Dept. of Financial Information Security

Department of Financial Information Security offers excellent education and interdisciplinary cutting-edge research programs to train future leaders and innovators in information security of financial services industry. Faculties from the fields of mathematics, management information system and business administration provide a broad range of courses and joint research projects in partnership with academia and industry.

❑ **Information Security Major**

Information security major focuses on producing researchers and specialists in privacy protection, protection against hacking, information authentication, and technology evaluation for information security, etc. Our program trains future leaders and innovators in information security by offering an excellent education and cutting-edge research projects.

❑ **Financial Security Major**

Financial security major focuses on producing researcher and specialists in managing and protecting financial big data, legal and institutional aspects of financial information security, consumer-oriented financial services and e-Discovery, etc. Our program trains future leaders and innovators working for secure and sustainable environment in financial service areas by offering an excellent education and cutting-edge research projects.

☐ **Courses**

❑ **Core Courses**

· **Information Security Protocols (3)**

This is an introductory course for financial information security. After providing brief reviews for cryptographic algorithms, the course covers several topics in protocol including key distribution, secret sharing, authentication, and zero-knowledge protocol.

· **Financial Information Security (3)**

We study the information Security Technology in Financial Field, such as Electronic cash, Secure Electronic Transaction, and Internet Banking Systems, etc.

· **Research Ethics & Thesis Study (3)**

This course provides an overview of methods used to conduct and evaluate research. This course will include discussion on the scientific method, development of research questions, exploration of literature, formulation of research designs, and professional critique of methodologies. Also, ethical issues in research are discussed.

· **Legal and Institutional Issues in Informational Security of Financial Services (3)**

This course covers legal and institutional issues in Information Security of Financial Services with real-life examples in the field. For example, information security laws, structures of governments and private firms including financial institutions for information security will be discussed.

❑ **Information Security Major**

· **Cryptographic Algorithms (3)**

We study classical cryptography and modern cryptography such as stream ciphers and block ciphers based on Shannon theory.

· **Hash Functions and Message Authentication (3)**

This course covers the design principle of collision-free hash functions and message authentication codes which can be used in digital signatures.

· **Cryptanalysis of Public-key Cryptosystems (3)**

This course covers the cryptanalysis of public key cryptosystem based on the mathematical methods such as factorization of numbers, discrete logarithm problems.

· **Topics in Symmetric Key Cryptanalysis (3)**

This course covers the cryptanalysis of symmetric key cryptosystem such as stream ciphers and block ciphers.

· **Parallel Implementation of Cryptographic Algorithms (3)**

This course provides a systematic approach to parallel implementations of cryptographic algorithms. Topics include a brief introduction to computer architecture and operation system. Particularly, parallel computing with GPU will be considered in depth.

· **Evaluation and Validation Techniques for Cryptographic Modules (3)**

This course is an introductory guide for developers who build cryptographic modules. Mandatory standards for cryptographic modules including ISO 19790, 24759, and FIPS 140 will be considered. Students are supposed to understand CMVP(Cryptographic Module Validation Program) in US and Korea and related polices. Also, techniques for security evaluation will be studied.

· **Side Channel Attacks (3)**

This course covers any attack based on side channel information such as timing information, power consumption, electromagnetic leaks or even sound gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis).

· Countermeasures of Side Channel Attacks (3)

This course provides secure S/W and H/W cryptographic design and implementations against side channel attacks. The countermeasures fall into two main categories: (1) eliminate or reduce the release of such side channel information; and (2) eliminate the relationship between the leaked information and the secret data.

· Security Implementation Methodology (3)

This is a practical guide for implementing security functions. Based on the understanding of cryptographic algorithms, students are required to build an application as a group project and learn how to protect their software from malicious attacks by removing potential vulnerabilities.

· Introduction to PKI (3)

The goal of the course is to provide an introduction to PKI (Public Key Infrastructure) and relevant technologies including public key encryption, authentication, and digital signature. As an application. we study how to apply PKI to financial services.

· Mobile Security (3)

We study the latest mobile networks security architecture and technology.

· Wireless Security (3)

We study the latest wireless communications technology and the security technology of the applications.

· IT Convergence and Security (3)

We study Convergence Technology on IT field and other fields, and the security technology of the applications.

· Financial Information Security Policy (3)

We study the management and the policy of information security. We study the management methodology that can supplement the limit of information security techniques.

· Information Security Consulting (3)

This course is a field that focuses on advising IT businesses on how best to use information technology to meet their business objectives. To providing advice, we study how to estimate, manage, implement, deploy, and administer information security products or the IT security related organization about security level, vulnerability, policy, standard, and monitoring process.

· Information Security System Evaluation Methodology (3)

This course covers evaluation methodology for information security systems. To understand conformance tests, we refer testing methodology in CC (Common Criteria),

CMVP(Cryptographic Module Validation Program), and PIV(Personal Identity Verification).

· Analysis and Implementation of Security Technical Standards (3)

This course has two main goals. One is understanding of standardizations of security techniques and the other is having ability to build systems based on the standard techniques. We refer standard documents by ISO/IEC, IETF (Internet Engineering Task Force), ITU-T. Students are supposed to be familiar with standards and applying them.

· Introduction to Digital Forensics (3)

We study the forensic science encompassing the recovery and investigation of material found in digital devices such as personal computers, notebook computers and cellular phones, often in relation to computer crime.

· Special Research of Digital Forensics (3)

Study and research current cutting-edge technologies and methodologies in digital forensics.

· Financial Device Attacks (3)

The goal of the course is how to seeks and exploits weaknesses in financial device such as PC, smart phone, smart card, Micro-SD, OTP and so on. And then we study some countermeasures which are secure against these attacks.

· Countermeasures against Financial Device Attacks (3)

Study various H/W- and S/W-based methods and technologies for protecting financial transaction devices from current avaliable security attacks.

· Financial Key Management System (3)

Study key management systems used for providing secure financial services and protecting systems for those services. Students will study the current technologies and theories applied in generating, distributing, and recovering keys used in security systems and mechanisms for financial transactions.

· Financial Networks Security (3)

Students will learn security technologies and theories for protecting important and valuable financial data transmitted through communication systems, e.g., VPN (Virtual Private Networks), IPSec, SSL, TLS, and so forth.

· Electronic Commerce Security (3)

Topics covered include information security schemes to protect the electronic commerce, especially electronic cash, electronic payment, electronic wallet.

· Provable Security (3)

Deals with Computational complexity, Unconditional security, Complexity theoretic

security, Provable security under assumptions, Ad hoc security.

· Implementation of Cryptographic S/W (3)

Acquire the software implementation technologies of International standard Symmetric Key Encryption Algorithm and public key Encryption Algorithm.

· Analysis of Randomness (3)

Deals with Probabilistic theory of randomness, Design and security analysis of cryptographic random number generators, Statistical test of random sequences.

❑ Financial Security Major

· Advanced Information Communication Theory (3)

It aims to educate about the ubiquitous network and context awareness and localization that are the core technologies of computing. It provides information on various application systems including context-awareness / localization, and ubiquitous network architecture, requirements of ubiquitous network, etc.

· Model-based System Design (3)

This course is an introduction to model-based system design with domain specific and domain independent aspects. The metamodeling concepts are introduced for various information systems, and hybrid system such as cyber physical systems. From the fundamental system design with UML up to metamodeling system design will be covered. The object programming language is used to implement the design process.

· Data Mining (3)

Data mining is concerned with the extraction of novel knowledge from large amounts of data. This course introduces and studies the concepts, issues, tasks and techniques of data mining. Topics include data preparation and feature selection, association rules, classification, clustering, evaluation and validation, scalability, spatial and sequence mining, and data mining applications.

· Data Management (3)

This course is concerned with the use of Database Management Systems (DBMS) to solve a wide range of information storage, management and retrieval problems, in organizations ranging from large corporations to personal applications, such as research data management. The course combines the practical aspects of DBMS use with more theoretical discussions of database design methodologies and the "internals" of database systems.

· IoT Network (3)

It educates about the next generation network such as IoT(Internet of Things), M2M(Machine to Machine Communication), WoT(Web of Things), UIoT(Underwater IoT) and so on. Furthermore, we will also study about the related international standards.

· **Embedded System (3)**

This course aims to enhance the understanding of ARM architecture and the ability to design and implement embedded system based on firmware.

· **Real-time System (3)**

This course aims to enhance the understanding of real-time system and the ability to design and implement embedded system based on RTOS(Real-Time Operating System).

· **Information System Development Methodology (3)**

It educates about the methodology of developing information system concerning embedded system. Thus, we will study about the data structures and algorithms, the overall process of design and implementation of embedded system and so on.

· **Intellectual Property and IT Patent (3)**

This course focuses on promoting the global mind on intellectual property among the university students by studying IP education course. The fundamental concepts of intellectual property such as patent, trademark, industrial design, and patent information are covered, and the impact of IP on international trade also studied in the perspective of business domain and IT applicable domains.

· **Financial Management (3)**

An introduction to advanced concepts and methods of financial management. Topics include risk and return, asset evaluation, capital budgeting, capital structure, business financial planning and working capital management.

· **Financial Institutions (3)**

This course focuses on financial institutions, and will cover both markets and intermediaries. We will examine the structure of debt, equity and derivatives markets, as well as specific financial instruments traded on these markets. In addition, we will study financial intermediaries such as commercial and investment banks, mutual funds and insurance companies in order to develop a critical awareness of the risks faced by these institutions.

· **Statistics for Financial Analysis (3)**

This course deals with statistical techniques related to financial analysis. The techniques include probability & sampling distributions, estimation, hypothesis testing, linear and nonlinear regression, experimental design, modern business decision theory.

· **Financial Engineering (3)**

This course is the design, development and implementation of innovative financial products and financial processes in the major segment of equities, currencies, interest rates and commodities for trading investment hedging and complete risk management.

· Principle of Entrepreneurship (3)

This is an introductory course focusing on the individual entrepreneur, the generation of innovative business ideas, the creation of business ventures, and the role of entrepreneurship within society.

· Practice of Entrepreneurship (3)

This course is aiming to inspire students and provide them with the entrepreneurial skill and confidence needed to put plans into action. Students gain a full understanding of the practice of entrepreneurship through exposure to the experience of successful entrepreneurs and are given a solid understanding of the realities of business start-up.

· Entrepreneurial Finance (3)

This course examines the elements of entrepreneurial finance, focusing on technology-based start-up ventures and the early stages of company development.

· Strategic Management of Technological Innovation (3)

This course examines certain fundaments of enterprise success as derive from the strategic management and innovative deployment of technology – with particular emphasis on the ICT sector.

· Strategic Management (3)

This course covers topics of mission, goal, strategy formulation, strategy implementation and strategy evaluation. Strategic techniques include Industry: Analysis, Analysis of the Competitive Environment, Key Success Factors, Strategic Scenario Analysis and SWOT Analysis. Additional topics covered include strategic thinking, competitive advantage, vertical and horizontal integration, and planning horizon.

· Entrepreneurship in Financial Information Security

This course focuses on the industry structure, especially the barriers to potential entrants and competition, and market characteristics in the area of financial information security. The course also provides the analysis of successful startups, which allows students to design appropriate business model for their potential entrepreneurial opportunity.

· IT Audit Technique (3)

We study an information technology audit, which is an examination of the management controls within an Information technology (IT) infrastructure. It covers IT audit process such as planning, studying and evaluating controls, testing and evaluating controls, reporting and follow-up. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives.

· **Business Data Communication (3)**

This course is about the fundamentals of data communications and networking. We will discuss information representation, network topologies, transmission medium, OSI model and TCP/IP networking models, and mainstream LAN and WAN technologies. The OSI model is used as a framework to organize and discuss the network technologies. The technical and managerial aspects of data communications and networking are both emphasized.

· **Cloud Computing (3)**

This course introduces the fundamental technologies and issues in this cloud computing environment. In terms of everything as a Service in cloud computing service, we learn main considerations in SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service), and the related technologies. Students learn concepts and applicable areas of infrastructure system of cloud computing and VM provisioning via cloud environment. Also we will study the trends of enterprise cloud adoption, application integration, and various service provider and application to form the cloud service.

· **Big Data Infrastructure System (3)**

This course provides the fundamental concepts and knowledge of distributed system and middleware technologies for Big Data Infra system architecture. To understand IT infrastructure of Big Data processing, this course gives a lesson about the Hadoop Distributed File System and Map Reduce technique for storing and processing big data. Also, the recent IT evolution of conventional infra system of the Big Data domain and applications is introduced. Distributed systems, middleware, Hadoop Ecosystem, infra technologies, and IT service architectures are covered.

· **Financial Accounting (3)**

Financial Accounting provides an introduction to the concepts and uses of financial accounting information in a business environment and its role in the economic decision-making process.

· **Managerial Accounting (3)**

This course examines the principles, techniques, and uses of accounting in the planning and control of business organizations from a management perspective.

· **Investments (3)**

An examination of investment markets, transactions, planning and information. Topics include investment risk and return measures, debt and equity instruments, evaluation techniques, hybrid and derivative securities, mutual funds, real estate investments, tax planning and the investment process, and portfolio management.

· **Research Methodology in Finance (3)**

This course is an introduction to empirical methods commonly employed in finance. The course is organized around empirical papers with an emphasis on econometric methods. heories and real-life cases of risk management in corporations and financial institutions.

· **Derivatives (3)**

In this course, students develop an understanding of financial derivative instruments and their applications to corporate strategy and risk management.

· **Introduction to Payment and Settlement System (3)**

This course covers legal and institutional structures on payments and settlements among financial institutions. Also, the course identifies risks that arises from payments and settlements and discusses how to manage the risks.

· **Operational Risk Management (3)**

This course focuses on the risks arising from the people, systems and processes through which a company operates. It also include other classes of risk, such as fraud, legal risks, physical or environmental risks.

☐ Faculty Members

Yi, Okyeon
Korea Univ., B.S.
Korea Univ., M.S.
University of Kentucky, Ph.D.
Mobile security and cryptographic module
oyyi@kookmin.ac.kr

Kang, Ju-Sung
Korea Univ., B.S.
Korea Univ., M.S.
Korea Univ., Ph.D.
Design and security analysis of cryptographic algorithms
jskang@kookmin.ac.kr

Han, Dong-Guk
Korea Univ., B.S.
Korea Univ., M.S.
Korea Univ., Ph.D.
Cryptographic engineering - Cryptographic implementations, Attacks against implementations and countermeasures against these attacks
christa@kookmin.ac.kr

Yeom, Yongjin
Seoul National Univ., B.S.
Seoul National Univ., M.S..
Seoul National Univ., Ph.D.
Implementation and evaluation of cryptographic techniques
salt@kookmin.ac.kr

Kim, Jongsung
Korea Univ., B.S.
Korea Univ., M.S.
Katholieke Universiteit Leuven, Ph.D.
Design and Cryptanalysis of cryptographic algorithms
jskim@kookmin.ac.kr

Park, Soo Hyun
Korea Univ., B.S.
Korea Univ., M.S.
Korea Univ., Ph.D.
Research for Ubiquitous network, M2M /IoT techniques.
shpark21@kookmin.ac.kr

Choi, Eunmi
Korea Univ., B.S.
Michigan State University, M.S.
Michigan State University, Ph.D.
Distributed System and Cloud Computing
emchoi@kookmin.ac.kr

Kim, Dohyeon
Seoul National Univ., B.S.
Seoul National Univ., M.S.
University of Warwick, Ph.D.
Entrepreneurship and strategic management
drkim@kookmin.ac.kr

Kwon, Yongjae
Sogang Univ., B.A.
Michigan State University, M.A., M.S.
George Washington University, Ph.D.
Investments and Risk Management
yjkwon@kookmin.ac.kr

Dong-Chan Kim
Sogang Univ., B.S.
Sogang Univ., M.S.
Sogang Univ., Ph.D.
Cryptography, Coding theory
dckim@kookmin.ac.kr

Seo, SeogChung
Ajou Univ., B.S.
GIST, M.S.
Korea Univ., Ph.D.
Information Security
scseo@kookmin.ac.kr