to make cyberspace and digital technologies safer and more reliable. To achieve the goal, it studies a variety of technologies and policy measures, such as encryption technology, digital forensics, hacking attack response technology, fraud detection technology, artificial intelligence security, and information protection policy.

**Aims to make cyberspace
and digital technologies
safer and more reliable**

Organization



History



1999. 08.	Founded as Korea University's affiliated Center for Information Security Technologies (CIST)
2000. 08.	Selected as a University IT Research Center (ITRC)
2004. 09.	Selected as the best ITRC by the Ministry of Information and Communication
2006. 08.	Selected as the best research center in ITRC Phase 2
2008. 03.	Expanded and promoted from a research center to a research institute with multiple research centers
2008. 06.	Selected for the IT industry source technology development project (Car-Health Care Security Center)
2009. 03.	Selected as Culture Technology Research Center (CTRC; Research Center for Copyright Protection and Fair Use)
2009. 12.	Awarded the Grand Prize at the Digital Forensic Challenge by the DoD Cyber Crime Center (Digital Forensic Research Center)
2010. 06.	Selected as an ITRC (Smart Grid Security Research Center)
2012. 06.	Established the Cyber Defense Research Center (CDRC)
2013. 02.	Selected as a Specialized Technical Support Institution in Defense Information Security by the Ministry of Defense
2014. 01.	Selected as an ITRC (Control System Security Research Center)
2014. 10.	Received the ITRC FORUM 2014 Best Research Achievement Minister Award
2015. 08.	Established an open ICT convergence education center and creative space
2016. 06.	Selected as Communication Policy Research Center (CPRC) (Digital Social Integration Policy Research Center)
2016. 06.	Established the Center for Cyber Security Policy (CCSP)
2016. 09.	Selected as the best research institute among engineering institutes at Korea University (4th time after 2012, 2014, and 2015)

2016. 12.	Established the KU-LIG Nex1 Cyber Warfare Technology Research Center
2017. 04	Established the Cyber Weapons Testing and Evaluation Center (CW-TEC)
2017. 09.	Changed its English-language name to the Institute of Cybersecurity & Privacy (ICSP)
2017. 09.	Reorganized into a structure of 2 offices and 7 centers (established Planning Office, Internet Illegal Activity Response Center, Hacking Information Analysis Center, and Cryptology Research Center)
2017. 09.	Selected as the honorary best research institute among engineering departments at Korea University (3 consecutive years)
2017. 12.	Selected as a Defense Specialized University Research Center (Military Crypto Research Center)
2018. 04.	Reshuffled into a structure of 2 offices and 9 centers by establishing the Blockchain Security Research Center and Cryptocurrency Research Center
2018. 06.	Blockchain Security Research Center selected for the project called the University Blockchain Research Initiative supported by Ripple (17 universities worldwide, the only in Korea)
2019. 10.	Reorganized into a structure of 2 offices, 1 headquarters, and 9 centers by establishing the Research Coordination Headquarter
2020. 03.	Renamed CW-TEC to Army RMF Research Center
2020. 03.	Restructured into a structure of 2 offices, 1 headquarters and 7 centers by establishing the Cyber Resilience Center while closing the Cyber Defense Center, Cryptocurrency Research Center, Internet Illegal Activity Response Center
2020. 04.	Established the KU-Samsung SDS Joint Security Research Center

Research Centers

- a. Army RMF Research Center

Founded in April 2017, the Army RMF Research Center is devoted to research on the methodology of developing, testing, operating advanced weapon systems that are safe against various cyberattacks, while serving as Specialized Technical Support Institution in Defense Information Security designated by the Ministry of Defense. It studies core technologies related to the defense risk management framework (RMF). It consists of a high-reliability encryption equipment development lab, a high-reliability system/network equipment development lab, a high-risk management lab, a red team for simulated hacking of advanced weapon systems, and an external advisory group.
- b. Global Intelligence Center

The Global Intelligence Center was established to provide comprehensive analysis services through cyber- and open source information analysis on various global threats. It continues to develop a cyber genome system that generates and provides cyber threat information (CTI) through malicious code analysis, hacker trend analysis, and hacking event collection and analysis. It carries out various projects such as similarity checks for malicious code families, visualization of similarity between malicious codes based on static and dynamic analysis, and hacker profiling.
- c. Digital Forensics Research Center

The Digital Forensics Research Center aims to study digital forensic technologies and provide digital forensic services under the leadership of KU's Digital Forensic Research Lab, Korea's first university organization for digital forensic research. It has been engaged in various activities such as collecting and analyzing digital evidence, studying legal submission techniques and procedures, developing the nation's own digital forensic standards and guidelines as well as computer forensic tools, and performing open-source projects. It is contributing greatly to improving digital forensics capabilities at the national level, while achieving excellent results in international digital forensic challenges.
- d. Blockchain Security Research Center

The Blockchain Security Research Center was founded to study blockchain security and nurture specialized researchers for the field. It studies technologies to improve blockchain safety and privacy, consensus protocols used in public and private blockchains, smart contracts used in blockchains, and various application protocol designs using blockchain. In 2018, it was selected as Korea's first and only partner university of the University Blockchain Research Initiative (UBRI) project sponsored by Ripple.
- e. Center for Cyber Resilience Research

Established in 2020, the Center for Cyber Resilience Research builds organizational cyber resilience framework capability to sense, resist and react to disruptive cyber events against government and defense operations, and to recover in a timely fashion. To achieve missions above, the Center provides scientific measurement and standardization of cyber disaster damage, identification and analysis of disaster risk factors, development of cyber disaster response training scenarios and expert education content development, case profiling by cyber disaster types, and research on cyber disaster response framework and a resilience platform.
- f. Center for Cyber Security Policy

The Center for Cyber Security Policy was created in 2016 to conduct interdisciplinary research on cybersecurity issues and provide reasonable policy alternatives. It comprises a cyber security lab, cyber law policy lab, risk management lab, privacy protection policy lab, financial security policy lab, and cyber peace and human rights lab. The Center provides various types of services such as security consulting, legal advice, and legislative proposals, as well as conducting policy research to solve cybersecurity problems in various areas both for domestic and international communities and the public and private sectors.
- g. Cryptology Research Center

The Cryptology Research Center was founded to study theories on cryptographic design, analysis, and implementation, the decryption of cryptographic equipment, and hacking into cryptographic device as well as to design cryptographic algorithms suitable for various environments, optimize cryptographic libraries, and develop cryptographic hardware accelerators. It leads research on domestic cryptography-related theories and applications by developing the international standard block cipher algorithm HIGHT, hash functions, quantum (quantum-safe) cryptography, and KLIB accredited by KCMVP (Korea Cryptographic Module Validation Program). Selected as a Defense Specialized University Research Center (DURC) in 2017, it has contributed to securing source defense technologies and nurturing cryptographic researchers.
- h. Research Coordination Headquarters

The Research Coordination Headquarters was created to support the research activities and processes of the Institute of Cybersecurity & Privacy and its affiliated professors such as preliminary research planning, execution, and post-performance management. It performs various support and collaboration tasks, from creating research opportunities through industry-academia research planning, packaging excellent security technologies possessed by affiliated professors, aiding commercialization through platformization, and organizing events to promote and impart research results.
- i. Cyber Warfare Technology Research Center

The Cyber Warfare Technology Research Center was founded in 2016 under a business agreement between Korea University and LIG Nex1, a leading domestic defense company. The Center aims to strengthen the national defense by developing core technologies for cyber warfare and enhancing the security of the defense weapon system. To achieve the goal, it conducts various cooperation programs in the field of cyber warfare technologies, including joint R&D projects, joint hosting of workshops, and support for training.
- j. KU-Samsung SDS Joint Security Research Center

The Center, established in 2020, has promoted long-term industry-academia strategic research cooperation in security technologies between Korea University and Samsung SDS. It conducts various industry-university joint research programs to acquire advanced security technologies while promoting close collaboration to recruit outstanding talents for the security field.



GLOBAL LEADING EXPERTS

Global Leading Experts in Information Security

Korea University
School of Cybersecurity

INFORMATION SECURITY



KOREA UNIVERSITY
SCHOOL OF CYBERSECURITY

address. 02841 Room 615, International Center for Converging Technology Building,
Anam Campus(Science), Korea University, 145 Anam-ro, Seongbuk-gu, Seoul, 02841, KOREA.
tel. 02-3290-4251~3 fax. 02-928-9109 <https://scs.korea.ac.kr/>