【신청서요약문】

<신청서 요약문>

<table>
<tr><td rowspan="3">중심어</td><td>정보보안</td><td>5G / 6G 이동통신 보안</td><td>디바이스 보안</td></tr>
<tr><td>암호기술</td><td>인공지능 (AI)</td><td>디지털 포렌식</td></tr>
<tr><td>양자내성암호</td><td>초연결사회</td><td>초신뢰사회</td></tr>
<tr><td>교육연구단의 비전과 목표</td><td colspan="3">▣연구단 목표 : 안전한 초연결사회를 위한 문제해결형 정보보안 교육연구 및 전문인력 양성
- 미래통신 정보보안 전문인력 양성
- 디바이스 보안 및 포렌식 전문인력 양성
- 양자내성암호 전문인력 양성
- 자율성장 AI 보안기술 기반 지능형 시스템과 사회 안전망 확보 기술 전문인력 양성</td></tr>
<tr><td>교육역량 영역</td><td colspan="3">▣ 교육관점에서 교육연구단의 특징
- 정보보안의 특성상 컴퓨터공학 및 암호 전공자의 융합 학문분야이며, 어느 한쪽의 전공지식만으로는 정보보안 위협을 이해하거나 대응할 수 없는 분야임
- 본 교육연구단은 정보보안전공 교수 7인과 컴퓨터공학 전공 교수 3인의 교수들로 구성되었으며, 중견교수 및 신진교수의 구성이며, 경험과 도전정신을 모두 갖춘 연구단임
- 또한, 교수진은 미래 초연결사회에 필수적으로 요구되는 AI 보안, 무선통신 보안, 이동통신 보안, 암호모듈 국가검증, 암호설계 및 분석, 디바이스 보안 등 5G/6G 초연결시대에 필수적인 다양한 정보보안 전공경험과 실무 경험을 모두 갖추고 있음
- 또한, 단순 강의가 아닌 다양한 외부과제 및 정보보안 사례 기반 교육, 프로젝트 기반 교육 등 다양한 교육방법을 통해 교육하며, 강의평가가 매우 우수함
- 5G, 6G, IoT 기반의 지상망을 중심으로 위성, 수상통신, 수중통신에 이르는 공간통신의 모든 연결성 완성을 목표로 진행되는 초성능, 초대역, 초공간, 초정밀, 초지능, 초경험 시대의 초신뢰 정보보안 전문인력 양성을 위한 교육역량을 갖춤
- IT 환경의 소재/부품/장비를 구성하는 정보보안 제품에 대한 부채널 정보 기반 디바이스 역공학 지식 및 기술을 함양한 인재를 양성할 역량을 갖춘 교육연구단이며 부채널 정보 수집 기술, 분석 성능 향상을 위한 부채널 신호 처리 기술, 부채널 신호에 내재되어 있는 유의미한 정보 추출 기술 교육을 통한 전문인력이 가능함
- IaaS, PaaS, SaaS 각각에 대한 특징과 각 서비스에 대한 네트워크 선행 교육을 실시하고, 이후 클라우드 컴퓨팅 환경에서의 다양한 데이터 접근, 전송, 암호화 과정 등의 정보보안을 교육하는 적정한 교육프로그램을 갖춤 또한, 기존 ICT 인프라의 보안체계를 양자컴퓨팅 환경에서도 안전한 양자내성 암호 기반으로 교체할 수 있는 전문인력 양성 프로그램을 보유함
- 이와 같은 전문인력 양성 프로그램은 기존 보안체계에 대한 깊은 이해와 문제점들의 명확한 파악이 반드시 선행되어야 하며, 최근 제안되는 다양한 보안공격 기법들을 항상 예의주시하면서 미래암호의 방향성을 제시할 수 있을 것임
- 본 교육연구단은 IoT 기술과 관련된 통신 시스템, 대용량 데이터 기반 AI 기술, 적대적 공격 및 방어와 관련된 교육 체계를 보유하고 있으며, 이에 대한 프로젝트 기반 수업을 통하여 학생들이 실제 사회에서 발생할 수 있는 다양한 문제를 해결할 수 있는 능력을</td></tr>
</table>

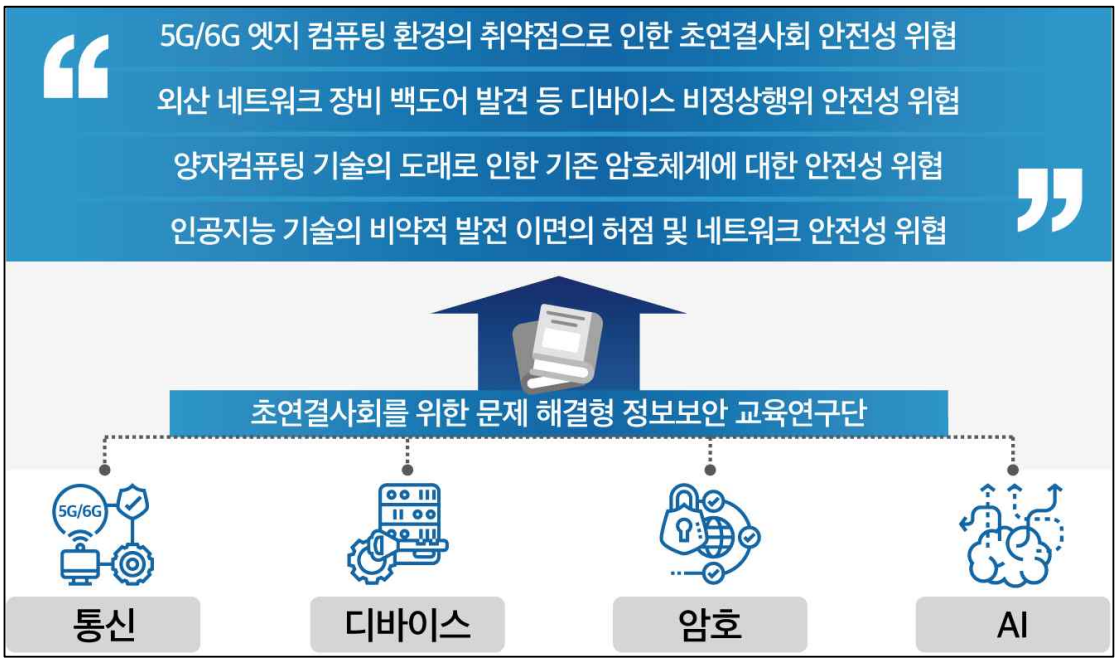
	갖출 수 있도록 하는 교육프로그램을 보유함
연구역량 영역	**▣ 연구관점에서 교육연구단의 특징** **▶다양한 정보보안 산업문제 해결 역량 보유한 연구진으로 구성** - KIST 양자정보연구단과 양자난수발생기 공동연구 진행하여 국내 특허 2건 등록 - 화이트박스 암호 연구를 진행하여 국내 특허 4건 등록과 기술이전 2건 - 디자인 및 영상 유사도 검색 및 표절 시스템 개발 및 특허 등록 - M2M/IoT(사물인터넷) 환경용 지능형 디바이스 플랫폼 설계 방안 기술이전 - 난수발생기 구조, 엔트로피 평가 방법 관련 국내 특허 6건 등록, 1건의 기술이전, TTA 표준문서 제정 및 개정함 - ISO/IEC SC27 WG2 한국대표로 활동하며, ISO/IEC 29192-2:2019 프로젝트 주도함 - 양자 컴퓨팅 환경을 위한 암호키 설정 방법의 최적화 구현 기술 제시함 - 교통신호제어기 표준 내 통신보안규격 및 군 드론 안전성 검증 기술 개발함 - 한국전력공사 전력연구원과 공동으로 스마트그리드용 검증필암호모듈 개발함 - IoT, 스마트미터 등 6G에 포함될 수 있는 다양한 환경에서 보안 서비스 개발함 - 동글 사용 무선 키보드 취약성 및 Mifare 카드 복제 가능 취약점 분석함 **▶새로운 사회문제 해결 역량 보유한 연구진으로 구성** - 세계적인 포렌식 업체와 함께 협력하여 본 교육연구단에서의 교육 및 연구를 통해 개발한 분석기술을 상용화하여 포렌식 수사에 기여하고 있으며, 포렌식 분석 시장을 선도하는 기술을 보유함 - 카카오톡이나 한글과컴퓨터 등 세계적인 포렌식 업체에서도 그 분석을 지원하지 못하는 실정이고, 신규 기기나 새로운 프로그램에 대한 분석, FBE/FDE, iOS와 같은 환경에서의 데이터 분석은 세계적인 포렌식 분석도구 개발 업체에서도 불가능한 경우가 많으나 본 교육연구단은 해당 분야의 연구역량을 갖고 있음
기대 효과	**▣ 산업・사회문제 해결형 정보보안 전문인력 양성의 기대 효과** **▶통신환경의 정보보안 분야 핵심기술 전문인력 양성** - 5G, 6G, WiFi, 무선 LAN, TVWS 등과 같은 무선망용이나 이동통신망용 암호 장비 개발과 사회 기간 이동통신 및 무선 서비스를 위한 핵심 암호 기술을 바탕으로 국내외 IT 산업 및 사회에서 필요한 정보보안 전문가 양성에 기여함 **▶디바이스 보안 전문인력 양성** - 자국 기술력 확보를 통해 기존 해외로 유출되는 기술 컨설팅 비용 등의 절감을 위한 국내 산업을 위한 전문 인력을 양성하고, 민간-공공 산업에 배출하여 국외 기술 의존도를 낮추고, 국내 정보보안 보안 수준 향상 및 국가 경쟁력 향상에 기여함 **▶양자내성암호 분야 핵심기술 전문인력 양성** - 최근 많은 글로벌 기업들의 양자 컴퓨터 개발이 가시화 되고 있으며, 실용적 수준의 양자 컴퓨터 시대가 가시권에 들어왔기 때문에, 이러한 시대의 변화에 대비하기 위해 기존 암호를 시급히 양자내성암호로 교체하는 산업 및 사회의 정보보안 시스템 구축에 필요한 정보보안 전문인력 양성으로 국내외 산업 및 사회 발전에 기여함 **▶자율 성장 AI 보안 인력 양성을 통한 학계 선도 및 새로운 융합 연구 개척** - AI 기술이 다양한 산업 및 사회에 내재되는 상황에서 AI 기술의 허점을 활용한 공격을 방어할 수 있을 뿐만 아니라, 정보보안 기술의 개발을 통하여 지능형 시스템의 안전성과 신뢰성 확보가 가능함

I. 교육연구단 구성, 비전 및 목표

1. 교육연구단 구성, 비전 및 목표

1.1 교육연구단의 필요성

▣ 연구단 목표 : 안전한 초연결사회를 위한 문제해결형 정보보안 교육연구 및 전문인력 양성



▶ 안전한 초연결사회를 위한 5G/6G 이동통신 정보보안 전문인력 양성

- 이동통신 네트워크 산업의 특성으로 초기 R&D 대응 미흡으로 기술 선도그룹에서 뒤쳐질 경우, 글로벌 경쟁력 및 주도적 지위의 상실이 우려되어 기술 선점과 표준화 주도가 반드시 필요하므로, 해당 분야의 전문인력 양성이 시급함
- 이동통신 기술 표준화를 담당하고 있는 3GPP 내 보안 워킹그룹은 3GPP TSG WG3이며, WG3에서 담당하고 있는 이동통신 보안 내 암호기술표준은 전체 보안 표준 189개 중 157개인 약 83%로 이동통신 암호 기술은 반드시 필요한 연구 분야임
- 대한민국에서는 표준화 기구인 TTA와 삼성전자, LG전자 등이 3GPP에 참여하고 있지만 정보보안 분야에서는 참여하고 있는 단체 및 기업이 전무한 상황임
- 5G에서의 초고속, 초저지연, 초연결 네트워크의 구축과 6G에서의 초성능, 초대역, 초경험, 초지능, 초정밀, 초공간 네트워크의 구축은 다양한 산업 및 서비스간의 융합화가 예상되는 가운데 스마트 기기 및 IoT 기기, 자율주행차, 드론 등 다양한 연동에 따른 암호화 및 인증 등의 정보보안 인력양성이 요구됨
- 5G 이후의 이동통신 서비스는 저사양의 IoT 장치, 임베디드 장치부터 고성능 PC와 클라우드 서비스까지 모두 네트워크에 연결시키는 방향으로 발전 중이고, 특히 2020년 말까지 네트워크에 연결되는 장치가 약 260억개로 예상됨에 따라, 다양한 사이버 공격에 대비하고자 하는 가용성 높은 암호 기술 연구가 필수적임
- 사물인터넷(Internet of Things, IoT) 시대의 현실화 및 이동통신 기술 발달로 인하여 데이터 중심의 '초연결사회(Hyper Connected Society)'가 가속화되고 있으며, 현재의 5G 및 도래할 6G 시대에서는 모든 데이터가 연결되어 공유(Open) 및 상호작용(Interactive)을 하므로 기본적인 연결성 이외에도 체계적인 정보보안 및 보안 시스템이 중요한 요소로 대두되고 있음

▶ **안전한 초연결사회를 위한 디바이스 보안 전문인력 양성**

- 2011년과 2012년 영국의 다국적 통신회사인 보다폰이 이탈리아에서 운용하던 외산기업의 네트워크 장비에서 백도어를 발견함
- 2020년 1월 미국 온라인 커뮤니티 레딧에서 2018년 이후 출시된 삼성 갤럭시 스마트폰 전 제품에 설치되는 기본 앱이 타국의 무료 백신 프로그램인 치후 360을 사용하고, 캐시 정리를 할 때 타국 서버와 통신을 한다는 사실이 밝혀져 논란됨
- 전 세계적 이슈인 백도어를 탐지하여 자국의 산업 보호 필요성이 부가되었고, 국외에서는 2002년부터 부채널 정보를 이용하여 스마트카드 등과 같은 임베디드 장비에서 동작하는 알고리즘 정보를 획득하는 부채널 정보 기반 디바이스 역공학 기술 연구를 진행하고 있지만, 국내에서의 관련 연구 및 인력양성 프로그램은 충분하지 않음
- 부채널 정보 기반 디바이스 역공학 기술 연구를 통해 디바이스 이상행위 탐지 절차 수립 기술 확보 및 관련 전문인력 양성이 필요함
- 최근 n번방 사건에서의 텔레그램 어플리케이션 분석까지 사회적으로 큰 파장을 일으킨 사건들의 디지털 증거 분석에는 포렌식 전문가가 필수적임
- 디바이스 포렌식의 사회적 중요성을 뒷받침하듯, 정부 부처별 디지털 포렌식(증거 복원 · 분석) 장비 · 프로그램 관련 2020년도 정부 예산안에 따르면 디지털 증거 분석 관련 수요가 연 21.4%씩 폭발적으로 증가함
- 다양하게 등장하는 새로운 디지털 기기 분석기술에 대한 교육 및 연구가 필요하며, 적절한 디지털 증거 수집 능력을 함양을 통해, 5G/6G 기반의 새로운 서비스나 어플리케이션이 가지는 데이터 분석능력을 갖춘 전문가가 필요함
- 2020년 1월, 국회 본회의를 통과한 데이터 3법 개정안의 주요 내용 중 하나는 데이터 이용 활성화를 위한 가명 정보 개념을 도입하여 사용할 수 있다는 점으로, 이에 따라 암호화가 된 개인정보를 원래의 정보 없이 다룰 수 있는 동형 암호가 대두됨
- 동형 암호는 암호화가 된 상태로도 사용자가 원하는 연산을 수행할 수 있어 사용자 프라이버시 보호가 가능한 것으로 알려져 있으나, 연산이 매우 느리다는 단점이 있음
- 이에 따라 해외에서는 IBM, MS를 필두로 연산 속도를 보완하기 위해 소프트웨어 환경에서 벗어나 하드웨어적으로 동형 암호를 고속 구현하는 연구가 활발히 진행되고 있음
- 그러나 국내에서는 하드웨어 상에서 동형 암호를 고속 설계하는 전문가가 부족한 상황이며, 따라서 국내에서도 데이터 3법 하에서 동형 암호를 포함하여 다양한 보안 응용을 효율적으로 설계하고 구현할 수 있는 정보보안 및 암호기술 전문인력 양성이 필요함

▶ **안전한 초연결사회를 위한 암호 전문인력 양성**

- 오늘날 세계가 사용하는 DH 키공유암호(1976년), RSA 공개키암호(1977년), 타원곡선 암호(1985년)는 수학적 난제로 분류되는 인수분해 문제와 이산대수 문제를 기반으로 설계된 암호이며, 현재의 컴퓨팅 및 네트워크 환경의 변화에 따라 안전성 위협이 계속되고 있음
- 암호의 안전성 수준(security level)은 기반 문제의 해법 알고리즘 계산복잡도에 의해 결정되며, 1994년 Peter Shor가 인수분해/이산대수 문제는 양자의 성질을 이용하면 다항식 시간 내에 풀 수 있음을 증명
- 최근 양자 컴퓨팅 기술이 비약적으로 발전하면서 기존 암호 체계의 안전성을 위협함
- 영국 GCHQ/NCSC와 미국 NIST에서는 2030년경에는 암호해독 전용 양자 컴퓨터 등장이

가능할 것이라고 전망함(GCHQ whitepaper, Quantum-safe Cryptography, 2016.11월)

- 암호 학계는 실용적 양자컴퓨터 시대를 대비하기 위해 양자 내성 암호(Quantum Safe Cryptography)라는 (포스트 퀀텀 암호(PQC, Post Quantum Cryptography)라고도 함) 이름의 새로운 방식의 암호 알고리즘을 제안하기 시작함
- 2016년부터 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)가 주관하여 국제 양자 내성 암호 표준 알고리즘 공모전이 진행 중이며, 2021년에 알고리즘을 선정한 후 2024년에 표준으로 제정할 예정임
- 미숙한 암호의 구현과 사용은 암호의 기대 안전성 저하를 초래하게 되며, 현재 대부분의 양자 내성 암호 표준 후보 알고리즘은 구조가 복잡하여 구현 난이도가 매우 높고, 파라미터 설정 등 사용 방법 또한 매우 다양하기 때문에, 알고리즘 관련 지식을 습득하는 데 오랜 시간이 필요함
- 따라서 기존 ICT 인프라의 보안체계를 양자컴퓨터에서도 안전한 양자 내성 암호 기반으로 교체하기 위한 장기간의 전문 인력양성 프로그램이 필요함

▶ 자율성장 AI 보안기술을 활용한 지능형 시스템과 사회 안전망 확보 기술 전문인력 양성

- 딥러닝을 비롯한 기계학습 기술의 발전으로 기존의 수동 가공된 데이터 기반 AI 기술은 데이터의 특성 및 양에 따라 성능이 좌우되며 보안성이 취약하여 이를 개선하기 위하여 많은 시간과 비용이 요구됨
- 학습된 데이터를 활용할 수 있는 도메인이 제한적이기 때문에 다른 분야에의 적용 및 확산에 제한적임
- 미국에서는 구글, 마이크로소프트, IBM과 같은 거대 IT 기업을 중심으로 다양한 AI 기술을 활용하여 다양한 IoT 서비스를 제공하고 있으며, 이 과정에서 발생하는 다양한 데이터를 수집・분석하기 위한 데이터 센터 및 관련 연구를 진행하고 있음
- 중국에서는 바이두 및 텐센트를 중심으로 한 IT 기업에서는 모바일 환경에서 수집된 데이터를 기반으로 다양한 사회문제를 선제적으로 분석함과 동시에 이를 활용하고 있음
- 샤오미는 홈 IoT 관련 제품을 출시함과 동시에 관련된 데이터를 기반으로 스스로 성장할 수 있는 AI 기술을 확보하고 있으나, 해킹 등 관련 문제가 발생하고 있기 때문에 이에 대한 해결 방안에 대한 연구가 진행되고 있음
- 자율 성장 환경 취약점 발견 및 보안 기술을 통한 사회 지능형 시스템의 안정성 확보가 필요하며, 해당 분야의 전문인력 양성 프로그램 구축이 시급함
- 기술 개발 내/외부 공격에 의하여 변형 조작된 데이터는 자율 성장에 방해가 되며, 지능형 시스템에서 매우 심각한 문제를 야기할 수 있기 때문에 이에 대한 이해 및 방어 기술이 필요하고, 해당 분야의 전문인력 양성 프로그램 확보가 시급함

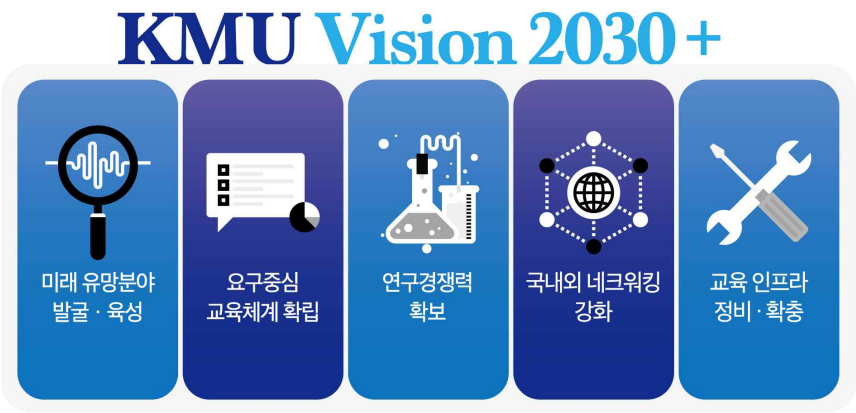
1. 교육연구단 구성, 비전 및 목표

1.2 교육연구단의 비전 및 목표

▣ 본 교육연구단의 비전

▶제안기관 및 학과 소개

- 국민대학교는 1946년 해공 신익희 선생을 비롯한 상해 임시정부 요인들이 건국에 필요한 인재를 양성하고자 설립한 해방 후 최초의 사립대학으로서, '민족정체성을 지닌 민족인', '인본주의에 기반한 지도자', '지식사회를 선도하는 전문인', '세계화 정보화에 부응하는 실용인' 육성을 교육목적으로 정하고 이를 달성하기 위해 지금껏 다양한 지원과 노력을 기울여 왔음
- 정보보안기술과 초연결사회에 대한 균형 잡힌 이해를 바탕으로 전문성을 발휘할 수 있는 융합형 정보보안 전문인력을 양성하기에는 협동과정 운영이 효과적이므로, 2014년부터 정보보안 전문가 양성을 위한 협동과정으로 대학원에 학과를 설치 운영해오고 있음



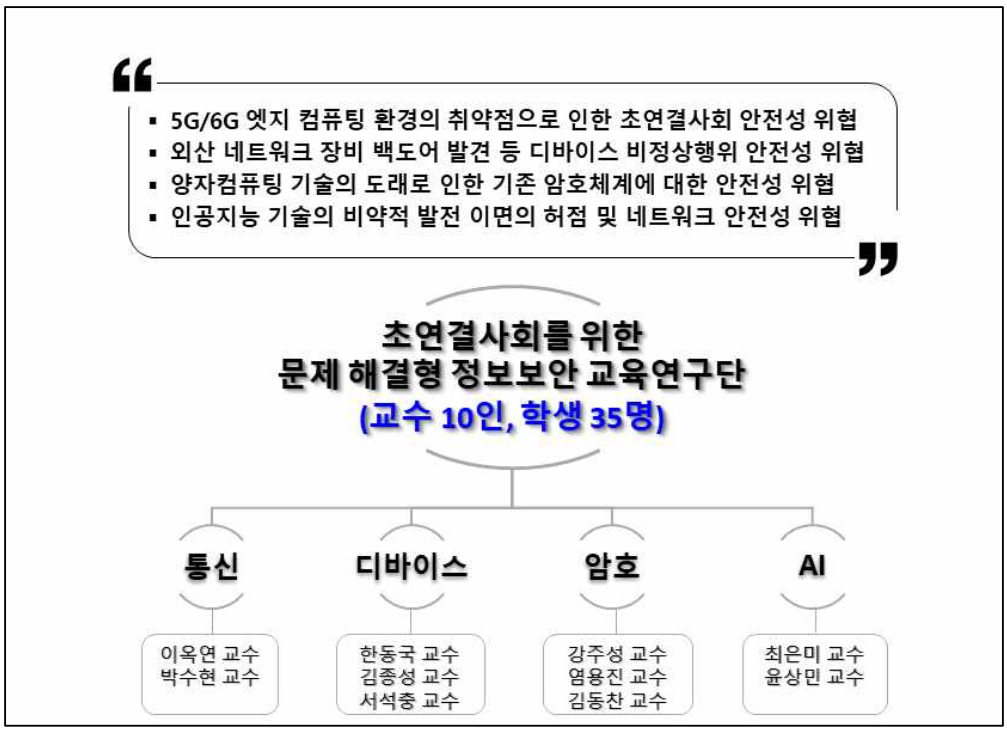
- 미래에는 국민생활과 사회 전반에 걸쳐 이동통신과 AI에 대한 의존도가 커질 것이고, 이에 따른 정보보안 관련 위협은 사회적 안정과 국가 안위에 직결된 문제가 될 것이므로 정보보안 전문 인력 양성을 본 학과의 주요 목표로 정함
- 최근 들어, 5G와 6G 이동통신 사회의 등장으로 정보보안 위협이 고도화됨에 따라 대응기술과 관련 제도도 복잡성이 증가하고 있어, 사회의 정보자산 보호를 위해서는 보안 전문가의 역할이 필수적이며, 따라서 전문지식을 갖춘 CISO와 보안 컨설턴트 등의 정보보안 전문가의 중요성이 부각되고 있음
- AI보안, 드론, 자율이동체, 위성 등의 다양한 통신환경의 등장으로 초연결사회로 급속히 변화하고 있어, 초고속, 초신뢰 환경 변화에 대응할 수 있는 정보보안 전문가의 중요성은 지속적으로 증대될 것이 예상되므로 해당 분야의 전공 교수진으로 본 교육연구단을 구성함
- 본 교육연구단의 정보보안 협동과정은 정보보안 핵심 기술을 기반 지식으로 하고, 시대적 흐름에 부합하는 사회문제 해결형 관련 지식을 보유하게 하는 융합형 전문 교육과정이 될 것이므로, 질적인 면과 양적인 면 모두에서 지속적인 성장이 이루어질 것으로 확신함

▶ 교육관점에서 본 교육연구단의 특징

- 정보보안은 특성상 컴퓨터공학 및 암호 전공자의 융합 학문분야이며, 어느 한쪽의 전공지식만으로는 정보보안 위협을 이해하거나 대응할 수 없음
- 본 교육연구단은 정보보안전공 교수 7인과 컴퓨터공학 전공 교수 3인의 교수들로 구성되었으며, 중견교수 및 신진교수의 구성 비율이 적정하여, 경험과 도전정신을 모두 갖춘 구성임
- 또한, 단순 강의가 아닌 다양한 외부과제 및 정보보안 사례 기반 교육, 프로젝트 기반 교육 등 다

양한 교육방법을 통해 교육하며, 강의평가가 매우 우수함

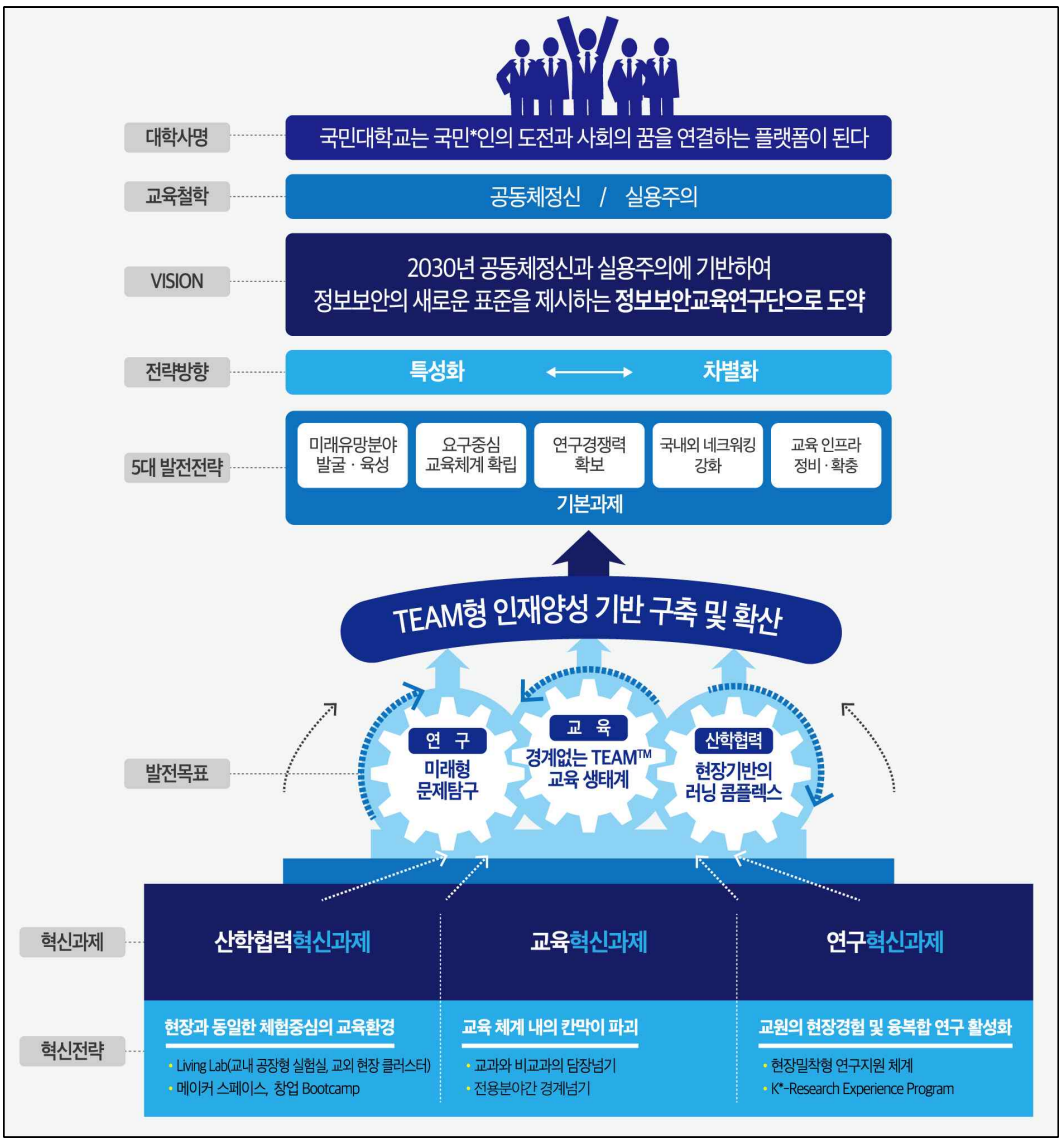
- 본 교육연구단을 구성하고 있는 교수진은 미래 초연결사회에 필수적으로 요구되는 AI 보안, 무선통신 보안, 이동통신 보안, 국가용 암호모듈 검증, 암호설계 및 분석, 디바이스 보안 등 5G/6G 초연결시대에 필수적인 다양한 정보보안 전공경험과 실무 경험을 모두 갖추고 있음



- 본 사업단의 참여대학원생들의 취업 진로는 국내 진로 희망 최상위층의 국가 기관, 정부출연연구소 및 민간 정보보안 관련 회사들로, 양적뿐만 아니라 질적으로도 우수한 성과를 내고 있음
- [국가기관/정부출연연구소] 국가 관련 기관(2014년 2월 장OO, 2015년 2월 석사 박OO, 2015년 8월 석사 주OO, 2017년 2월 박사 김OO, 황OO, 안OO, 2019년 2월 박사 유OO, 2019년 2월 석사 김OO, 석사 송OO), 군 관련 기관 (2019년 2월 박사 박OO), 한국인터넷진흥원(2017년 2월 석사 김OO), 한국기계전기전자시험연구원(2016년 2월 석사 김OO), 한국과학기술정보연구원(2016년 2월 석사 박OO), 한국전자통신연구원 (2014년 2월 석사 이OO) 등
- [정보보안기업] 삼성전자(2018년 2월 박사 원OO), LG CNS (2016년 8월 석사 윤OO), 이니텍 (2018년 2월 석사 강OO), 펜타시큐리티 (2018년 2월 석사 배OO), 드림시큐리티 (2019년 2월 석사 김OO), 코나아이 (2014년 2월 석사 최OO), 한국시스템보증 (2018년 2월 석사 이OO, 2019년 2월 석사 김OO), 유비벨록스 (2015년 2월 석사 김OO), 세이퍼존 (2015년 2월 석사 이OO), 윈스 (2015년 8월 석사 김OO), NSHC (2019년 2월 석사 함OO) 등
- [일반기업] 김앤장 법률사무소 (2018년 2월 석사 홍OO, 2019년 2월 석사 강OO), 행복마루컨설팅(2017년 2월 석사 신OO), 넥스트리컨설팅 (2019년 2월 박사 함OOO OOOO), 아이콘루프 (2018년 2월 석사 유OO) 등

▶ **연구관점에서 본 교육연구단의 특징**

- 클라우드 컴퓨팅 서비스에서 대용량 암호화 정보 고속 설계 기술을 보유하고 있는 전문가 양성을 통해 추후 국가 및 공공기관과도 협력하여 국가 공공기관 전용 클라우드 서비스를 개발하여 보안 위협에 안전하면서도 고속화된 대용량 암호화 클라우드 서비스를 제공하려는 연구를 진행 중임
- 세계적인 포렌식 업체와 함께 협력하여 본 교육연구단에서의 교육 및 연구를 통해 개발한 분석기술을 상용화하여 포렌식 수사에 기여하고 있으며, 포렌식 분석적 시장을 선도하는 기술을 보유함
- 우리가 주로 사용하는 카카오톡이나 한글과컴퓨터와 같은 프로그램의 경우 세계적인 포렌식 업체에서도 그 분석을 지원하지 않는 실정이고, 신규 기기나 새로운 프로그램에 대한 분석, FBE/FDE, iOS와 같은 환경에서의 데이터 분석은 세계적인 포렌식 분석도구 개발 업체에서도 불가능한 경우가 많으나 본 교육연구단은 해당 분야의 연구실적을 보유하고 있으며, 관련 전문인력을 양성하고 있음



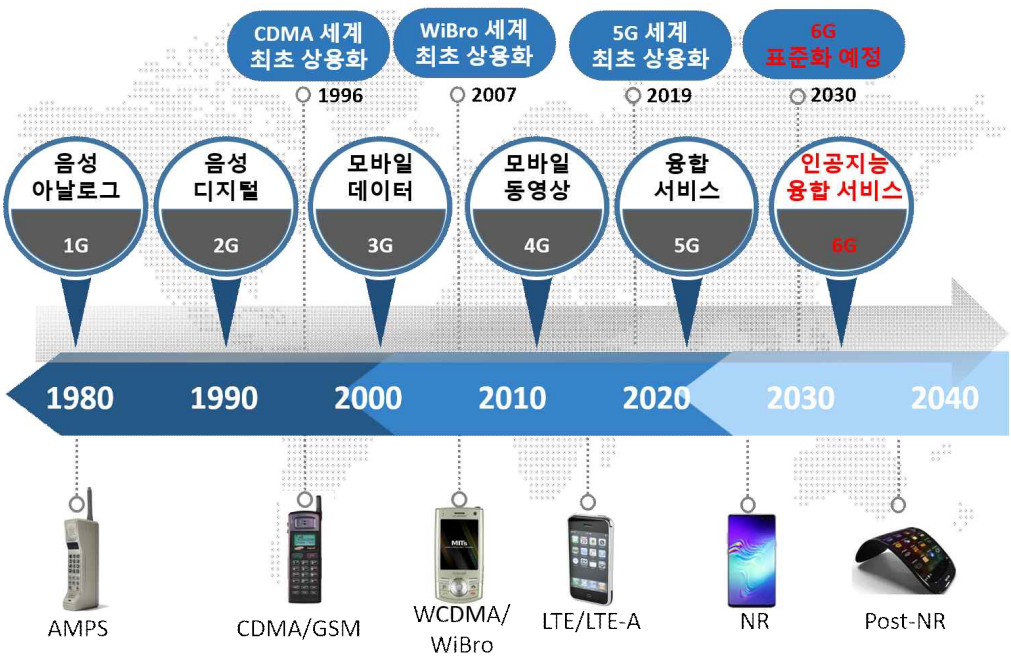
- 동형 암호에 대한 디바이스 고속 설계 기술을 보유한 전문인력이 양성되면 관련 업체와의 상호 업무 협약을 통해 개발한 디바이스를 실사용할 수 있도록 할 것이며, 업체 및 연구소와의 지속적인 협약 관계를 통해 지식을 공유하고 피드백을 관리함으로써 지속 가능한 발전이 가능한 체계를 구축할 예정임
- 사회망 정보보안 분야의 인재 양성을 통해 국가기반시설, 국가보안목표시설(국가정보원), 국가중요시설(국방부, 경찰청) 등으로의 전문인력을 배출하고 있음
- 본 연구단은 부채널 정보 기반 디바이스 역공학 기술을 연구하고, 이를 국산화하여 자국의 산업을 보호할 뿐만 아니라 해외 기술 종속 관계에서 벗어나 해외 시장에 기술을 수출하여 시장을 선도할 수 있는 기술과 역량을 갖춘 전문인력을 배출하고 있음

▣ 교육연구단의 교육목표

▶ 최종목표 : 미래통신 / 디바이스 / 암호 / AI 분야의 정보보안 문제 해결형 융합 교육의 실현 및 전문인력 양성

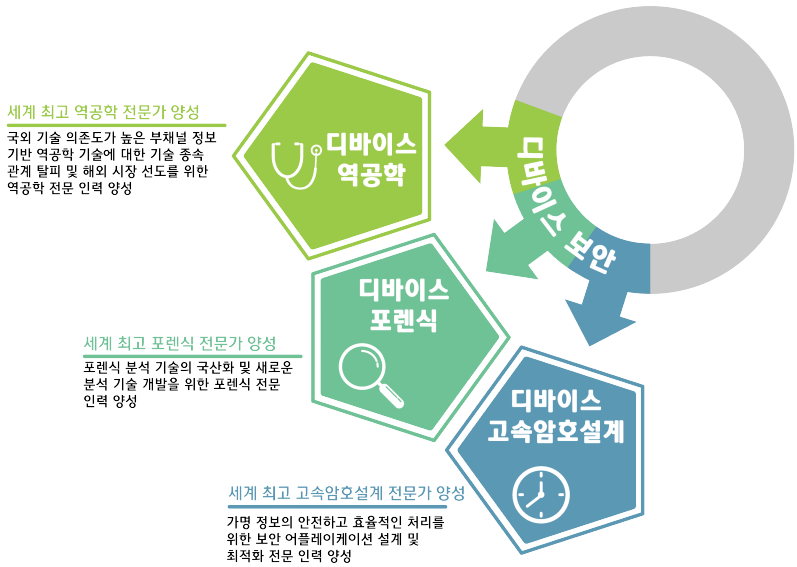
▶ 미래통신 정보보안 전문인력 양성

- 5G, 6G, IoT 기반의 지상망을 중심으로 위성, 수상통신, 수중통신에 이르는 공간통신의 모든 연결성 완성을 목표로 진행되는 초성능, 초대역, 초공간, 초정밀, 초지능, 초경험 시대의 초신뢰 정보보안 전문인력 양성을 목표로 함
- ICT 환경의 지속적인 발전에 따라 미래의 IoT의 중심망이 될 이동통신망(5G/6G)과 위성통신 및 수중통신의 정보보안 문제를 해결 가능한 전문인력 양성을 목표로 함
- 미래산업 및 사회의 변화는 기하급수적인 데이터 사용량의 증가와 함께 데이터 대용량의 처리가 가능한 6G 네트워크의 등장에 맞는 새로운 통신환경을 선도할 정보보안 전문인력 양성이 목표임
- 본 교육연구단에서는 5G / 6G와 IoT를 수상통신, 위성통신, 수중통신 3차원 공간의 통신환경을 모두 통합 분석능력을 갖춘 정보보안 전문가 양성을 목표로 함



▶ **안전한 초연결사회를 위한 디바이스 보안 전문인력 양성**

- 본 교육연구단은 안전한 초연결사회 구축에 필수적인 디바이스 보안 관련 부채널 분석, 디지털 포렌식, 고속구현 전문가를 양성함
- IT 환경의 소재/부품/장비를 구성하는 정보보안 제품에 대한 부채널 정보 기반 디바이스 역공학 지식 및 기술을 함양한 인재 양성 및 국내 산업 활성화에 기여함
- 부채널 정보 수집 기술, 분석 성능 향상을 위한 부채널 신호 처리 기술, 부채널 신호에 내재되어 있는 유의미한 정보 추출 기술 교육을 통한 전문인력을 양성함
- 국내외 시중에서 사용되고 있는 부채널 안전성 검증 시스템을 개선하고, 이를 활용하여 효율적인 디바이스 이상행위 탐지 기술 연구수행 및 관련 전문가를 양성함
- 날이 갈수록 다양해지는 디지털 기기의 방대한 데이터로부터 정확한 증거를 수집하여 객관적으로 증명가능한 법정 제출용 디지털 증거를 수집 및 분석하는 디지털 포렌식(Digital Forensics) 전문역량을 갖춘 디지털 포렌식 수사 전문인력을 양성함
- 디지털 범죄수사 등을 위한 디지털 증거를 법정에 제출하기 위해 밟아야만 하는 정확한 원칙 및 절차를 교육하여 올바른 포렌식 수사 방법을 학습할 수 있게 구성함
- 다양한 디바이스가 가지는 각각의 특징 및 데이터에 대한 기본적인 이해를 돕기 위해 OS, 메모리, 저장공간 등의 전반적인 컴퓨터 이론을 교육함
- 이스라엘 Cellebrite사의 UFED, 미국 Opentext의 EnCase, 국내 한컴위드의 MD-NEXT, MD-RED 등의 상용 포렌식 분석 도구의 증거 수집 및 분석방법을 교육함
- 상용 분석도구로 분석이 불가능한 신규 기기나 새로운 프로그램에서 얻을 수 있는 데이터 분석 방법을 연구 교육함



- 이에 본 교육연구단은 고속 암호 설계 기술을 적용하는 동형 암호, 클라우드 서비스, 양자내성 암호 등으로 나누고, 디바이스 고속 암호 설계 지식 및 기술을 함양한 인재를 양성하고자 함
- 디바이스 보안 문제에 대한 지속적인 관심과 연구가 요구됨에 따라 디바이스 동작 성능에 큰 영향을 끼치는 디바이스 고속화 설계 기술이 핵심이며, 특히 첨단 산업 시대에 대용량 데이터를 활용한 디바이스 및 서비스들이 개발되면서 그에 맞는 정보보안 전문가 양성이

필수적임

- 동형 암호는 암호문을 복호화하지 않고도 계산할 수 있도록 해주는 암호화 방식이며, 암호화된 데이터들을 이용하여 계산한 결과를 복호화하면 암호화 해주지 않은 상태로 계산한 값과 일치하는 장점 존재함
- 본 연구단은 동형 암호 디바이스 고속 설계 기술 교육을 통하여 데이터 3법 하의 사용자 가명 정보를 안전하고 효율적으로 처리할 수 있는 다양한 보안 어플리케이션을 설계하고 최적화할 수 있는 전문인력을 양성하는 것이 목표임
- 동형 암호를 교육하기 위해서는 많은 교과목의 이해가 필수적이므로, 현대대수학 등 동형 암호의 수학적인 원리에 대한 선수 과목과 양자내성 암호에서도 다루어지는 Lattice 기반 동형 암호 등의 보안 방식에 대한 원리 또한 학습되어야 함
- 동형 암호를 학습할 때에는 암호에 대한 소프트웨어 및 하드웨어 상에서의 고속화 설계 및 최적화 구현을 시도할 수 있도록 다양한 예제를 동원하고 구현을 위해 필요한 환경의 이해와 FPGA 구조 및 개발 언어에 대한 교육 또한 실시할 예정임
- IBM이나 MS에서 개발된 동형 암호 구현물을 벤치마킹하여 연구하거나 해당 기술을 분석하여 개발에 활용할 수 있도록 함
- IaaS, PaaS, SaaS 각각에 대한 특징과 각 서비스에 대한 네트워크 선행 교육을 실시하고 이후 클라우드 컴퓨팅 환경에서의 다양한 데이터 접근, 전송, 암호화 과정 등의 정보보안을 교육함

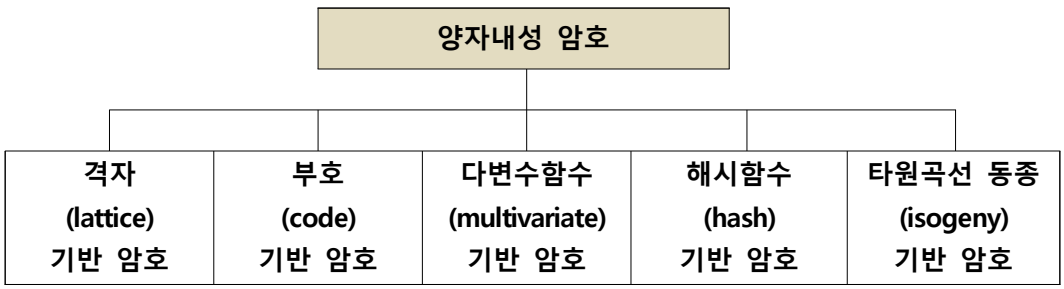
▶양자내성 암호 정보보안 전문인력 양성

- 본 교육연구단은 미래 정보통신 환경의 가장 큰 변화가 될 것으로 예상되는 양자내성 암호 전문인력 양성을 목표로 함
- 오늘날 ICT 인프라 보호를 위해 사용하는 DH 키공유 암호(1976년), RSA 암호(1977년), 타원곡선 암호(1985년)는 수학적 난제로 분류되는 인수분해 문제와 이산대수 문제를 기반으로 설계된 암호임

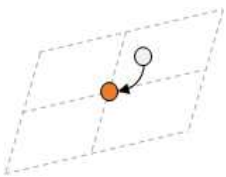
인수분해 문제 **(Integer Factorization Problem)**	**이산대수 문제** **(Discrete Logarithm Problem)**
두 소수 p와 q의 곱 $N=pq$이 주어졌을 때, 소수 p와 q를 찾는 문제	어느 군(group) $(G,*)$ 의 원소 $g\in G$와 정수 $n\in Z$에 대해 $h=\underbrace{g*g*\cdots*g}_{n}$가 주어졌을 때, n를 찾는 문제

- 이 암호들의 안전성 수준(security level)은 기반 문제의 해법 알고리즘 계산복잡도에 의해 결정되는데, 1994년 Peter Shor가 인수분해/이산대수 문제는 양자의 성질을 이용하면 다항식 시간 내에 풀 수 있음을 증명함
- DH 키공유 암호, RSA 암호, 타원곡선 암호는 네트워크 상의 사용자 및 기기 인증, 공인인증서 등에 사용하는 가장 핵심 인증 기술임
- 따라서 실용적 수준의 양자컴퓨터가 개발되면 현재 사용하는 모든 암호 체계가 되는 안전성을 보장하지 못하기 때문에, 공격자에게 무방비로 노출되는 상황이 발생함

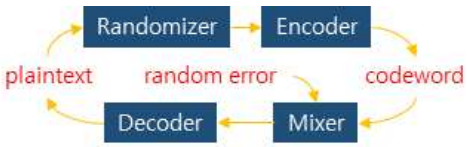
- Peter Shor의 논문이 발표되었을 때 학계에서는 양자 컴퓨팅의 실현성에 의구심을 가졌으나, 2010년 이후부터 양자 컴퓨팅의 괄목할만한 결과들이 소개되면서 학계의 지대한 관심을 받고 있으며, 2020년 현재는 양자 컴퓨팅 환경에서도 안전한 양자내성 암호 연구와 전문인력 양성이 가장 큰 연구주제가 되고 있음
- 미래 경제적 가치 선점을 위해 Google, IBM, MS 등에서 양자컴퓨터 개발을 위한 구성요소(양자 프로그래밍 환경, 양자 컴파일러, 큐비트 칩 등) 전반에 대한 공격적인 연구개발 투자를 진행하고 있음
- 2018년 D-wave는 무료 양자컴퓨터 클라우드 Leap을 출시하였고, CES 2019에서는 IBM이 Q 시스템을 이용하여 개발한 20큐빗의 양자 컴퓨터를 소개하였음
- 암호 학계는 실용적 양자컴퓨터 시대를 대비하기 위해 양자내성 암호(Quantum Safe Cryptography)라는 이름의 새로운 방식의 암호 알고리즘 연구에 많은 집중하기 시작함
- 2016년부터 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)가 주관하여 국제 양자내성 암호 표준 알고리즘 공모전이 진행 중이며, 2021년에 알고리즘을 선정한 후 2024년에 표준으로 제정할 예정임
- 양자내성 암호 기반 암호 체계의 조기 확보는 단기적으로는 보안방법 전환 비용을 감소시키며, 장기적으로는 국내 ICT 인프라 보안체계의 국외 의존도를 낮출 수 있음
- 양자내성 암호는 기반 문제에 따라 다음의 5개로 분류됨



- 2라운드 후보 알고리즘은 총 26종이며, 이중 격자 기반 암호와 부호 기반 암호가 NIST 주관 양자내성 암호 표준 알고리즘 공모전 2라운드에 각각 12종, 7종이 선정되어 유력한 표준 알고리즘으로 평가받고 있음
- 미숙한 암호의 구현과 사용은 암호의 기대 안전성 저하를 초래하므로, 현재 대부분의 표준 알고리즘은 구조가 복잡하여 구현 난이도가 매우 높고, 파라미터 설정 등 사용 방법 또한 매우 다양하기 때문에, 알고리즘 관련 지식을 습득하는 데 오랜 시간이 필요함



격자 기반 암호



부호 기반 암호

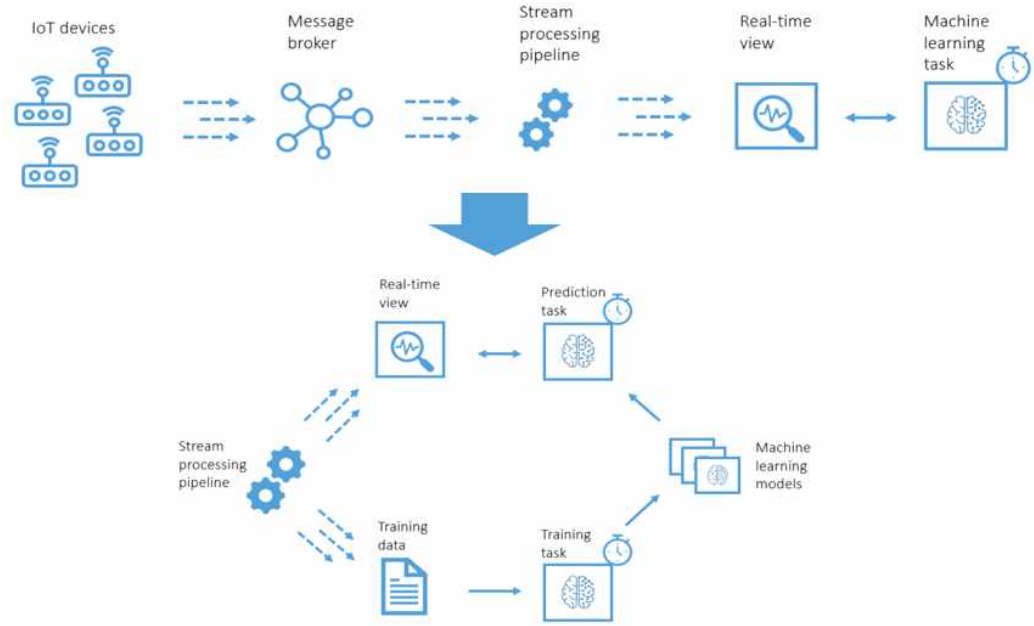
- 따라서, 기존 ICT 인프라의 보안체계를 양자컴퓨터에서도 안전한 양자내성 암호 기반으로

교체를 하기 위해서는 장기간의 전문인력 양성 프로그램이 필요함

- 이 양성 프로그램은 기존 보안체계에 대한 깊은 이해와 문제점들의 명확한 파악이 반드시 선행되어야 하며, 최근 제안되는 다양한 보안공격 기법들을 항상 예의주시하면서 미래암호의 방향성에 대해 제시할 수 있는 전문인력 양성을 목표로 함
- 본 교육연구단은 지난 7년간 체계적인 교육과정과 철저한 학사관리를 통해 수준 높은 보안 전문인력을 지속해서 양성했음
- 본 교육연구단은 기존 교육과정을 유력한 표준 양자내성 암호(격자 기반 암호, 부호 기반 암호) 중심으로 개편하고, 2024년 표준 제정에 맞춰 산업계와의 연계성을 최우선으로 한 교육 진행 방식으로 해당분야의 전문인력 교육과 연구를 진행할 계획임

▶자율 성장 AI 보안 기술을 활용한 지능형 시스템 기술 전문가 양성

- 다양한 IoT 및 관련 엑세스 네트워크 환경에서의 데이터 수집, 분석을 통하여 스스로 학습하고, 이해하고, 취약점에 대한 공격에 대한 방어 체계를 수립하고 교육할 계획임
- 다양한 사회 안전망에서의 시스템 신뢰성 보장 모델 개발 역량을 갖춘 AI 정보보안 전문가를 양성함
- 다양한 시스템 환경에서 지속적으로 생산되는 데이터를 기반으로 스스로 학습하고 성장하는 AI 모델을 정립함으로써 수많은 사람과 기기, 기기와 기기 간에 발생할 수 있는 보안 문제 해결을 목표로 함
- IoT 시스템의 활용을 시스템 구성을 위한 연구를 통하여 국제적 경쟁력을 갖춘 연구 수행 및 교육기관들과의 협력 연구를 목표로 함
- IoT 기술과 관련된 통신 시스템, 대용량 데이터 기반 AI 기술, 적대적 공격 및 방어와 관련된 교육 체계를 수립하고 이에 대한 프로젝트 기반 수업을 통하여 학생들이 실제 사회에서 발생할 수 있는 문제를 해결할 수 있는 능력을 배양할 수 있도록 교육함



Ⅰ. 교육연구단 구성, 비전 및 목표

1. 교육연구단 구성

1.1 교육연구단장의 교육연구행정 역량

성 명	한글	이옥연	영문	Yi, Okyeon
소 속 기 관	국민대학교	과학기술대학	정보보안암호수학과	

<표 1-1> 교육연구단장 최근 5년간 연구실적

연번	저자/수상자/발명자/창업자	논문제목/저서제목/book chapter 제목	저널명/출판사명	권(호), 페이지/ISSN/ISBN (pp. ** - **)	게재/출판	DOI 번호 (해당 시)
1	저자	Cryptanalysis of hash functions based on blockciphers suitable for IoT service platform security	Multimedia Tools and Application/Springer	78, 3107-3130/1380-7501	게재	10.1007/s11042-018-5630-4
2	저자	Proposal of Piecewise Key Management Design Considering Capability of Underwater Communication nodes	Journal of Computational and Theoretical Nanoscience	23(12), 12729-12733	게재	10.1166/asl.2017.10888
3	저자	Suggestion SSL-VPN for Traffic Signal Control System	Journal of Computational and Theoretical Nanoscience	23(12), 12725-12728	게재	10.1166/asl.2017.10887
4	저자	Encryption scheme in portable electric vehicle charging infrastructure:Encryption scheme using symmetric key	cInternational Conference on Computer Applications and	Publisher : IEEE, INSPEC Accession Number : 17650166	게재	10.1109/CAIPT.2017.8320674
5	저자	Analysis of Radio based Train Control System using LTE-R and Analysis of Security Requirements	International Conference on Computer Applications and	Publisher : IEEE, INSPEC Accession Number : 17650175	게재	10.1109/CAIPT.2017.8320741

1.3 교육연구단의 구성

① 교육연구단장의 교육·연구·행정 역량

▣ 산업・사회 문제 해결분야 관련 교육연구단장의 연구・교육・행정 역량

▶국내 정보보안 및 암호산업 발전에 기여

- 2007년부터 현재까지 대검찰청의 디지털수사 자문위원으로 디지털 포렌식 분야의 기술력 연구 및 관련 기술확보에 기여함
- 2013년부터 한국암호포럼의 안전성평가분과위원장과 정책분과위원장을 역임하며, 정보보안의 핵심 원천기술인 암호모듈 시험기술 개발 및 표준화에 기여함
- 2014년부터 현재까지 미래창조과학부 정보통신망 침해사고 사이버보안전문단원으로 활동하며, 국내 사이버보안의 첨병으로 기여함
- 2016년부터 한국정보화진흥원(NIA)와 교통신호제어시스템용 무선모뎀용 정보보안 표준규격서를 개발을 성공하여, 2017년 4월 경찰청의 교통신호제어기용 표준규격서 (NPA-TSC-STANDARD-2018-04-30(2010R16) 제정에 기여함
- 과학기술정보통신부의 5G 보안협의회 위원으로 5G 보안기술 및 상용화 방안 수립에 기여하고 있음

▶국내 정보보안 및 암호관련 사회문제 해결에 기여

- 교육연구단장은 IoT, 스마트미터 등 6G에 포함될 수 있는 다양한 환경에서 보안 서비스 개발을 위한 다수의 암호 및 보안 라이브러리 기술 및 개발, KCMVP 검증 실적, 상용화 실적을 보유하고 있음
- 이러한 기술을 바탕으로 한국전력공사 전력연구원과 공동으로 2016년 3월과 2017년 11월에 스마트그리드용 검증필암호모듈(CM-112-2021.03, CM-132-2022.11) 개발에 성공하여, 2016년 2,500억 규모의 200만 가구 및 2017년 3,000억원 규모의 300만 가구용 지능형전략망의 AMI 보급사업이 재개될 수 있었으며, 관련된 국내 정보보안 산업 및 전력산업에서의 정보보안 문제 해결에 기여함
- 다양한 무선 IoT 디바이스용 암호/인증 라이브러리 상용화
  - CCTV, IoT Wi-Fi, LTE, TVWS 등의 IoT 통신 환경용 암호/인증 라이브러리 상용화
  - 스마트 그리드용 경량 암호/인증 알고리즘 상용화

▶공공시설용 이동 영상감시의 무선 데이터 기밀성 보장 WiFi 장비 개발 및 상용화

- 군 훈련장용 영상/센서정보 실시간 무선 WiFi 보안장비 개발 및 상용화
- 군 주요시설 온도, 습도 및 영상 데이터 기밀성 보장 WiFi 장비 개발 및 상용화
- 시내버스 탑재 카메라를 통한 주정차위반 단속영상용 LTE 장비 개발 및 상용화
- 정수장/가압장용 감시영상/관측 데이터 전송을 위한 유선 장비 개발 및 상용화
- 모바일 전기차 충전기용 데이터 전송을 위한 3G/LTE 보안장비 개발 및 상용화
- 교통신호제어기용 LTE 기반 SSL VPN 보안 표준과 호환성 장비 개발과 상용화
- 스마트시티 및 방범용 CCTV 일체형 SSL VPN(CC인증) 장비 개발 성공 및 상용화

▶국내 정보보안 전문인력양성에 기여

- 2013년 9월부터 현재까지 BK21+ 미래금융정보보안전문인력양성사업단장을 역임하며, 금융보안, IoT 보안, 산업제어 보안 인력양성에 기여함
- 한국암호포럼이 주최하고, 국가정보원, 미래창조과학부가 후원하는 '2013년, 2014년, 2015년 국가암호공모전 심사위원장'을 맡아 암호기술 발전에 기여함
- 한국암호포럼이 주최하고, 국가정보원, 미래창조과학부가 후원하는 '2014년 LEA암호구현공모전', '2015년 LSH 암호구현공모전' 심사위원장을 맡아 암호기술 발전에 기여함

② 대학원 신청학과 소속 전체 교수 및 참여연구진

<표 1-2> 교육연구단 신청학과 소속 참여교수 현황

기준일	신청 학과	전체 교수 수			참여교수 수						
					기존교수 수			신임교수 수			총계
		전임	겸임	계	전임	겸임	계	전임	겸임	계	
2020. 05.14	금융정보보안학과	0	12	12	0	9	9	0	1	1	10

③ 교육연구단 구성의 적절성

<표 1-3> 참여교수진의 해당 산업·사회 문제 해결분야 교육 실적 및 연구 분야

연번	성명 (한글/영문)	직급	연구자등록번호	소속 대학 및 신청학과	세부전공분야	산업·사회 문제 해결분야 관련 대학원 교과목 개설 실적
	산업·사회 문제 해결 관련 연구분야와의 연계성					
1	이옥연	교수	10056884	국민대학교 금융정보보안학과	유무선통신보안	정보보안시스템 평가방법론(2019년 2학기)
	IT 제품 및 시스템의 보안성 평가방법론을 교육함					
2	이옥연	교수	10056884	국민대학교 금융정보보안학과	유무선통신보안	이동통신 보안(2018년 2학기)
	3G, 4G 및 5G 이동통신의 인증 및 키 일치 구조를 교육함					
3	강주성	교수	10127144	국민대학교 금융정보보안학과	확률과정론	난수성분석론(2019년 2학기)
	정보보안 시스템의 난수발생기 설계 및 안전성 분석 관련 내용을 교육함					
4	강주성	교수	10127144	국민대학교 금융정보보안학과	확률과정론	정보보안프로토콜(2019년 1학기)
	정보보안 관련 프로토콜 안전성과 효율성 분석 기술을 교육함					

연번	성명 (한글/영문)	직급	연구자등록번호	소속 대학 및 신청학과	세부전공분야	산업·사회 문제 해결분야 관련 대학원 교과목 개설 실적
	산업·사회 문제 해결 관련 연구분야와의 연계성					
5	김동찬	부교수	11579260	국민대학교 금융정보보안학과	암호론	보안구현개발방법론(2018년 2학기)
	양자내성암호 중 하나인 부호기반 암호를 교육함					
6	김동찬	부교수	11579260	국민대학교 금융정보보안학과	암호론	공개키암호분석이론(2019년 2학기)
	타원곡선암호와 양자내성암호 후보군 중 하나인 격자기반암호를 교육함					
7	김종성	부교수	10182694	국민대학교 금융정보보안학과	정보보호	디지털포렌식개론(2018년 2학기)
	디지털 포렌식 수사 증거분석 도구 사용법 및 증거분석 기술을 교육함					
8	김종성	부교수	10182694	국민대학교 금융정보보안학과	정보보호	디지털포렌식특수연구 (2019년 1학기)
	디지털 포렌식증거 데이터를 해석하는 방법을 교육함					

연번	성명 (한글/영문)	직급	연구자등록번호	소속 대학 및 신청학과	세부전공분야	산업·사회 문제 해결분야 관련 대학원 교과목 개설 실적
	산업·사회 문제 해결 관련 연구분야와의 연계성					
9	박수현	교수	10056675	국민대학교 금융정보보안학과	컴퓨터학	고급정보통신론(2017년 1학기)
	네트워킹 및 통신 원리에 근거한 p2p 패러다임 변화에 대해 교육함					
10	박수현	교수	10056675	국민대학교 금융정보보안학과	컴퓨터학	실시간시스템(2018년 2학기)
	실시간 시스템 이해기반 임베디드 시스템 설계 및 구현에 대해 교육함					
11	서석충	조교수	10875717	국민대학교 금융정보보안학과	컴퓨터보안	암호소프트웨어구현(2019년 2학기)
	타원곡선 기반 암호를 임베디드 및 GPU 환경에서의 최적화 구현 방법을 교육함					
12	염용진	교수	10090653	국민대학교 금융정보보안학과	해석학	융합보안특강(2019년 1학기)
	암호 및 보안기술을 바탕으로 산업에 응용할 수 있는 기술을 교육함					

연번	성명 (한글/영문)	직급	연구자등록번호	소속 대학 및 신청학과	세부전공분야	산업·사회 문제 해결분야 관련 대학원 교과목 개설 실적
	산업·사회 문제 해결 관련 연구분야와의 연계성					
13	염용진	교수	10090653	국민대학교 금융정보보안학과	해석학	정보보안컨설팅(2017년 1학기)
	정보보안 관련 표준 및 제도를 바탕으로 정보보안 컨설턴트를 위한 지식을 확보함					
14	최은미	교수	10116354	국민대학교 금융정보보안학과	컴퓨터학	클라우드컴퓨팅(2016년 1학기)
	클라우드 컴퓨팅과 활용을 통해 초연결시대의 시스템 인프라 기술을 교육함					
15	한동국	교수	10128486	국민대학교 금융정보보안학과	암호론	디바이스공격론(2017년 2학기)
	디바이스(금융IC카드, USIM 등)에 대한 적용 가능한 부채널 공격방법을 교육함					
16	한동국	교수	10128486	국민대학교 금융정보보안학과	암호론	디바이스공격대응론(2018년 2학기)
	디바이스(금융IC카드, USIM 등)를 보호하기 위한 대응기법을 교육함					

1.3 교육연구단의 구성

③ 교육연구단 구성의 적절성

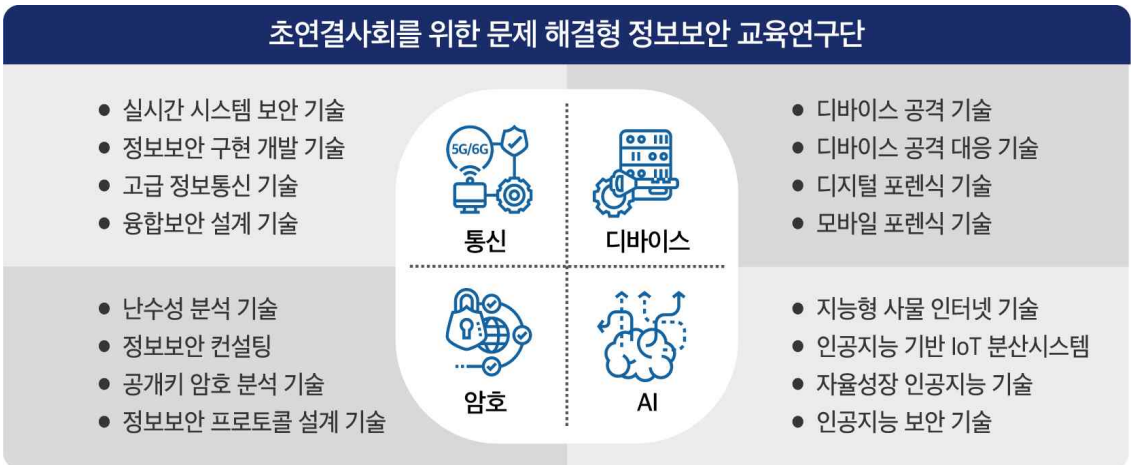
1. 안전한 초연결사회를 위한 문제해결형 정보보안 교육 연구단 배경 및 타당성

▣ 배경

- 5G와 6G, 그리고 인공지능의 등장으로 다양한 형태의 디바이스 장치가 인터넷에 연결되어 동작하는 자동화 초연결사회로 도약하고 있음
- 이에 따라 분리된 영역에서 독자적으로 발생하던 정보보안 위협이 더욱 고도화되어, 연결된 모든 장치와 네트워크에도 심각한 영향을 미치는 수준에 이르고 있음
- 초연결사회에서 발생하는 다양한 보안사고와 문제를 해결하기 위해서는 초연결사회의 근간 기술을 이루고 있는 통신, 디바이스, 암호, 인공지능에 대한 융합적인 이해와 기술력을 보유한 정보보안 전문인력 양성이 필수적임

▣ 타당성

- 본 교육단에 소속된 10인의 교수는 안전한 초연결사회에 필수적으로 요구되는 5G/6G 통신 분야, 디바이스 보안 분야, 암호 분야, 인공지능 분야 등에 전문성을 보유함
- 소속된 10인의 교수는 전문지식을 바탕으로 단순 전달식 강의가 아닌 다양한 외부과제 및 정보보안 사례기반 교육, 실습 위주의 실사구시 교육을 통하여 다양한 산업·사회 문제 해결이 가능한 정보보안 전문인력을 양성해오고 있으며 양성된 인력은 보안전문기업, 국가연구소, 국가기관 등 다양한 분야로 진출하여 중추적 역할을 수행하고 있음
- 기존에 수행한 다양한 전공수업을 바탕으로 향후 초연결사회의 정보보안 문제 해결을 위한 교과목을 확장하여 추가할 계획이며 이는 암호, 정보보안, 하드웨어, 통신, 인공지능 등을 아우르는 융합교육의 형태가 될 것임
- 수학, 컴퓨터, 보안 등의 전공 경계를 허물고 융합전공 참여교수진 및 대학원생으로 구성된 교육연구단은 초연결사회에서의 보안 문제를 다각적인 시각으로 분석하여 최적의 솔루션을 제시할 수 있는 마중물 역할을 할 것으로 기대됨
- 다가올 5G/6G 기반 초연결사회 산업에 적용하기 위한 관련 지식을 깊이 있게 연마하고, 연구 또한 성공적으로 수행한 경험이 있는 참여교수진으로부터 학습 및 지도받을 수 있는 전문화된 교과과정 제공은 미래융합형 혁신인재 양성을 위한 초석이 될 것임



2. 참여교수진 구성의 적절성

▣ 안전한 초연결사회를 위한 5G/6G 이동통신 분야 (이옥연 교수, 박수현 교수)

▶실시간 시스템 보안 기술

- 사물인터넷(IoT)을 위한 실시간 시스템에 대한 이해와 RTOS (Real-Time Operating System) 기반의 임베디드 시스템 설계 및 구현 능력을 함양하기 위해 기본 개념과 모델을 분석하고 평가기술 등을 연구하고 교육함
- IoT, 어플리케이션, 프레임워크, 프로토콜, 데이터 통신 및 네트워크 아키텍처의 기본 개념에 대해 교육함
- 더 나아가 실제로 IoT 관리 분야에 어떻게 실시간 개념을 적용할 것인지에 대하여 사례를 통한 학습을 진행하므로 초연결사회가 도래함에 따라 야기되는 산업적/사회적 문제에 대하여 실시간으로 해결할 수 있는 능력을 향상시킴

▶정보보안 구현 개발 기술

- 양자내성암호 안전성 이론 및 구현 방법론 수업으로 양자내성암호 후보군 중 하나인 부호기반암호 Classical McEliece 암호체계에 대해 교육함
- Classical McEliece 암호체계는 현재 NIST 표준 양자내성암호 2라운드 후보로서 표준으로 채택될 가능성이 높으며, 해당 암호시스템에 사용되는 오류정정부호인 이진 Goppa 부호의 성질과 생성 방법, Patterson 디코딩 알고리즘에 대한 지식을 전달함
- 본 교과목을 통하여 양자내성암호를 실제 구현하고 운영할 수 있는 전문가를 양성함

▶고급 정보통신 기술

- 차세대 인터넷 환경으로 초연결 네트워크를 기반으로 사물인터넷(IoT) 네트워크 및 컴퓨팅의 핵심기술인 상황인지(context-awareness) 및 위치인식(localization)에 대해 연구함
- 이론적 기초를 토대로 underwater와 같은 차세대 네트워크 도메인까지 확장된 정보통신 관련 기술의 세부지식을 제공하므로 산업 경쟁력 제고 및 성장동력으로 확장함

▶융합보안 설계 기술

- ICT와 산업과 연계된 암호・보안기술에 대한 기반 이론부터 응용까지 체계적인 지식을 제공함
- 개설되는 시기에 따라 특화된 분야를 선정하고 해당 분야의 기술적 배경부터 응용까지 이해할 할 수 있는 학문적, 기술적 기반을 학습함
- 암호의 역기능에 대한 내용을 중심으로 랜섬웨어와 백도어에 활용되는 암호기술과 대응방안을 다루었으며 이를 바탕으로 참여 대학원생들이 관련 연구과제를 훌륭히 수행할 수 있는 토대를 구축하였음

▣ 안전한 초연결사회를 위한 디바이스 보안 분야 (한동국 교수, 김종성 교수, 서석충 교수)

▶디바이스 공격 기술

- 암호 알고리즘이 수학적으로 안전하게 설계되어있더라도 실제 디바이스에서 연산이 수행되면서 발생하는 부채널 정보(연산 수행 시간, 소비 전력, 방출 전자파 등)를 이용하여 비밀 키를 탈취하는 물리적인 취약점이 존재함

- 부채널 분석 방법과 이에 대한 대응기법을 연구하여 금융 IC 카드와 USIM 등에 대한 물리적 보안과 관련된 많은 산업·사회 문제를 해결에 기여함
- 금융 IC카드 등 실제 디바이스를 대상으로 부채널 정보를 수집하고, 가공하여 분석까지 진행하고, 실제 디바이스를 대상으로 역공학을 진행할 수 있는 전문가를 양성함

▶디바이스 공격 대응 기술

- 실제 디바이스에 적용된 부채널 분석 대응기법을 교육. 실험실 환경에 비해 부채널 정보 수집 단계에서 어려움이 존재하는 경우 대응기법을 극복하기 위한 방법을 교육함으로써 역공학 역량을 향상시킴
- 최근 화웨이 사태를 시작으로 통신 장비뿐만 아니라, 정보보안을 요구하는 전자기기 내의 백도어에 대한 탐지가 요구되고 있으며, 백도어 탐지 방법으로 부채널을 이용하는 방법에 관한 연구를 진행할 계획임
- 부채널 정보를 비밀 정보를 탈취하는 것뿐만 아니라 디바이스 역공학 및 이상 탐지에 활용 가능. 부채널 정보를 활용한 디바이스 역공학 연구를 통해 백도어 탐지 등의 산업·사회 문제를 해결 가능함

▶디지털 포렌식 기술

- 디지털 기기를 매개로 이루어지는 범죄에 대한 법적 증거자료를 수집 및 분석, 보존하여 법적 증거물로 제출하는 각 과정에서 디지털 포렌식 수사관이 지켜야만 하는 원칙과 증거 분석 과정에 대하여 교육함
- 디지털 증거분석 도구를 사용하는 방법 뿐 아니라 디지털 증거 수집 절차를 통해 데이터의 무결성을 확보하는 방법 및 디지털 포렌식 분석도구 사용법을 다루어, 디지털 범죄나 사고를 조사할 수 있는 전문가를 양성함

▶모바일 포렌식 기술

- 새롭게 출시되는 기기나 어플리케이션, 혹은 국내에서만 사용되는 어플리케이션들은 포렌식 관점에서 연구되지 않은 경우가 많으며, 일부 데이터 분석도구의 경우 비싼 가격에 구매가 가능하여 일반적으로 사용하기가 쉽지 않음
- 새로운 포렌식 분석기술을 개발할 수 있도록 교육하여 기존 세계적인 포렌식 분석도구에 적용된 포렌식 분석기술을 연구함
- 이를 통해 디지털 기기를 통해 일어나는 범죄나 사고를 예방 및 조사할 수 있는 포렌식 분석 전문가를 양성함
- 본 교육을 통하여 양성된 전문인력은 국가보안기술연구소, 한국전자통신연구원, 한국인터넷진흥원, 군, 공공기관 등 정부 기관 주관의 디지털 포렌식 및 암호기술 분야 연구과제에 참여하여 디지털 기기를 통해 일어나는 범죄나 사고를 예방 및 조사할 수 있는 포렌식 분석기술 연구에 기여해 왔으며, 이후에도 지속할 계획임

▣ 안전한 초연결사회를 위한 암호기술 (강주성 교수, 염용진 교수, 김동찬 교수)

▶난수성 분석 기술

- 암호학적으로 안전한 난수발생기의 세부 구성 요소의 설계 및 안전성 분석 기법에 대한 교육 수행

- 확률론과 확률과정론에 기반한 난수열에 대한 독립성, 동일 분포성, 예측가능성, 정류적 성질 등의 분석 이론, 정보이론과 통계적 추론에 기반한 난수성 검정법 등을 종합적으로 교육함
- 본 교과목을 통하여 정보보안시스템에 필수적 요소인 실용적인 난수발생기에 대한 안전성 분석 및 평가를 수행할 수 있는 전문가를 양성함

▶정보보안 컨설팅
- 암호 보안기술의 올바른 활용을 위해서는 관련 제도와 표준의 이해가 필수적이며, 기술적인 이해도를 높이는 노력이 병행되어야 함
- CMVP(암호모듈 검증제도)와 CC(국제공통평가기준)의 제도의 운영과 관련된 기술과 표준의 활용 능력을 배양하여 정보보안 컨설턴트에 필요한 역량을 확보할 수 있도록 함

▶공개키 암호 분석 기술
- 양자내성암호 안전성 이론 및 구현 방법론 수업으로 기존 공개키 암호에 대한 이해를 위해 타원곡선암호와 양자내성암호 후보군 중 하나인 격자기반암호에 대해 교육함
- 타원곡선암호는 현재 주요 키공유 및 인증 프로토콜에 사용되는 암호로 생성원리 및 군연산 식 유도 방법, 주요 타원곡선인 Short Weierstrass, Montgomery 곡선의 성질을 교육함
- 또한, 격자기반암호의 기반문제인 SIS, LWE 문제를 이해하기 위해 필요한 고급 선형대수학 이론을 함께 교육함
- 본 교과목을 통하여 기존 공개키 암호시스템 및 양자내성암호에 대한 전반적인 안전성 분석 및 구현이 가능한 전문가를 양성함

▶정보보안 프로토콜 설계 기술
- 디지털서명, 개인식별, 메시지 인증, 출처 인증, 프라이버시 보존형 합의 프로토콜, 시도-응답 방식, 영지식 증명 방식, 안전한 키설정 및 분배, 안전한 다자간 계산(SMC) 등의 정보보안 관련 프로토콜에 대한 안전성과 효율성 분석 기술을 교육함
- 본 교과목을 통하여 정보보안시스템의 외부 공격자 뿐만 아니라 내부 공격자와 제3의 신뢰기관(TTP)에 의한 보안 침해 사고에 대처할 수 있는 전문가를 양성함

▣ 안전한 초연결사회를 위한 자율성장 AI 보안 기술(윤상민 교수, 최은미 교수)

▶지능형 사물 인터넷 기술
- IoT 환경에서의 자율 성장 AI 취약점 발견 및 보안 기술에 대한 교육을 수행함
- AI 기반 IoT common platform/Distributed system을 구성하기 위한 연구를 진행해 왔으며, 이를 기반으로 IoT 디바이스를 이용한 다양한 융합 서비스 생성에 관한 교육을 진행함

▶인공지능 기반 IoT 분산시스템 기술
- 장치 간 새로운 통신 시스템을 위하여 사용자 프로필 및 서비스 프로필을 정의하여 새로운 서비스를 제공할 수 있는 지능형 시스템에 대한 기술 개발 연구를 수행함
- 임의의 service provider가 DSC 서비스 프로필 상에 명시된 service lifetime 동안 서비스 사용권 소유를 주장할 수 있는 multi-ownership에 대한 연구를 수행함
- 이와 같은 연구를 바탕으로 인공지능 기반 분산 처리 시스템 교육을 함으로써 분산 인공

지능 시스템에서 발생할 수 있는 다양한 문제를 해결할 수 있는 전문가를 양성하고자 함

▶자율성장 인공지능 기술

- 지능형 시스템의 효율적 운영을 가능하도록 분산 시스템 관련 연구 및 교육을 진행함
- 이를 바탕으로 사람-기기, 기기-기기 사이에서 생성되는 데이터를 기반으로 스스로 학습하고 성장할 수 있는 swarm intelligence 연구를 진행함
- 지속적으로 발생하는 AI 기술의 단점을 보완하고 동시에 스스로 학습하고 수정할 수 있는 모델을 개발할 수 있도록 함
- 본 교육을 통하여 다양환 환경에서 최적화된 인공지능 기술을 설계하고 운영할 수 있는 전문가 양성 가능함

▶인공지능 보안 기술

- 지능형 시스템에서 인공지능 기술이 많이 활용되고 있으며, 자율 성장 시스템에서 데이터에 의한 시스템 및 모델 취약점을 발견하고 이에 대처하기 위한 보안 기술을 개발하고 교육함
- 인공지능의 허점을 연구하고 분석하여 사회 시스템에 적용하기 위한 연구를 진행하고 교육함
- 본 교육을 통하여 인공지능 기술의 취약점 분석능력과 안전한 운영능력을 갖춘 전문가 양성 가능함

1.3 교육연구단의 구성

④ 전임교수(신임교수) 충원계획의 적절성

▣ 전임교수 충원 및 연구지원을 위한 제도 개선

▶학사 규정의 제정 및 개정

- 산학협력 교수, 연구중점교수 임용 및 처우에 관한 규정
- K* 스타 교수 및 우수연구교수에 대한 처우 규정
- 연구의 국제화/대학원생 해외파견(SGE) 규정
- K* 스타 교수 및 우수연구교수에 대한 처우 규정
- 교육연구단장 강의시수 감면 규정

▶우수 신임교원 충원을 위한 계획

- 특히 대학원의 우수한 인재들이 실질적인 연구활동을 수행할 수 있는 학·연·산 협동과정을 확대하고자 함
- 현재는 5개 연구기관(2019학년도 기준)과 학·연·산 협동과정을 운영 중이나 'Small Giant'의 특화 전략을 바탕으로 하여 민간 기업체 중심으로 협동과정을 신설할 계획임
- 이를 통해 대학원이 갖고 있는 첨단원천기술을 산업계에 이전하고 해당 과정에 참여한 인력을 산업계에 배출함으로써 산업체와 대학원간의 Win-Win 전략을 도모하고자 함

현행 대학원 운영 체계에 대한 SWOT 분석

내부 요인	
강점(Strengths)	약점(Weaknesses)
►학문 분야별로 일원화된 관리체계 구축으로 학부과정과 석박사과정의 유기적 연계 체계 확보 ►우수한 전임교원의 학부과정 및 석박사과정 소속 겸직 가능 ►학과·전공별 주임교수 겸무 용이 ►대학원 연구·교육을 강화할 수 있는 우수한 산학협력 및 창업 조직 및 운영 노하우 보유	►학부 중심의 학문분야 운영 구조로 전문 연구인력 양성의 어려움 ►학문분야별로 적은 수의 석박사과정생 운영으로 연구인력의 층 얇음 ►일상적 학사관리 위주로 대학원의 역량 강화를 위한 전문화된 조직운영 체계 부재
외부 요인	
기회(Opportunities)	위협(Threats)
►산업계 수요변화에 따른 융복합 전공 신설로 시장 선점의 기회 ►산학연계 등 실용성을 강조하는 우리 대학만의 차별화된 대학원 발전전략 수립 및 추진으로 도약의 전환점 마련	►사회적 수요가 있는 유망전공의 신설 및 기존 전공의 개편이 어려워 타 대학과의 경쟁에서 뒤떨어질 가능성 ►학문단위별 운영으로 융합을 필요로 하는 연구역량의 저하

- 수요자 중심의 맞춤형 교육·연구 지원체계 고도화 지원체제를 가동하여 대학원 거버넌스 및 교원인사제도 개혁, 학사규정 개정을 통한 교수·학생·신진연구자의 교육·연구 지원체계를 고도화할 예정임
- 위의 표의 국민대학교 대학원의 SWOT 분석을 통해, 우수한 신임교원의 충원에 필요한

연계체계를 지속적으로 개선함

- 우리대학은 대학원 운영을 위해 총 636명의 행정지원 인력을 배치하여 각 학과·전공의 제반 학사관리를 수행하고 있으며, 이러한 인력 중 신임교원에 대한 전담지원 담당자 제도를 계획하고 있음
- 대학원 교학팀에 정규사무직원 5명, 업무보조직원 2명, 행정지원 조교 66명이 배치되어 있고, 대학원의 42개 학과(92개 전공)에는 13개 단과대학의 학부(과) 전공과 통합 운영하여 정규사무직원 24명, 실험실습실기기사 11명, 업무보조직원 72명, 행정지원 조교 90명 및 행정지원 학생근로 368명이 배치되어 있으므로, 신임교원 전담지원자를 1-1 매칭하여, 연구과제 및 행정업무를 지원할 예정임

▶우수 신임교원 지원을 위한 계획

- 대학 본부에서 신설 예정인 대학원발전기획팀에 본 협동과정 전체의 발전계획 및 실행방안을 수립하여 제안하며, 산학협력단과의 유기적인 협조체제를 구축하여 대학원의 경쟁력을 극대화함
- 대학원발전기획팀의 역할은 대학원발전계획 수립 및 세부계획 실행, 대학원자체평가 및 환류, 유연한 학사구조(융합학과 및 전공)의 도입을 포함한 대학원 교육과정 혁신, 대학원 제도혁신, 대학원 산학협력, 연구역량의 국제화 인프라 구축, 대학원혁신추진단 지원 등으로 요약될 수 있음.
- 대학원장 산하에 설치되는 ‘융합전공관리위원회’(위원장: 대학원장, 위원: 융합협동과정 주임교수, 융합형 국책사업 책임자, BK21+ 4단계 교육연구단장 및 교육연구팀장 등 7명 내외)에 적극 참여하여 융합분야를 발굴하고, 커리큘럼 설계, 운영, 모니터링, 개선조치 등을 관장함
- 산학협력단의 연구기획팀, 산학협력팀의 새로운 기능 수행을 통한 긴밀한 협조를 받아 대학원 전체의 정책수립과 실행안을 도출하고, 유망 분야의 전공(융합전공)을 파악하고, 해당분야의 신임교원의 연구역량을 강화하기 위한 교육연구단장에게 권한을 부여하여 지원할 계획임
- 기존의 학사관리(입학, 교과과정 편성 및 수업, 외국어 및 종합시험, 학위논문심사, 장학생 추천 및 조교임용, 학사관리, 학술지원) 업무 외에 유망 분야의 전공 신설 및 새로운 커리큘럼 설계에 따른 교과과정 운영 등 신임교원 및 전임교원의 교육연구사업을 대학원 교학팀을 중심으로 지원함

⑤ 대학원생 현황

<표 1-4> 교육연구단 참여교수 지도학생 현황

(단위 : 명, %)

기준일	신청 학과	참여 인력 구성	대학원생 수											
			석사			박사			석 · 박사 통합			계		
			전체	참여	참여 비율 (%)	전체	참여	참여 비율 (%)	전체	참여	참여 비율 (%)	전체	참여	참여 비율 (%)
2020. 05.14	금융정보 보안학과	전체	25	25	100.00	13	13	100.00	2	2	100.00	40	40	100.00
		자교 학사	20	20	100.00	8	8	100.00	2	2	100.00	30	30	100.00
		외국인	0	0	-	2	2	100.00	0	0	-	2	2	100.00
참여교수 대 참여학생 비율						400.00								

<표 1-5> 교육연구단 참여교수 지도 외국인 학생 현황

연번	성명	국적	학사출신대학	공인어학성적		비고
				국어	영어	
1	KESARI MARY DELPHIN RAJ	India	B.Sc Software Engineering COLLEGE : Malankara Catholic College, M.S.University	-	-	
2	SUGANYA SELVARAJ	India	Bachelor of Science in Mathematics, Government arts Collegee,	-	-	

1. 교육연구단 구성, 비전 및 목표

1.4 기대효과

▣ 산업・사회 문제해결형 정보보안 전문인력 양성의 기대 효과

- 본 사업은 미래 IT산업 발전을 선도하기 위한 보안산업 및 정보보안 관련 사회적 문제의 해결을 목적으로 하는 문제해결형 교육사업임
- 기존의 정보보안 관련 기술과 직업 영역을 뛰어넘는 새로운 일자리 창출의 가능성을 제시할 수 있을 것이며, 관련된 신규 분야의 인력을 안정적으로 배출할 수 있을 것으로 기대함
- 미래 IT 환경의 보안위협을 예방하고 보안사고에 즉각 대응할 수 있는 정보보안 전문 인력 양성을 위한 체계적인 교육 및 연구 체계의 개발과 보급에 기여함
- 정보보안 기술 중심 교육 트랙과 상용서비스를 고려한 정보보안 법령, 정책, 실무 중심의 트랙을 운영하여 경쟁력 높은 전문성을 확보하고, 산업체에서 필요로 하는 정보보안 코디네이터 양성에 기여함
- 본 교육연구단의 교육 및 연구 활동에 따라 국내 정보보안 전문가를 양성함으로써 연구단 내 여러 분야에서의 연계적인 기술적 교류와 활용에 따른 다방면의 지식을 습득한 미래형 기술자들을 배출하는 데 기여함

▶초연결사회의 통신환경을 위한 정보보안 분야 핵심기술 전문인력 양성

- 장비 간 정보보안과 5G, LTE, WiFi, 무선 LAN, TVWS 등과 같은 무선망용이나 이동통신 망용 암호 장비 개발과 이동통신 및 무선 서비스를 위한 핵심 암호 기술을 바탕으로 국내외 IT산업 및 사회에서 꼭 필요한 정보보안 전문가 양성에 기여함
- 본 교육연구단을 통해 양성된 미래 초연결사회를 위한 정보보안 전문 인력은 사회 전반의 성장 동력이 되어 변화되는 6G 환경을 주도할 창의적 인재 배출에 기여할 것임
- 4차산업혁명 기술이 다양한 분야에 접목됨에 따라 지표의 70%가 넘는 바다를 활용하는 기술 패러다임으로 전환되고 있으며, 2030년 상용화 예정인 6G 네트워크와 Underwater IoT가 하나가 되는 초연결사회를 위한 속도감 있는 혁신성장이 예상되므로, 이를 위한 체계적이고 심도 있는 학술연구 및 전문지식 습득을 바탕으로 한 전문인력 양성이 요구되며, 더 나아가 6G 이동통신 적응형 Underwater IoT 강화를 통하여 수중통신의 한계 돌파 및 산업화를 통한 다양한 신규 일자리를 창출하는 등 다각적인 기대효과가 예상됨

▶디바이스 보안 전문인력 양성

- 부채널 정보 기반 디바이스 역공학 기술 확보를 통해 기존 해외 기술 종속 관계에서 벗어나 자국의 산업을 보호할 뿐만 아니라 해외 암호 기술 시장을 선도함
- 자국 기술력 확보를 통해 기존에 해외로 유출되던 기술 컨설팅 비용 등의 절감을 통한 국내 산업 활성화에 기여함
- 디바이스 보안 전문 인력을 양성하여 국내 민간-공공 산업에 진출시킴으로써 국외 기술 의존도를 낮추고, 국내 정보보안 제품 보안 수준 향상 및 국가 경쟁력 향상에 기여함
- 디지털 기기를 통해 일어나는 범죄나 사고를 적절하게 조사할 수 있는 포렌식 수사 전문가를 양성함
- 국내외에서 새롭게 출시되는 디지털 기기나 어플리케이션의 데이터의 분석기술을 개발해 포렌식 수사에 기여하고 분석 도구를 개발할 수 있는 포렌식 분석 전문가를 양성함
- 소프트웨어뿐만 아니라 하드웨어에서의 디바이스 고속 암호설계 기술 개발을 통해 해외에서 활발하게 연구되고 있는 디바이스 고속 암호설계 기술을 확보함
- 동형 암호나 클라우드 서비스와 같은 대용량 데이터에 대한 고속 설계 필요성이나 양자

내성 암호와 같은 최적화가 필요한 암호화 알고리즘에 대한 고속 구현 필요성에 대하여 효과적인 대응이 가능할 것임

▶암호 분야 핵심기술 전문인력 양성

- 현재 사용자 및 기기 인증에 이용되는 핵심 기술은 인수분해 문제와 이산대수 문제를 기반으로 설계된 암호임
- 인증에 필요한 핵심 기술인 암호들은 양자 성질을 이용하면 쉽게 무력화할 수 있음이 1994년 Peter Shor에 의해 알려짐
- 최근 많은 글로벌 기업들이 양자 컴퓨터 개발 사업을 시작하면서 괄목할만한 성과를 발표하고 있어서 실용적 수준의 양자 컴퓨터 시대가 가시권에 들어왔음을 의미하기 때문에, 이를 대비하기 위해 기존 암호를 시급히 양자 내성 암호로 교체해야 함
- 양자 내성 암호는 격자 기반, 부호 기반, 해시함수 기반, 다변수함수 기반, 타원곡선 동종 기반 암호로 분류되는데 각 암호 군마다 구조가 복잡하여 구현 난이도가 높고, 파라미터 설정과 같은 알고리즘 운용 측면의 제약 조건이 많음
- 따라서 양자 컴퓨팅 시대에 안전한 ICT 인프라 보안체계를 구축하기 위해서는 양자 내성 암호에 대한 전문 지식이 필수임
- 본 교육연구단을 통하여 시급한 산업계 요구인 양자 내성 암호의 고급 전문 인력을 양성한다면, 양자 컴퓨팅 시대에 적합한 산업사회의 정보보안 시스템 구축을 위한 초석을 다지는 데 큰 역할을 할 것으로 판단됨

▶자율 성장 AI 보안 인력 양성을 통한 학계 선도 및 새로운 융합 연구 분야의 개척

- 현재까지 AI 전문가에 대한 수요가 매우 많음에도 불구하고 지속적인 인력 수요 및 공급의 불균형 현상이 발생하고 있으므로 본 교육연구단이 이 문제의 해소에 기여할 것임
- 다양한 데이터를 기반으로 기계학습 및 지능형 시스템에 대한 이해를 바탕으로 자율 성장 AI 분야를 개척함과 동시에 관련 연구 분야를 선도함
- AI 기술에 대한 이해와 정보보안에 대한 이해를 바탕으로 다양한 지능형 시스템 환경에 적용함으로써 새로운 학문 분야를 개척 및 선도하는 것이 가능함
- AI 기술은 다양한 금융 및 통신 분야에서 활용도가 높아지고 있으나, 이와 더불어 사생활 보호 및 해킹의 위협도 높아지고 있으므로, 이에 대한 대비로 시스템의 안정성 확보 및 사생활 침해 예방에 기여할 수 있음
- 자율주행자동차 등 지능형 시스템에서 다양한 기기들로부터 생산되는 데이터를 기반으로 한 자율 성장 시스템을 통하여 데이터 가공 및 학습을 위한 경제적 손실을 최소화할 수 있을 것으로 기대함
- AI 기술에 대한 이해와 이를 공격 및 방어할 수 있는 기술개발이 가능하며, 또한 지능형 시스템에 대한 해킹 방지 기술을 통하여 다양한 산업 분야의 기반 기술로 활용함
- 사람-기기와의 상호작용에 대한 많은 연구를 바탕으로 사람-기기 및 기기-기기간 상호작용에 대한 연구를 통하여 다양한 환경에서의 지능화된 IoT 시장 활성화에 기여함
- AI 기술이 다양한 산업 분야에 내재되는 상황에서 AI 기술의 허점을 차단하기 위한 방어 기술 개발을 통하여 지능형 시스템의 안전성과 신뢰성 확보에 기여함

Ⅱ. 교육역량 영역

1. 교육과정 구성 및 운영 계획

▣ 본 교육연구단의 교육 목표

▶초연결사회의 정보보안을 선도하는 전문가 양성을 위한 미래 정보보안 교육과정 운영

▣ 문제해결형 전문가 양성을 위한 교육 과정 세부 목표

▶암호이론/정보보안/AI 분야의 융합교육 실현

▶미래 초연결 환경의 지속 가능한 발전을 선도하는 정보보안 전문인력 양성

▶보안위협에 대한 선제적 대응을 위한 원천기술 개발 및 상용화를 통한 실무형 인재 교육

▶ICT 기술의 융합을 통한 새로운 미래 비즈니스 모델 창출형 인재 교육

▣ 세부 목표별 교육 방향

▶암호이론/정보보안/AI 분야의 융합교육 실현

- 수학 및 확률론 기반의 암호이론 기술을 바탕으로 실용기술 융합이 가능한 인재 양성
- 프라이버시 보호 및 인증 기술에 대한 전문지식과 AI 관련 핵심 기술을 겸비한 융합형 창의적 인재 양성
- 보안사고 예방 및 조사 전문가 및 정보보안 리스크 관리 전문가 육성
- 학제간 협동과정의 공통 필수과목으로 균형있는 기반을 갖춘 인재 양성
- 전문지식과 커뮤니케이션 능력을 갖춘 정보보안 전문가 양성
- 정보보안 산업 및 사회 문제를 해결 가능한 융합교육을 통해 미래 정보기술 환경에 능동적으로 대처할 수 있는 정보보안 전문 인력 양성

▶미래 초연결 환경의 지속 가능한 발전을 선도하는 정보보안 전문인력 양성

- 스마트 플랫폼 기반으로 ICT에 대한 의존도가 심화될 미래 정보통신환경을 능동적으로 선도할 수 있는 정보보안 인재 양성
- 진화하는 ICT 환경에 대한 전문지식을 바탕으로 서비스의 안전성을 진단하고 보안 문제를 해결할 수 있는 전문가 양성
- ICT 인프라와 보안기술의 전문지식을 갖춘 보안 시스템 전문가 양성

▶보안위협에 대한 선제적 대응을 위한 원천기술 개발 및 상용화를 통한 실무형 인재 교육

- 미래 사회의 안정적인 발전과 진화를 위한 정보보안 원천기술 개발형 인재 양성
- 초연결사회에 대한 이해를 바탕으로 보안이슈의 분석·대응 실무능력을 갖춘 인재 양성
- 사회의 변화관리와 정보보안의 전문지식을 겸비한 보안 리스크관리 전문가, 보안사고 대응 전문가 양성
- 미래 IT 서비스의 발생가능한 정보보안의 취약점을 극복하고, AI 기반의 미래 IT 서비스를 선도하는 핵심 인력 양성

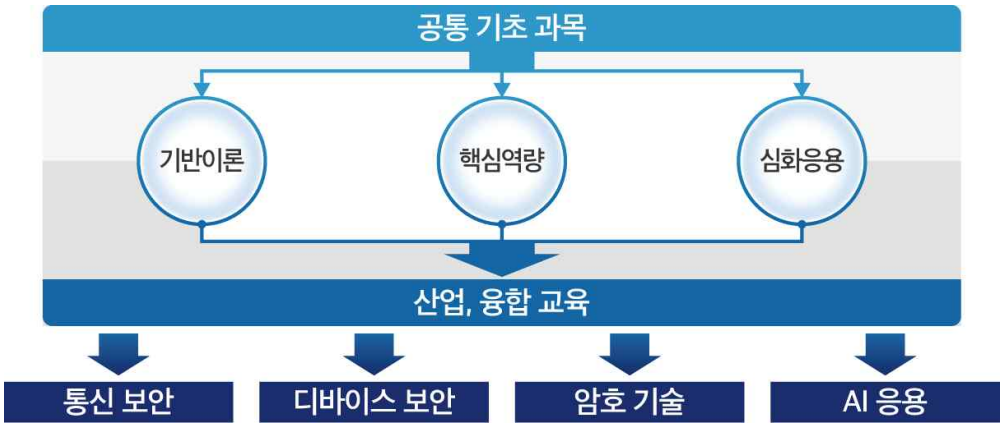
▶ ICT 기술의 융합을 통한 새로운 미래 비즈니스 모델 창출형 인재 교육

- 비즈니스 환경과 서비스에 대한 전문성과 함께 해당 분야의 정보보안 기술에 대한 적용능력을 갖춘 인재 양성
- 새로운 비즈니스를 창출할 수 있는 소양을 갖춘 보안 솔루션 개발 및 시스템 보안전문가 양성
- ICT 기반의 미래의 정보 환경에서 금융과 정보보안 기술의 융합을 통한 새로운 비즈니스 모델 개척 가능 인재 양성
- 초연결시대의 정보보안을 연구하고, 이를 학문적, 실무적으로 응용 및 확장 할 수 있는 전문성과 국제 경쟁력을 겸비한 창의적 정보보안 전문인력 양성

▣ 본 교육연구단의 교육과정 구성

▶교육과정 구성 방향

- 기존 금융정보보안학과의 교과목을 중심으로 교육단의 목표에 부합하는 과정으로 개편
- 다학제간 융합 프로그램을 위한 교과목 신설
- 새로운 가치 창출 및 실용적 문제 해결을 위한 교육과정 개설
- 신업계, 연구소 등의 외부 전문가와 함께 문제해결형 교과목의 팀티칭 추진
- 깊은 전문지식의 축적을 위해 교육과정의 체계화 및 세분화 추진



▶교과목 구성

- 공통기초 과정부터 실용과정까지 단계별로 체계화된 교과과정을 구성
- 4개 전문분야에 대한 핵심역량 및 심화응용 과정
- 산업・사회문제 해결 역량을 갖추기 위한 밀착형 연계 과정
- 산업계의 기술 수요와 사회적 환경의 변화에 따라 탄력적인 교과 운영

구분	개요
공통기초	- 각 분야의 전반에 걸쳐 공통으로 필요한 기초과목 - 전문가로서 갖춰야 할 연구윤리 및 논문작성법
기반이론	- 문제해결에 필요한 전문지식을 갖추기 위한 과정 - 전문가가 되기 위한 분야별 기반 이론의 체계적 학습
핵심역량	- 분야별 전문지식을 습득하는 과정 - 통신보안, 디바이스 보안, 암호, AI 분야의 전문성을 갖추는 과정
심화응용	- 다양한 문제를 스스로 인지・해결하는 역량을 갖추기 위한 과목 - 창의적인 문제해결 능력과 응용력을 배양
산업・융합	- 습득한 지식을 산업에 활용할 수 있는 능력을 배양 - 기술적 제도적 측면을 포함한 문제해결 역량을 확보

▣ 교과 구성

▶교육과정표

구분	개요	
공통 기초	- 연구윤리와논문연구 - 정보보안론	- 암호알고리즘 - PKI개론
기반 이론	- 고급정보통신론 (통신) - 임베디드시스템 (통신) - 실시간시스템 (통신) - 부채널공격론 (디바이스) - 보안구현개발방법론 (디바이스) - 디지털포렌식개론(디바이스)	- 해시함수와데이터인증 (암호) - 병렬암호구현 (암호) - 정보보안프로토콜 (암호) - 데이터마이닝 (AI) - 인공지능과보안이론 (AI)
핵심 역량	- 무선보안특강 (통신) - 클라우드컴퓨팅 (통신) - 부채널공격대응론 (디바이스) - 디지털포렌식특수연구 (디바이스)	- 공개키 암호분석이론 (암호) - 암호소프트웨어구현 (암호) - 대칭키암호분석 (암호) - 모델기반시스템설계 (AI) - 자율성장인공지능특론 (AI)
심화 응용	- 이동통신보안 (통신) - 정보시스템개발방법론 (통신) - IoT네트워크 (통신) - 디바이스공격대응론 (디바이스)	- 난수성분석론 (암호) - 증명가능안전성론 (암호) - 암호모듈평가및검증 (암호) - 인공지능융합기술특강 (AI)
산업 · 융합	- 정보보안시스템평가방법론 - 정보보안컨설팅 - 보안기술표준분석및구현	- 융합보안특강 - 사물지능망 특론

▣ 교과목 해설

▶공통기초 과목

- 연구윤리와논문연구(Research Ethics & Thesis Study)는 연구윤리 강화와 논문표절 근절을 위해 올바른 태도와 가치관을 갖도록 기본 인성을 함양시킴
- 암호알고리즘(Cryptographic Algorithm)은 고전 암호, Shannon의 이론에 기초한 스트림 암호와 블록 암호의 안전성 이론, 사용방법에 따른 문제점, 설계방법 등을 학습함
- 정보보안론(Introduction to Information Security)은 통신 및 금융 인프라에 필수적인 정보보안기술 전반에 대하여 살펴보고, 분야별 요소기술에 대하여 이해함
- PKI개론(Introduction to PKI)은 공개키 기반구조(PKI)의 필요성을 인식하고, 인프라 구축에 필요한 기술에 대한 이해를 목표로 하고, 공인인증서 체계를 비롯한 PKI의 사례를 중심으로 활용 현황과 보안 이슈를 점검하고 금융보안과 PKI의 관계를 학습함

▶기반이론 과목

- 고급정보통신론(Advanced Information Communication Theory)은 IoT connectivity / IoS(Internet of Service)에 대하여 학습
- 상황인지(context-awareness) / 위치인식(localization) 및 IoT 아키텍처, IoT 네트워크 요구사항 등 다양한 응용 시스템에 대하여 학습을 진행함임베디드시스템(Embedded System)은 ARM 아키텍처에 대한 이해 및 펌웨어 기반의 임베디드 시스템 설계 및 구현 능력을 함양함

- 실시간시스템(Real-time System)은 실시간 시스템에 대한 이해 및 실시간운영체제 기반의 임베디드 시스템의 설계 및 구현 능력을 함양함
- 부채널공격론(Side Channel Attacks)은 스마트디바이스의 물리적 취약성 분석 기술을 학습함
- 보안구현개발방법론(Security Implementation Methodology)은 정보보안에 필요한 암호기능을 구현하는 실무적인 방법을 익히고, 안전한 코딩기술을 바탕으로 환경에 맞는 보안기능을 식별하고 구현할 수 있는 능력을 배양함
- 디지털포렌식개론(Introduction to Digital Forensic)은 PC나 노트북, 휴대폰 등 각종 저장매체 또는 인터넷 상에 남아 있는 각종 디지털 정보를 분석해 의미있는 정보를 찾는 방법 및 기술에 대해 학습함
- 해시함수와데이터인증(Hash Function and Message Authentication)은 전자서명에 활용되는 충돌 회피 해쉬 함수 및 이를 이용하여 데이터 위변조를 검출할 수 있는 MAC 생성 방법의 설계원리를 학습함
- 병렬암호구현(Parallel Implementation of Cryptographic Algorithms)은 병렬처리를 위한 하드웨어와 운영체제에 대한 체계적인 이해를 바탕으로 암호알고리즘의 고속 병렬 구현기술을 습득함. 특히, 그래픽프로세서(GPU)를 이용한 고속구현 실습으로 암호알고리즘에 대한 이해와 함께 응용능력 향상을 도모함
- 정보보안프로토콜(Information Security Protocols) 다양한 암호 알고리즘의 역할과 안전성 개념을 정확히 인식하여 키교환 프로토콜, 위탁 프로토콜, 식별 프로토콜, 영지식 프로토콜, 다자간 계산 프로토콜 등의 보안 목적에 부합하는 정보보안프로토콜의 안전성과 효율성을 올바르게 분석할 수 있도록 함
- 데이터마이닝(Data Mining)은 데이터 마이닝의 기본 개념 학습, 실습을 통한 사례 학습을 진행하고, Association, Clustering, Classification 등 데이터 마이닝을 통해 발굴되는 지식의 패턴에 대해 배우고, 가장 널리 사용되고 있는 도구인 SAS Enterprise Miner를 활용하여 실습 능력을 배양하도록 함
- 인공지능과 보안 이론(AI and Security)은 인공지능을 활용한 보안 기술 및 인공지능의 허점을 분석하기 위한 개념 및 이론을 연구함

▶핵심역량 과목

- 무선보안특강(Wireless Security)은 최신의 무선통신 기술과 그 응용에 필요한 보안기술을 학습함
- 클라우드컴퓨팅(Cloud Computing)은 기업의 비즈니스 활동을 지원하고, 소비자들의 편익을 증대시켜 주는 클라우드 컴퓨팅 및 응용 서비스에 대한 일반적인 개념을 이해하고, 본 과목에서는 클라우드 컴퓨팅 환경 하에서 요구되는 핵심 기술 및 이슈들에 대해 다루며, 서비스 대상에 따라 구분되는 SaaS, PaaS, IaaS 과 혼합된 형태의 서비스들에 대해 공부함
- 더불어, 분산 시스템, 미들웨어, 어플리케이션 통합 등 클라우드 서비스를 형성하는데 필요한 다양한 개념들, VM 관련 기술과 Public Cloud 의 사용 및 Open-source cloud 에 대하여 함께 습득함
- 부채널공격대응론(Countermeasures of Side Channel Attacks)은 부채널공격에 안정한 S/W 및 H/W 기반 대응방법의 설계 및 구현에 대하여 학습함
- 디지털포렌식특수연구(Special Research of Digital Forensics)은 디지털 포렌식 관련 최신

기술을 습득하고 연구함
- 공개키 암호분석이론(Cryptanalysis of Public-key Cryptosystem)은 인수분해, 이산로그, 등의 수학적 문제에 기반한 공개키 암호에 대한 설명과 기본적인 공격법 및 프로토콜의 적용에 따라 발생하는 제반 문제점을 소개한다. 아울러 각종 공개키 암호에 대한 안전성을 학습함
- 암호소프트웨어구현(Implementation of Cryptographic S/W)은 국제표준 대칭키 암호 및 공개키 암호의 소프트웨어 구현기술을 습득함
- 대칭키암호분석(Topics in Symmetric Key Cryptanalysis)은 블록암호 및 스트림암호 해시함수 등에 대한 안전성 분석을 위한 기본기술을 습득하고, 사용환경에 따라 안전한 알고리즘의 선택과 활용능력을 교육함
- 모델기반시스템설계(Model-based System Design)은 소프트웨어 설계 및 구현 패턴에 대한 기본적인 개론을 포함하여 일반적인 이해를 습득하며, Java와 같은 객체지향 프로그램 언어를 이용하여 디자인 패턴을 소프트웨어 시스템 설계에 적용 하는 다양한 작업들과 종류별 패턴들을 학습함
- 소프트웨어 디자인 패턴에서의 Creational Patterns, Structural Patterns, Behavioral Patterns의 다양한 세부 패턴들을 습득하며, 실제 시스템 설계에 적용하며 학생들의 설계 및 구현 능력을 함양함
- 자율성장인공지능특론(Advanced Self-supervised AI)은 자율성장 인공지능에 필요한 기본 개념과 모델을 분석하고 다양한 데이터 기반 문제 해결 능력 방법에 대하여 연구함

▶심화응용 과목
- 이동통신보안(Mobile Security)은 3G, 4G, 5G 등의 이동통신망의 최신 보안 구조 및 그 응용 기술을 학습함
- 정보시스템개발방법론(Information System Development Methodology)은 임베디드 시스템과 관련된 정보시스템 개발 방법론에 대해서 학습하고, 자료 구조와 알고리즘, 임베디드 시스템의 설계 및 구현에 대한 전반적인 과정 등에 대하여 학습함
- IoT 네트워크(IoT Network)은 IoT(Internet of Things), M2M(Machine to Machine Communication), WoT(Web of Things), UIoT(Underwater IoT)와 같은 차세대 네트워크와 관련 국제 표준에 대하여 학습함
- 디바이스공격대응론(Countermeasures against Financial Device Attacks)은 개인PC, 스마트폰, 스마트카드, Micro-SD, OTP 등 다양한 디바이스에서 발생 가능한 보안 취약성을 찾고 이를 안전하게 대응하는 기술에 대해 학습함
- 난수성분석론(Analysis of Randomness)는 정보보안 프로토콜 및 암호 알고리즘에 필수적으로 사용되는 난수발생기의 설계와 안전성 분석을 학습함
- 증명가능안전성론(Provable Security)는 Pseudo-randomness, 정보이론 관점의 안전성, 계산복잡도 측면의 안전성 등 암호 알고리즘 및 프로토콜에 대한 증명가능 안전성 이론을 학습함
- 암호모듈평가및검증(Evaluation and Validation Techniques for Cryptographic Modules)는 암호모듈 검증제도(CMVP)에 대한 정책적·제도적 이해를 바탕으로 암호모듈의 평가·검증을 위한 기준과 관련기술에 대한 이해와 적용방법을 습득하고, 각 검증기준에 대한 취지의 이해와 함께 평가기술의 적용방법에 대하여 학습함

- 인공지능 융합 기술 특강 (AI Convergence)은 인공지능 및 보안 기술과 관련된 다양한 분야에서의 활용 및 융합 연구에 대한 전문가 특강을 통해 새로운 연구동향을 학습함

▶산업・융합 과목

- 정보보안시스템평가방법론(Information Security System Evaluation Methodology)은 IT제품 및 시스템의 보안성 평가를 위한 공통 평가 기준 (Common Criteria), CMVP (Cryptographic Module Validation Program), PIV(Personal Identity Verification) 등의 평가 방법론을 학습함
- 정보보안컨설팅(Information Security Consulting)은 정보보안제품 또는 정보보안 관련 조직의 정보보안의 수준과 취약점 및 정보보안 정책, 표준 및 절차, 모니터링 과정 등을 평가하여 개선 방법을 제공하는 방법을 학습함
- 보안기술표준분석및구현(Analysis and Implementation of Security Technical Standards)은 IETF(Internet Engineering Task Force), 국제표준화기구(ISO), 미 국가표준기술연구원(NIST)에서 발간하는 보안기술과련 표준을 이해하고 구현과 관련한 지식을 학습함
- ISO/IEC, IETF 등의 국제표준기술에 대한 이해와 분석을 바탕으로 안전한 표준기술을 활용하여 보안시스템을 설계할 수 있는 능력을 배양함
- 융합보안특강(IT Convergence and Security)은 IT와 타 산업의 융합기술을 배우고, 그 응용에 필요한 보안기술을 학습함
- 사물지능망특론(Advanced Internet of Things)은 IoT/IoS를 위하여 인간과 사물 및 사물과 사물간 상호 협력적으로 센싱, 네트워크, 정보 처리에 필요한 기술에 대하여 학습함

▣ 단계별 인력양성 프로그램 로드맵

▶1단계(2020~2021) : 정보보안 교육체계 수립

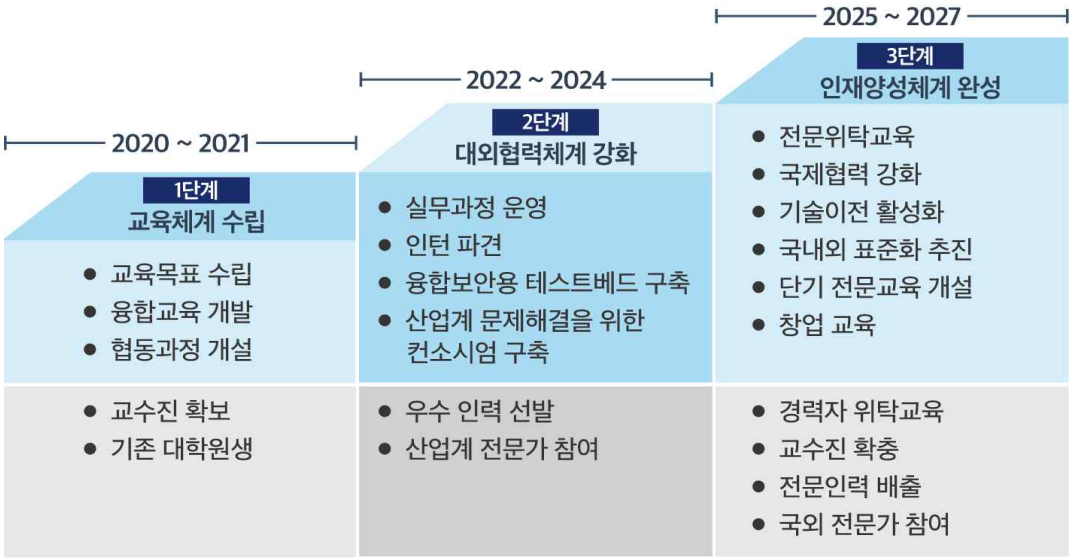
- 교육목표 및 비전 수립
- 정보보안 협동과정의 교과목 및 AI 융합과정 개발
- 기존 대학원생을 중심으로 협동과정 운영

▶2단계(2022~2024) : 정보보안 협력체계 강화

- 산업계의 전문가를 중심으로 정보보안 실무과정 운영 및 재학생의 인턴파견 추진
- 정보보안 기술개발과 커뮤니케이션의 활성화를 위한 보안기술 통합 테스트베드 구축
- 연구소, 산업계 전문가와 함께 하는 교육과정 개설
- 산업계의 정보보안 문제 해결을 위한 컨소시엄 구축

▶3단계(2025~2027) : CISO급 인재 양성체계 완성

- 현장 경력자 전문위탁 교육
- 미래 국제 통신환경 변화를 선도하기 위한 국제협력 강화
- 공공기관 임직원을 위한 경력자 단기 전문교육 프로그램 운영
- 연구개발 결과의 활발한 활용을 위한 지재권확보 및 기술이전
- 창업을 통한 산업문제 해결을 지원하기 위한 창업 교육 및 인큐베이터 운영



▣ 교육목표 및 비전을 실현하기 위한 추진 전략

▶보안문제해결형 교육과정 개발: 본 교육연구단의 교육 프로그램은 미래 초연결환경의 특성을 이해하는 보안 전문가 육성, 정보보안에 필요한 시스템 고급 개발자 육성, 보안사고 예방 및 조사 전문가 육성 등을 이루기 위한 다음의 특성화된 교육과정을 수행함

- 정보보안과 AI 분야의 우수한 교수진 확보
- 융합과정의 개발로 IT보안과 컴퓨터 공학의 기초역량 강화
- 산업계와 연계한 보안실무과정의 신설
- 재학 중 한 학기 이상의 인턴십 의무화
- 산업체 연계 맞춤형 교육 프로그램의 추진을 통해 교육 및 연구 결과의 성과물을 현장에서 실질적으로 적용할 수 있으며, 이를 활용한 비즈니스 수익 모델 개발
- 국내외 정보보안 IT 기업들과의 산학 네트워크를 구축하고 이를 토대로 유기적 산학협력 체계 정착
- 5G, IoT, AI, 빅데이터, 클라우드 등 신산업 분야의 도래가 예견되는 미래의 금융환경에 능동적으로 대처할 수 있는 상상력과 창의력을 가진 융합형 인재양성 프로그램을 구축

▶협동과정의 장점 극대화

- 정보보안 협동과정의 필수 기본과정으로 정보보안과 시스템보안 분야의 필수 소양을 겸비하도록 함
- 정보보안 기술 중심의 트랙과 정보중심의 트랙을 운영하여 경쟁력 있는 전문성을 확보함과 동시에 실무적으로는 보안 코디네이터 역할을 수행할 수 있도록 육성함
- 보안실무를 체험할 수 있는 교육장을 확보하여 현장에서의 보안기술 활용 방법에 적응하며, 개발기술을 테스트하고 데모할 수 있는 쇼룸으로 활용함
- 심화과정으로 인공지능 융합기술, 디바이스공격대응론 등의 연구를 공동으로 수행할 수 있는 융합과목을 운영함
- 산업계의 전문인력을 활용한 사례 중심의 실무과정 개설하여 실무적응능력을 극대화함
- 관련 산업계의 임직원에 대한 재교육 및 심화교육의 수요에 따라 장단기 위탁교육 프로그램을 구성하여 기관별로 내부 인력을 CISO로 활용할 수 있도록 지원함

▶문제해결을 위한 실무능력을 갖춘 인재 양성

- 참여 대학원의 정보보안, AI, 시스템보안 관련 교육경험을 바탕으로 분야별 체계적 교육을 실시할 계획이며, 다양한 분야의 기초교육 후 세부 연구 분야에 따라 교육과정의 목표를 달리 설정하여 목표에 맞는 교과목 운영함
- 진로를 고려한 맞춤형 교육: 석사과정의 경우 석사 한 학기 후 향후 진로를 지도교수와 결정하여 진로에 따른 교과목 선정을 통한 맞춤형 교육 실시함
- 교육과 훈련을 통한 전문가 양성: 수업 내용은 실습이 병행되도록 하여, 이론 위주의 연구가 아닌 이론과 기술을 겸비한 전문가를 양성함

▶고용연계형 교육과정 개설

- 본 사업을 통해 정보보안 분야의 독보적인 기술인력이 양성될 예정이지만, 이와 같은 역량이 성공적인 창업으로 연계되기 위해서는 시장에 적합한 사업모델(Business Model)의 개발이 필수적임
- 융합교육 및 실무교육을 통해 일차적인 검증이 이루어진 기술 및 인력의 경우 교내 인큐베이터 또는 교외 엑셀러레이터에 입주시키고, 창업준비자금을 지원하여 교과이수와 창업실행이 단절없이 진행되도록 하는 체제를 갖추게 됨

▣ 연구단의 교육실적

▶본 교육연구단 구성 교수진의 특성화된 융·복합 교육 실적

- 본 교육연구단은 2020년 4월 현재 3단계 두뇌한국(BK21) 사업을 통해 금융분야와 IT 분야를 포괄하는 “미래 금융보안 전문인력 양성 사업”을 통해 정보보안 전문인력 양성을 목적으로 융·복합 모델을 운영 중임
- BK21 3단계 사업을 수행하고 있는 본 학과는 소속 대학원생들이 관련 분야의 국제 연구동향을 습득하고 연구 공유 및 교류할 기회를 갖고, 국제적 경쟁력을 갖춘 정보보안 전문인력으로 성장할 수 있도록, 국제학회 참석 및 논문 발표를 하도록 독려하고 있음
- 또한, 참여 대학원생의 전문역량을 기르기 위해 다양한 연구과제에 참여하도록 하고 있으며, 연구를 통해 얻은 독창적인 연구성과는 국내외 학술대회와 논문지에 발표, 공모전 참여, 특허출원 등을 통해 성과를 얻고 있음
- BK21 3단계 사업에 참여하는 동안 국제 학술대회에 발표한 논문은 50건, 국내 학술대회에 발표한 논문은 130건, 국제 논문지에 발표한 논문은 20건, 국내논문지에 발표한 논문은 34건, 각종 국내외 공모전 수상은 11건, 국제특허 등록 1건, 국내특허 등록 30건, 국 내특허 출원 15건, 국제 PCT 출원 2건 등의 성과를 얻음
- 3단계 BK21 사업의 융·복합 경험을 바탕으로 학문간 융합을 통한 초연결시대의 정보보안 분야의 특성화 사업을 본격 추진, 특성화 분야에 대한 육성 및 지원을 진행할 예정임

▶특성화된 교육과정의 운영 실적

- 국민대학교 학부과정인 정보보안암호수학과는 자체 발전계획 수립하여 2001년 이후 암호학 및 정보보안 분야의 특성화를 지속적으로 추진하여 현재는 국내에서 유일하게 정보보안암호수학과 내에 7명의 정보보안 전공 교수를 확보하고 있으며, 수학적 지식의 기반 위에 컴퓨터 과학을 융합한 교육과정을 학부에서부터 대학원까지 연계하여 운영하고 있음
- 국민대학교 일반대학원 수학과에 정보보안전공을 신설하여 특성화된 교과과정을 운영하고 있으며, 2009년에는 정보보안연구소를 설립하여 국내의 유수의 연구기관 및 기업체와 정보보안

관련 공동연구를 활발히 수행하고 있음
- 국민대학교 수학과는 교육부의 비IT학과 교과과정 개편지원사업을 최우수 평가실적으로 수행한 바 있으며, 이를 통하여 암호학 및 정보보안 특성화 학과로 자리매김할 수 있는 최고의 교육환경과 제도적 장치를 마련했던 경험이 있음
- 국민대학교 소프트웨어융합대학은 조형대학 및 전자정보대학과 함께 교육부의 UIT디자인 특성화 인력양성 사업을 수행하면서 타 전공과의 융합교과과정 운영을 통한 창의적 인재양성을 시도한 바 있으며, 사업의 종료 후에도 “3C세미나”, “창업론”, “창의적프로젝트 실습” 등의 혁신적인 융합형 창의경영 교과목을 운영하고 있음
- 2014년 일반대학원 금융정보보안학과를 신설하여 신뢰 기반 사회 및 경제 정보 생태계 구현을 위한 금융정보보안 관련 제반 문제를 학문적으로 심도 있게 연구하고 이를 실무적으로 응용할 수 있는 전문성과 국제 경쟁력을 겸비한 창의적 정보보안 전문인력 양성을 목적으로 융합형 교육과정을 운영하고 있음

▣ 교육과정 운영 방향

▶교육과정과 교육대상의 특성화
- 기본과정: 정보보안, AI보안 분야의 기초과정을 개설하여 타 분야에 대한 적응력을 향상 시키고 융합형 인재가 될 수 있는 기본 소양을 배양함
- 전문과정: 개별적으로 선택할 수 있는 다양한 전문지식을 제공하는 과정으로 희망하는 트랙에 따라 해당분야의 경쟁력 있는 전문인력이 되도록 교육하는 과정임
- 실무과정: 현장의 실무를 체험하는 과정으로 교육내용에 따라 전문기관, 업계의 전문가와 전임교수가 공동으로 운영함
- 인턴/연수과정: 재학기간 중 한 학기 이상을 인턴이나 국외연수 과정으로 진행하며, 실무능력과 국제적 감각을 갖춘 전문인력으로 육성함
- 경력자 단기 전문과정: 학위과정과는 별도로 산업계의 경력자 위탁교육과정을 운영하여 보안기술과 비즈니스에 대한 전문성을 유지할 수 있도록 지원함

▶ 인적 네트워크를 형성을 위한 인적 피드백 형성
- 취업, 창업인력 배출 후 지속적인 협력과 교류를 통해 문제의 해결을 위한 인적 네트워크로 활용함
- 동문회와 원우회를 구성하여 정기/비정기적 모임을 통해 원우/동문간의 원활한 교류 및 활성화를 도모하여 졸업생들과의 관계를 강화하고 실무에서의 지식을 공유하도록 함

▣ 주관대학의 지원제도

▶ 주관대학 창업지원제도
- 국민대학교에서는 1999년부터 교내에서 수행되는 각종 연구 성과의 사업화 지원을 위해 창업보육센터를 운영해 왔고, 현재 13개 업체가 입주하고 있으며 향후 점진적인 공간 확충을 준비하고 있음
- 2013년 2학기 개원한 ‘지암 Innovator’s Studio’는 도전적 창업정신을 가진 학부 및 대학원생 30여 명을 선발하여 수업료 전액을 장학금으로 지급하고 벤처창업을 위한 전용 공간에서 청년창업이 이루어질 수 있도록 운영함
- 경영대학의 경우 “창업론” 수업을 통해 창업교육이 지속적으로 이루어져, 학부 졸업생 가운데 연간 2-3팀의 창업이 지속되고 있음. 특히 “창업론” 수업에는 최근 가장 각광받는 창업자

들이 수시로 참여하여 특강 및 멘토링을 수해함으로써 창업팀의 네트워크 확보에도 기여하고 있음

▶ 주관대학 취업지원제도

- 국민대학교에서는 취업지원 프로그램을 2012년부터 혁신적으로 강화한 바 있고, 각 전공단위별로 취업멘토 교수를 선정하여 학생 개개인의 경력개발 목표를 파악하고 그에 맞는 진로지도를 실행하고 있으며, 2013년부터는 “인생설계와 진로”라는 진로설계 프로그램을 모든 학부생의 필수교과로 지정한 바 있음
- 경력개발센터는 학부생 뿐 아니라 대학원생을 포함한 모든 학생들에게 진로설계부터, 적성시험 및 영어시험, 지원서작성, 면접 등 전 취업과정에 걸친 맞춤형 강좌 및 멘토링을 제공함
- 단과대학 및 전공별로도 별도의 노력이 투여되고 있는데, 경영대학은 단과대학차원의 취업지원실을 별도로 설립하여, 경영학 전공자들의 취업분야에 심도 깊게 특성화된 다양한 취업지원 프로그램을 운영 중임
- 2학년부터 3학년 사이 모든 학생들이 경력설계, 역량준비, 취업실전준비에 필요한 지식과 경험을 습득할 수 있는 교과과정이 설계되어 있으며, 각 분야별 취업멘토가 선정되어 소그룹 지도가 활성화되어 있음

▣ 통신보안 분야 교육과정 운영계획

▶대표문제 : 5G/6G 이동통신 엣지 컴퓨팅 해킹에 의한 초연결사회 안전성 위협

- 5G / 6G와 수중통신 환경의 정보보안 구현
- 초연결 통신환경을 위한 정보보안 서비스 신뢰성 확보

▶참여교수: 이옥연, 박수현

- 이옥연 교수: 이동통신보안, 암호 및 보안시스템 개발
- 박수현 교수: 임베디드시스템, 통신표준

▶주요 과목

구분	개요
기반 이론	- 고급정보통신론(Advanced Information Communication Theory) - 임베디드시스템(Embedded System) - 실시간시스템(Real-time System)
핵심 역량	- 무선보안특강(Wireless Security) - 클라우드컴퓨팅(Cloud Computing)
심화 응용	- 이동통신보안(Mobile Security) - 정보시스템개발방법론(Information System Development Methodology) - IoT네트워크(IoT Network)

▶전임교원 강의 계획 및 추진 방향

- 6G 맞춤형 고급 정보 통신론 및 Underwater IoT 6G 기술과 서비스 등과 같은 초연결사회를 대비한 특화된 교과과목이 개설될 예정임
- 도래할 6G 시대 수중↔지상 도메인에서의 초연결사회를 대비하여 신진 글로벌 전문인력

양성을 위한 본 교육연구단의 지속적인 교육프로그램은 지식체계를 확립하는 기본과정부터 실무지식을 축적하는 개발과정까지 단계별 지식수준을 고려한 모듈형 교육과정이 체계적으로 진행할 예정임

- 사회적 니즈(needs) 분석을 바탕으로 한 전문성 향상을 위한 전문화(specialization) 전략이 도입된 교육과정으로 개편될 것이며, 영어로 진행하는 수업을 일부 개설하여 운영하므로 세계적 수준의 대학원 교육과정으로 도약을 목표로 함
- 본 교육연구단은 유무선 통신 및 5G에서 6G에 이르는 보안 관련 기술의 표준화 분야 전문가들을 초청하여 워크숍 및 콜로키움(colloquium) 개최 등과 같이 특화된 교육 프로그램을 제공할 예정임
- 산업체, 지자체, 지역사회 등에 속한 다양한 구성원들을 중심으로 초연결사회를 위한 문제해결형 정보보안 연구를 위한 거버넌스(governance) 체제를 구축 및 운영하므로 정기적인 세미나 및 교육프로그램에 참여하는 대학원생들의 실무 역량이 강화되어 글로벌 경쟁력이 제고될 것임
- 5G/6G 이동통신 기술의 발전은 사람과 스마트한 사물간의 혁신적인 융복합 기술을 특수 도메인 영역까지 확대 적용 가능하게 하므로, 본 교육연구단이 제시하는 맞춤형 교육을 통하여 학습한 지식을 해양산업의 사회문제 해결을 위한 정보보안 등을 고려한 코어 기술 개발 연구에 적용하므로 전문성을 겸비한 인력양성 결과를 도출하게 될 것임
- 혁신 '인재' 양성에 초점을 둔 교육과 산업·사회 문제 해결을 위한 연구의 선순환 구조를 구축하기 위하여 본 교육연구단은 지식창출을 위한 핵심 주체로서 실용적 이론 및 실무 위주의 교육을 진행할 뿐만 아니라 산업현장의 수요를 반영한 연구를 진행할 예정임
- 또한, 6G 적응형 Underwater IoT의 글로벌 표준화를 주도하기 위하여 표준화 활동을 하는데 필요한 사항 등의 교육을 함께 제공할 것이고, 연구와 교육의 질적 향상으로 이어지는 선순환 구조를 실행하고, 미래의 국가 경쟁력 강화에 기여하게 될 것임
- IoT/ IoS의 trustworthiness Dynamic Service Composition 관련 교육을 통하여 IoT common platform에 대한 이해 및 AI 기반 service discovery 기술을 배양함
-

▣ 디바이스 보안 분야

▶대표문제 : 외산 네트워크 장비 백도어 발견 등 디바이스 비정상행위 안전성 위협

- 다양한 부채널 정보를 이용한 공격 및 대응기술 개발, 백도어 탐지
- 디바이스별 디지털 포렌식 기술을 이용한 증거획득 기술 및 산업보안 기술
- 디바이스별 암호 소프트웨어 및 하드웨어 고속 구현 기술

▶주요 과목

구분	개요
기반 이론	- 부채널공격론(Side Channel Attacks) - 보안구현개발방법론(Security Implementation Methodology) - 디지털포렌식개론(Introduction to Digital Forensic)
핵심 역량	- 부채널공격대응론(Countermeasures of Side Channel Attacks) - 디지털포렌식특수연구(Special Research of Digital Forensics)
심화 응용	- 디바이스공격대응론(Countermeasures against Financial Device Attacks)

▶참여교수: 한동국, 김종성, 서석충

- 한동국 교수: 디바이스 역공학
- 김종성 교수: 디지털 포렌식
- 서석충 교수: 디바이스 고속 설계, 소프트웨어 최적화

▶전임교원 강의 계획 및 추진 방향

- 부채널 정보 기반 디바이스 역공학을 수행하기 위해 최우선적으로 습득해야 하는 것은 디바이스에서 발생하는 부채널 정보를 수집하는 것으로, 본 교육연구단에서는 아두이노 보드와 같은 개발 실습 보드에 직접 저항을 달아 전력 파형을 수집하는 기초 교육부터 스마트폰 등과 같은 상용 장비에서 방출되는 전자파를 수집하는 응용 교육까지 실시함
- 수집되는 부채널 정보의 질은 분석 성능과 직결되므로, 노이즈를 최소화한 부채널 정보 수집과 노이즈 제거 기법에 대한 학습이 필요함
- 본 교육연구단에서는 오실로스코프와 스펙트럼 분석기 같은 고성능 장비를 활용한 부채널 정보 수집 환경을 제공할 뿐만 아니라, 노이즈를 제거하여 유의미한 신호를 증폭시키기 위한 압축 및 정렬과 같은 기초 전처리 기법부터 주파수 필터 등과 같은 다양한 신호처리 기법에 대한 교육을 제공함
- 다수의 부채널 정보를 활용하는 통계적인 분석 기법부터, 하나 또는 소수의 부채널 정보를 활용하는 정교한 분석 기법에 이르기까지 수집된 부채널 정보로부터 암호 알고리즘의 비밀 키를 획득하는 다양한 분석 방법들을 학습하여 부채널 신호에 내재하는 정보를 추출하는 방법을 교육함
- 상기 교과목들을 통해 최근 이슈화되고 있는 통신 디바이스 내의 백도어 탐지 등의 역량을 습득한 전문인력을 양성할 수 있음
- 또한, 비밀 암호 알고리즘 등 블랙박스 모델의 암호화 장비에 대한 역공학을 통해 기존의

비밀 키를 획득하는 부채널 분석 방법의 공격자 가정을 완화시키는 기술을 학습함
- 본 교육연구단 내에선 사전에 각종 디바이스에서 얻을 수 있는 데이터를 포렌식 관점에서 분석하여 실제 법정에서 규명할 수 있도록 해석해 제시하는 연구를 진행함
- 포렌식 분석도구 사용 및 해석, 실제 디바이스에서의 데이터 추출 및 분석을 진행하는 등 디바이스 포렌식 기술에 대한 강의 커리큘럼을 제공함
- 첫번째로 디바이스 포렌식을 수행과정이 법적으로 인정받기 위한 원칙들을 교육함
- 두번째로, 다양한 디바이스에 대한 이해를 기반으로 디지털 데이터를 포렌식 분석할 수 있게 함
- 세번째로, 디바이스를 포렌식 분석도구를 활용하여 분석하는 방법을 교육함
- 네번째로, 신규 기기나 새로운 프로그램을 분석할 수 있도록 교육함
- 디바이스 포렌식에는 해당 디바이스에 대한 충분한 이해가 필요하여 PC나 스마트폰, 태블릿, IoT 기기 등의 디지털 기기에 대한 기본적인 이해를 위해 OS, 메모리, 저장공간 등의 전반적인 컴퓨터 이론을 교육함
- 다양한 기기의 동작과정 및 데이터 포맷을 사전적으로 숙지하도록 하며, 데이터를 추출 및 분석해 보면서 포렌식 분석 기술 향상을 도모함
- 디바이스별 데이터 추출 및 분석에 대한 교육을 마치면 EnCase, MD-RED 등의 상용 포렌식 분석 도구 사용 방법을 교육함
- 포렌식 분석도구를 통해 디지털 증거를 획득하는 것에서 더 나아가, 아직 포렌식 분석도구로 분석이 불가능한 신규 기기나 새로운 프로그램에서 얻을 수 있는 데이터를 직접 분석하는 방법을 교육하고 기존 포렌식 분석기술의 국산화 및 새로운 분석기술의 개발할 수 있는 인력을 양성함
- 다양한 암호 알고리즘 구현 및 설계, 그리고 실제로 동작하는 환경에 대한 취약점을 파악하는 등 디바이스에서 고려되는 기술 및 이슈에 대한 강의 커리큘럼을 제공함
- 디바이스 고속 설계 기술 전문가 양성을 위해, 첫 번째로, 동형 암호, 클라우드 서비스, 양자 내성 암호의 기초가 되는 수학적 원론을 학습함
- 두 번째로, 다양한 암호화 알고리즘을 소프트웨어상에서 구현할 수 있는 프로그래밍 기술을 교육함
- 세 번째로, 동형 암호, 클라우드 컴퓨팅, 양자 내성 암호 알고리즘에 대한 소프트웨어 구현 기술을 학습함
- 네 번째로, 소프트웨어로 구현된 동형 암호, 클라우드 컴퓨팅, 양자 내성 암호를 하드웨어상에서 구현할 수 있는 교육 프로그램을 제공함
- 마지막으로, 소프트웨어・하드웨어 상에서의 동형 암호, 클라우드 컴퓨팅, 양자 내성 암호에 대한 Codesign 기법을 이용해 최적화 방법론을 습득함
- 소프트웨어 구현 기술에 이어 하드웨어 구현 기술에 대한 교육을 마치면 각 환경에서의 최적화 방법론을 교육함
- 하드웨어-소프트웨어 통합설계(HW-SW Codesign) 기법을 이용하여 효과적인 설계 방법을 배우고 하드웨어-소프트웨어 분할 등의 설계 노하우를 함양함
- 소프트웨어 및 하드웨어 상에서의 고속 구현 기술을 학습하게 되면 동형 암호, 클라우드 컴퓨팅, 양자 내성 암호에 대한 디바이스 고속 설계 기술 개발로 교육을 확장함

▣ 암호기술 분야

▶대표문제 양자컴퓨팅 기술의 도래로 인한 기존 암호체계의 안전성 위협

- 안전한 양자내성암호의 개발 및 안전성 검증
- 양자내성암호의 안전하고 효율적인 구현을 통한 보안제품의 개발

▶참여교수: 강주성, 염용진, 김동찬

- 강주성 교수: 확률론 기반 난수성 연구 및 암호이론
- 염용진 교수: 안전성 분석 및 보안평가
- 김동찬 교수: 양자내성암호 설계 및 분석

▶주요 과목

구분	개요
기반 이론	- 해시함수와데이터인증(Hash Function and Message Authentication) - 병렬암호구현(Parallel Implementation of Cryptographic Algorithms) - 정보보안프로토콜(Information Security Protocols)
핵심 역량	- 공개키 암호분석이론(Cryptanalysis of Public-key Cryptosystem) - 암호소프트웨어구현(Implementation of Cryptographic S/W) - 대칭키암호분석(Topics in Symmetric Key Cryptanalysis)
심화 응용	- 난수성분석론(Analysis of Randomness) - 증명가능안전성론(Provable Security) - 암호모듈평가및검증(Evaluation and Validation Techniques for Cryptographic Modules)

▶전임교원 강의 계획 및 추진 방향

- 양자컴퓨터 시대에 대비하기 위한 암호기술로 양자내성암호가 활발히 연구되고 있으며 2024년에는 표준화를 통한 보급이 활성화될 것으로 예상되어 관련 전문인력의 양성이 필요함
- 양자내성암호의 수학적 기반원리부터 안전한 구현 및 활용까지 전반을 이해하며 산업에 적용할 수 있는 인력양성을 추진함
- 양자내성암호의 수학적 배경은 격자, 부호, 다변수함수, 해시함수, 타원곡선동종의 5가지로 분류되며, 이중 격자와 부호기반 암호가 표준으로 선정될 유력한 후보이므로, 이에 대한 안전성 분석과 구현기법에 대한 교육을 중점적으로 추진함
- 초연결사회에 필요한 보안 제품의 종류가 다양화되고 있으며, 관련 제품의 안전성에 대한 평가・검증기술의 연구개발이 필요하므로, 관련 기준 및 제도의 이해를 바탕으로 요소기술에 대한 전문적인 교육을 실시함
- 암호시스템의 안전성에 필수적인 난수발생기의 설계, 분석, 평가기술의 체계적인 교육을 통해, 불완전한 난수로 야기될 수 있는 디바이스 보안문제를 방지함
- 상용 보안시스템에 내장된 표준 난수발생기에 대한 증명가능안전성 연구 및 통계적 난수성 분석 등을 적용할 수 있는 역량을 갖추도록 함

▣ AI응용 분야

▶대표문제 : 인공지능 기술의 비약적 발전 이면의 허점 및 네트워크 안전성 위협

- 인공지능 기술의 적용에 따른 보안문제 및 인공지능 기술을 활용한 보안기술 개발

- 인공지능 기반한 적대적 공격에 대한 방어기술 개발
- 자율성장 환경에서의 딥러닝 모델을 활용한 인공지능 시스템 설계 기술

▶참여교수: 최은미, 윤상민

- 최은미 교수: 데이터마이닝, 분산지능화 시스템
- 윤상민 교수: 인공지능 기술, 빅데이터 분석 및 적대적 공격 / 방어 시스템

▶주요 과목

구분	개요
기반이론	- 데이터마이닝(Data Mining) - 인공지능과 보안 이론(AI and Security)
핵심역량	- 모델기반시스템설계(Model-based System Design) - 자율성장 인공지능 특론 (Advanced Self-supervised AI)
심화응용	- 인공지능 융합 기술 특강 (AI Convergence)

▶전임교원 강의 계획 및 추진 방향

- 자율 성장 인공지능 교육을 위하여 딥러닝을 비롯한 다양한 인공지능 기술에 대한 교육을 통하여 기계학습에 대한 이해도를 높일 수 있도록 함
- 자율성장 인공지능 기술을 위하여 self-supervised learning과 관련된 다양한 최신 기술에 대한 이해 및 분석을 통하여 generative model, low-density separation, graph-based model, heuristic model을 활용한 사회문제 해결을 위한 프로젝트 기반 교육 과정 마련함
- 학생 스스로 다양한 센서 네트워크를 구성하고, 발생한 데이터에 대한 수집, 저장, 분석과 관련된 일련의 과정에 대한 이해를 통하여 스스로 학습하고 이해할 수 있는 다양한 인공지능 모델을 개발함과 동시에 시스템에 적용함
- 딥러닝 모델에 대하여 개발자 스스로 이해할 수 있도록 설명가능한 인공지능 기술에 대한 지식을 습득함과 동시에 다양한 데이터를 기반 모델 구현 및 분석에 대하여 교육함
- 설명 가능한 인공지능 모델을 통하여 적대적 공격에 대한 다양한 모델을 비교 분석하고, 적대적 공격에 대한 효율적인 방어 기술을 개발하고 지능형 시스템에 실제적으로 적용함으로서 활용 가능성 및 문제점 분석할 수 있도록 구성함
- 자율 상장 환경 분산 AI 기술 및 보안 기술을 통하여 swarm intelligence 및 optimization, domain context analysis 및 모델링, 분산 시스템환경 취약점 분석 맞 방어기술을 교육함
- 실제적으로 사회에 활용되는 데이터를 기반으로 한 실습 및 분석을 통하여 학생들 스스로 사회 문제에 이해할 수 있도록 함
- 지능형 시스템 환경에서 꾸준히 취합되는 다양한 데이터를 기반으로 문제 해결 능력을 향상함과 동시에 지속적으로 생산되는 데이터에 대한 문제를 분석하는 역량을 교육함
- 지속적으로 성장하는 인공지능 모델을 교육, 연구함으로서 학생들의 인공지능 및 정보보안 기술에 대한 이해도를 동시에 높일 수 있는 연구 및 교육 구조를 마련함

2. 인력양성 계획 및 지원 방안

2.1 교육연구단의 우수 대학원생 확보 및 지원 계획

▣ 우수 대학원생 확보 노력

▶대학본부의 국고 예산 대비 20% 현금매칭 등의 지원 계획

- 우리대학은 국내외의 대규모 연구중심대학들과 비교했을 때 대학원의 학과나 전공단위의 규모가 상대적으로 작고, 연구 및 교육 인프라도 비교열위에 있는 것이 사실임
- 그럼에도 우리대학은 그동안 선택과 집중의 일관된 원칙에 입각하여 '특성화' 분야를 선정하여 집중적으로 자원을 배분함으로써 연구와 교육의 경쟁력을 강화해 왔으며 일부분야에서는 국제 경쟁력을 확보함
- 이제는 이들 특성화 분야를 해당 틈새시장에서 세계적 수준의 연구 및 교육의 허브로 발돋움할 수 있도록 집중 육성할 시점에 와 있음
- 국민대학교의 정보보안암호수학과 및 소프트웨어융합대학 학부생을 대상으로 '학부연구생' 제도 시행을 통해, 학부생들이 BK 교육연구단의 연구 프로젝트에 참여하여 정보보안 분야의 관심을 유도하고, 책임감과 전문성을 갖춘 학생으로 육성할 계획임
- 우수 대학원생 확보를 위해 본 교육연구단은 2017년, 2018년 본교인 국민대학교에서 진행한 '4차산업혁명 Festival'에 참여하여 본 교육연구단의 성과 및 대표 연구 내용을 국민대학교 학생들에게 소개 및 홍보를 진행하였으며, 지속적인 우수 신입생 유치를 위한 본 교육연구단의 대내외에 홍보할 계획임
- 4차 산업혁명 특성화분야 성과확산을 위한 '국민대학교 4차 산업혁명 Festival을 개최하여 미래 산업 및 사회의 다양한 문제와 해결방안을 찾는 과정을 지속할 예정임
- 2017 국민대학교 4차 산업혁명 Festival : 특성화분야 역량을 비특성화 학과로 확대함과 동시에 교내 구성원 공감 및 4차 산업혁명 연계 프로젝트 가능성을 모색했으며, 개최결과로서 4차 산업혁명 관련 강연 및 상설전시관 운영을 통해 1,008명이 참가하였음
- 2018 국민대학교 4차 산업혁명 Festival 시즌2 : 특성화 교육 성과 확산' 및 '창업 성과 및 문화 확산'을 위해 4차 산업혁명 시대를 선도하는 교육 콘텐츠 전시/체험 및 공연을 진행하였고, 교내 구성원 및 외부인 1,500여명이 참가하였음
- 본 교육연구단은 정보보안암호수학과 전체 학부생을 대상으로 연구실별 성과와 연구 내용을 소개하는 랩투어와 국민암호 페스티벌을 개최하여, 평소 학부생들이 가지고 있던 진학 관련 고민과 연구 과정에 대한 궁금증을 해소하는 장을 마련하여, 지속적인 우수 신입생을 유치할 수 있도록 하는 전략을 마련함
- 본 교육연구단은 2018년 본교 국민대학교에서 진행한 '랩투어데이'에 참여하여 학부생을 대상으로 랩별 성과 및 연구내용을 소개하고 진학관련 고민 및 궁금증에 대해 해소 할 수 있도록 상담을 진행함
- 우수 대학원생 확보를 위해 정보보안암호수학과 내에 부채널 분석 동아리, 난수 분석 동아리, 디지털 포렌식 동아리를 신설 및 운영에 지원함
- 본 교육연구단은 교수들이 수행 중에 있는 R&D 과제를 경험할 수 있도록 학부생들에게 지속적으로 참여기회를 주고 있으며, 특히 학기를 마치고 방학 동안에 학부생들에게 연구과제를 진행 및 발표를 통해서 연구실과 정보보안 및 정보 지능화의 응용 어플리케이션 소프트웨어 시스템 분야에 관심을 유도하고 있음
- 2008년부터 학부 우수 졸업 예정자 중에서 학사·석사 연계 과정 입학생을 선발함으로써 본교 출신 우수 학부생이 학부 졸업과 동시에 대학원에 입학해 석사과정을 이수할 수 있도록 제도를 운영하고 있음
- 이 제도는 학부 3학년에서 4학년으로 올라가는 학생 가운데 정보보안에 관심이 있는 학생

을 대상으로 정보보안 분야에 진학할 수 있도록 만들어진 과정으로, 학생들이 토론회 등에 참여할 수 있도록 교육 환경을 제공하고 대학원 입학 전에도 학생이 관심을 갖는 분야의 연구나 과제에 참여할 기회를 부여함
- 특히, 학생들에게 학습과 연구에 필요한 장소를 지원함으로써 학부 과정부터 체계있고 집중도 높은 사전 학습 단계를 밟을 수 있는 기회를 부여함
- 대학원 과목을 학부생이 사전에 이수할 수 있도록 하여 해당 학생이 석사과정이나 박사과정 진학 시 이수 학기를 단축할 수 있는 수업연한 단축 제도를 시행하고 있어, 본교 출신 학생으로 하여금 대학원 진학할 수 있도록 격려하고, 앞으로도 학부 졸업생들이 더욱 용이하게 대학원에 진학 할 수 있도록 제도를 꾸준히 개선할 예정임

▣ 우수 대학원생 지원 노력

▶우수 대학원생 확보를 위한 국민대학교 재정 지원
- 국민대학교 일반대학원은 우수한 신입생을 적극 유치하고자 ‘성곡장학금’ (수업료 전액), ‘교수 추천 우수 신입생 장학금’ (수업료의 50 % 지원), ‘교육 조교 장학금’ (수업료의 50 %), ‘연구 조교 장학금’ (연구 조교 A: 수업료의 100 %, 연구조교 B: 수업료의 70 %) 등 다양한 장학금 지원을 통해, 인재 확보, 연구 기회, 교육환경 제공에 크게 기여함
- 실무에 뛰어난 전문 인력을 양성하기 위해 정보보안 실무 업무에 필요한 다양한 교육 기회를 부여하고, 상용화하는 데 필요한 여건을 지원하여 창업 기회를 넓힐 예정임
- 교육연구단은 국내 주요 액설러레이터 (CCVC 밸류업센터, 아산나눔재단 정주영창업센터 등과 기협의)와 협력하여 자질이 우수한 학생이나 팀에게 학내 보육 수준을 넘어선 창업 멘토링 제공과 세계 시장 진출 지향형 보육 환경을 지원할 계획임
- 성과나 실적이 우수한 참여 교수와 대학 동문들이 (가칭) 국민엔젤펀드를 결성하여 자금 지원을 실행함으로써, 현재 모태펀드(한국벤처투자)나 아산나눔재단 등이 운영하는 엔젤 매칭펀드 등과 연계하여 학생들의 연구와 학업을 지원할 예정임

▶우수 대학원생 확보를 위한 국민대학교 연구 공간 지원
- 교육연구단의 원활한 연구수행을 위하여 2014년 10월 신축한 산학협력관에 교육연구단장 또는 사업 참여교수의 요청에 따라 연구공간을 다음과 같이 배정하여 지원하고 있음
- 미래 금융보안 전문인력양성 교육연구단: 산학협력관 203-1호(96㎡), 301호(40㎡), 306호(48㎡)을 활용하고 있으며, 이 공간은 BK21 FOUR 사업에서도 계속 활용할 계획임

▶우수 대학원생 확보를 위한 국민대학교 행정 인력 지원
- 각 교육연구단에 전담 행정인력을 1명씩 채용할 수 있도록 지원하고 있으며, 2019년 8월 기준으로 6개 교육연구단(팀) 중 4개 교육연구단(팀)이 전담 행정인력을 임용하고 있음
- 산학협력단 내에서는 BK21플러스사업 담당하는 협약 담당자 1명(정규직), 정산 담당자 1명(계약직)을 배정하여 행정업무를 지원하고 있음
- 지식재산 권리화, 교육 및 기술사업화 활성화를 위해 산학협력단은 변리사 1명을 2017년 5월 별도로 채용하였으며, 특허 및 기술이전 등 사업성과 관리를 지원하고 있음

▶우수 대학원생 확보를 위한 국민대학교 연구인력 지원

- 교육연구단장 및 참여교수에 대한 지원으로 우리 대학 ‘BK21 FOUR 사업운영에 관한 규정(안)’에 의거 예산 편성 및 집행에 대한 권한, 연구인력 인사권에 대한 권한, 학사운영상의 권한 등을 교육연구단장에게 부여할 계획임
- 교육연구단장 또는 참여교수에게 아래와 같이 사업수행학과 주임교수 직위를 부여함으로써 BK21 FOUR 사업을 중심으로 한 대학원 운영이 가능하도록 지원 계획임
- 신진연구인력에 대한 지원으로 우리 대학 전임교원을 대상으로 지원하는 ‘국고 지원 연구과제 제안서 작성 보조금’을 신진연구인력에게도 지급함으로써, 국가연구개발사업 등 정부지원 연구과제 신청에 보다 적극적인 자세를 갖게 함으로써 연구과제 채택 가능성을 제고할 계획임
- 또한 산학협력단에서는 국가연구개발사업 신청시 유망기술을 발굴하고 이에 맞게 사업 계획을 수립할 수 있도록 외부전문가를 초빙하여 강연을 실시할 계획임
- 대학원생에 대한 지원으로 우리대학 대학원 주요 장학제도인 ‘교수추천 우수 신입생 장학금’(수업료의 50% 감면), ‘교육조교 장학금’(수업료의 50% 감면), ‘연구조교 및 산학협력 조교 장학금’ (수업료의 70, 100% 감면), ‘이공계전일제 박사과정 장학금’(수업료 100% 감면) 등을 배정할 때, BK21 FOUR 교육연구단장이 학과장을 역임하므로, BK21 FOUR 사업 참여 대학원생을 우선적으로 배정할 계획임
- 본 사업개시 학기부터 ‘BK21 FOUR 장학금’을 신설하여 본 사업에 참여하는 전일제 재학생을 대상으로 ‘정부장학금’을 수령하지 못하는 대학원생에 대해 우리 대학 대응자금을 재원으로 하여 별도로 장학금을 지원할 예정이며, 본 장학금에 대한 대상자 선발 권한은 전적으로 교육연구단장에게 부여할 계획임
- 본교 학사과정에서 대학원 교과목을 6학점 이상 수강하여 소정의 학점을 취득한 석사과정 또는 석・박사 통합과정 입학자, 재학 중 저명한 국제학술지(SCI, SSCI, SCIE, A&HCI, SCOPUS)에 논문을 100% 게재한 자, 학・석사 연계과정으로 선발된 자에 대해 1학기 수업연한을 단축할 수 있도록 하고 있음
- 사업 참여 대학원생에 대한 본교 기숙사(생활관) 입주 우선 배정을 요청하여, 2016학년도 4명, 2017학년도 9명, 2018학년도 14명, 2019학년도 12명의 대학원생이 우리 대학 생활관에 입주하여 본 사업이 원활하게 수행되고, 참여 대학원생의 연구성과가 제고될 수 있도록 운영 중인 제도를 지속적으로 운영하여, BK21 FOUR 사업에도 운영할 계획임
- 해외 우수 대학원생 유치를 위한 ‘해외 우수연구인력 유치 지원사업’ 운영을 위하여 석사과정 1년, 박사과정 2년, 석・박사통합과 정 3년간 등록금 전액과 기숙사비의 50%, 매월 60만원의 생활비를 지원하고 있는 제도를 바탕으로, 본 교육연구단에 우수한 해외 대학원생 유치 노력을 지속할 예정임
- 국민대학교 본부는 본 교육연구단에 속한 외국계 우수 유학생에게 학교 기숙사를 우선해 배정하기로 했으며, 이들을 우선해 조교로 배정함으로써 국제화에 전력을 다 할 예정임
- 지원받은 해외 우수인력은 석사과정 1편, 박사과정 2편, 석・박사 통합과정 3편의 국제우수학술지(SCI, SSCI, A&HCI 등) 게재를 의무화하여 우수한 연구실적을 얻을 수 있도록 격려할 예정임
- 해외 우수 인력을 유치한 우리 대학 전임교원에게도 외부연구비 수주 등 의무사항을 부여하고 있고, 기숙사비와 생활비의 50%를 지도교수가 부담하도록 제도를 운영할 예정임

2. 인력양성 계획 및 지원 방안

2.2 대학원생 학술활동 지원 계획

▣ 우수 대학원생의 창의적 학술활동을 위한 창의적 연구 환경 조성 및 제도 마련

▶창의적 연구 환경 조성

- 교육연구단 소속연구원 전용공간 구축 및 연구 장비 지원을 통해 연구원 간 원활한 의사소통 및 장비의 효율적 활용이 이루어질 수 있도록 유도함
- 국내·외 전문가 초청 강연 세미나 및 심포지엄 개최하여 전공 분야 최신 연구주제 집중특강 및 교수/국내외전문가/대학원생 간 3자 간담회 등을 통해 연구 활동과 학문에 대한 다양한 경험과 열정을 공유함으로써 대학원생에게 미래가 요구하는 과학 인재로 성장할 기회를 제공할 것임
- 최신 연구정보를 획득하고 국제적 연구 감각을 익힐 수 있도록 창의적이고 도전적인 우수 대학원생을 선발하여, 공동연구 협력을 맺은 해외 연구소 및 대학에 장기연수를 보낼 것임

▶대학원생 주도 연구 및 창의적 연구 활동 지원 방안 마련

- 기존의 교수-대학원생간의 도제식 교육제도에서 벗어나 대학원생 스스로 문제에 사회 문제에 대한 문제를 제기함과 동시에 이를 주도적으로 수행할 수 있도록 지원하도록 함
- 대학원생 주도의 문제 제기 및 해결 방안을 마련함으로서 창의적인 연구 방법 및 활동에 대한 지원 및 프로젝트 수행을 적극적으로 지원함

▶연구몰입 및 연구 의욕 고취를 위한 제도 마련

- 국내·외 우수 대학원생 유치와 교육/연구의 최적화를 위해 장학금 지급함(등록금 50% 이상 장학금 보장)
- SCI급 국제학술지에 논문을 게재한 대학원생에게 학술지 Impact Factor 및 주저자 여부에 따라 성과보수를 차등 지급함
- SCI급 국제학술지에 논문을 100% 게재한 대학원생에게 수업연한을 한 학기 단축함

▶연구 수월성에 중점을 둔 학위취득 평가 방법 도입

- 논문의 질적 향상을 위해 해당 연구 분야 상위 20% 이내 저널 1편 이상 혹은 상위 40% 2편 이상을 학위 취득요건으로 할 것임(2차년도 입학생부터 순차적 적용)
- 논문 출판 실적 외에 논문 심사 위원회에서 학위대상자의 창의성, 문제해결 능력 및 전공분야 전문가 자질 등을 종합적으로 판단하여 졸업 자격을 결정할 것임

▣ 우수 대학원생 지원 노력

▶우수 연구실적에 대한 인센티브

- 학술활동 결과물의 질적 향상의 동기부여를 위해 SCI 저널에 출판된 논문 저자에 대한 인센티브를 부여함으로써 연구 활동 결과물의 질적 향상을 격려함
- SCI 저널의 경우, 해당 저널에서 출판한 것으로 우수한 실적으로 판단하고 인센티브를 부여하고, SCI 논문의 경우, 출판된 저널의 IF(피인용지수)를 기준으로 연구 결과의 우수성을 판단하여 인센티브 차등 지급할 계획임
- IF 2.0 미만의 저널에 출판된 논문에 대해서는 대학원생을 대상으로 편당 최대 50만원을 기준으로 논문 저자 수에 따라 나눠 지급할 계획이고, IF 2.0 이상의 저널에 출판된 논문에 대해서는 대학원생을 대상으로 편당 최대 100만원을 기준으로 논문 저자 수에 따라 나눠 지급할 계획임
- SCI 논문 출판 외에도 유명 국제 학회에 제출된 논문 또한 우수한 학술활동의 결과물로 판단할 수 있으며 해당 결과에 대한 인센티브를 부여함으로써 연구활동 결과물의 질적 향상을 야기할 것으로 기대함
- USENIX, ACM CCS, CHES 등 정보보안 분야에서 유명한 국제 학술대회에 발표한 논문을 우수한 실적으로 판단하고 인센티브를 부여할 계획임
- 유명 국제 학술대회에 발표한 논문에 대해서는 대학원생을 대상으로 편당 최대 50만원을 기준으로 논문 저자 수에 따라 나눠 지급할 계획임

▶우수 학술활동에 대한 인센티브

- 상기 해당하는 저널 혹은 학술대회에 논문이 선정되지 않은 대학원생들에 대해서도 출판 혹은 발표한 논문의 수가 기준을 초과한 대학원생들에 대해 성실함을 인센티브를 지급하여 꾸준한 학술활동을 진행할 동기를 부여할 계획임
- 해당 기준은 석사과정 혹은 박사과정(석박사통합과정 포함)에 따라 기준을 달리 적용하며 해당 기준을 초과한 실적을 달성한 학생들에 대해 인센티브를 지급함
- 석사과정은 과정 내 학술대회 5편 혹은 저널 2편 이상 작성한 경우 소정의 인센티브를 제공하여 학술활동을 이어 진행할 수 있도록 동기를 부여함
- 박사과정(석박사통합과정 포함)은 과정 내 학술대회 10편 혹은 저널 5편 이상 작성한 경우 소정의 인센티브를 제공하여 학술활동을 이어 진행할 수 있도록 동기를 부여함

▣ 국내・외 전문가와의 긴밀한 협력을 통한 글로벌 인재 양성 방안 마련

▶정보보안 분야의 전문가 초빙을 통한 글로벌 역량 강화 및 네트워크 강화

- 국내・외 유명 논문 저자 혹은 연구소 및 기업체의 전문가를 초빙하여 국외 연구 동향 및 각종 이슈에 대해 습득할 수 있도록 세미나를 개최할 예정임
- 전문가의 기준은 정보보안 분야의 경력이 5년 이상이며 초빙 당시 기준으로 지속적으로 정보보안 분야에 대한 연구 활동을 진행하고 있는 사람으로 선정함

- 전문가와의 사회 문제에 대한 심도있는 논의 및 해결 방안을 마련할 수 있도록 내용 전달 위주의 세미나에서 벗어나 프로젝트 및 문제 해결 중심의 토론 및 세미나를 통하여 대학원생들의 문제 해결 능력을 강화할 수 있는 방안 마련

▶온·오프라인을 통한 국내, 국제 공동연구를 진행 환경 제공

- 오프라인으로 해외 교류 진행에 필요한 항공 운임비 및 체류비를 지원하여 원활한 국제 공동 연구가 진행될 수 있도록 지원할 계획임
- 항공 운임비 및 체류비는 본교 국외출장 기준을 적용하여 지급하도록 할 계획임
- 해외 교류를 통해 연구 결과물 혹은 해외 산업체의 업무 프로세스 경험을 얻을 수 있도록 진행할 계획임
- 학술활동을 목적으로 한 출장(학술대회, 경진대회 등)에서 우수한 성적을 거뒀을 경우, 차기 해외 연수 또는 해외 저명 학회 참가를 지원하여 우수한 성적을 얻을 수 있도록 동기부여할 계획임

▶오픈 소스 소프트웨어 활동 지원을 통하여 관련 연구 분야 연구자들과의 네트워크 강화

- GitHub를 통하여 개발된 자율 성장 인공지능 모델을 공개하여 다양한 연구자들과의 교류를 활성화할 수 있도록 지원함
- 정보보안 소프트웨어 기술을 공개함으로서 관련 연구 분야의 활성화 및 사회적 문제 해결에 기여할 수 있도록 지원함
- 정보보안 소프트웨어를 공개함으로서 다양한 분야에 적용할 수 있는 기회 마련함
- 연구를 통하여 개발된 소프트웨어를 공개함으로서 다양한 사회 문제 해결에 도움을 줄 수 있는 환경을 구축함과 동시에 학생들과 외부 전문가들과의 활발한 활동 및 교류를 유도할 수 있도록 함

▶산학연 공동 연구 추친 및 해외 기관 파견을 통하여 글로벌 역량 강화

- 주기적으로 정보보안 워크숍을 통하여 기업, 연구소, 학계 연구자들과의 교류를 통하여 사회에서 발생하는 문제에 대한 공유 및 해결방안 마련 워크숍 운영함
- 지속적인 워크숍을 통하여 사회문제에 대한 데이터 및 인공지능 모델을 공유하고 해결하기 위한 방안 마련함
- 정보보안 기술을 활용한 다양한 사례를 기반으로 한 국제 학술대회에서 관련 결과물에 대한 발표 및 참석에 대한 지원함

▶정보보안 및 지능형 시스템에서의 표준화 연구

- 초연결시대가 현실화되면서 신기술 혹은 새로운 산업에 대한 국제표준을 선점하기 위한 각국의 준비가 시작된 만큼, 사물인터넷 국제표준화를 수행하는 ISO/IEC JTC 1/SC 41(사물인터넷 및 관련 기술) 회의에 정기적으로 참여할 수 있도록 재정적으로 지원하여 초연결사회를 위한 문제해결형 정보보안 관련 선진 연구 개발 동향을 파악 및 현장에서 실무 경험을 체득할 수 있는 기회를 제공할 예정임
- 참여 대학원생들이 연구 분야의 국제학술대회 및 포럼 등과 같은 저명한 학술교류 네트워크에 참석하도록 함으로써, 연구 결과 교류 및 폭 넓은 논의를 통해 초연결사회에서 요구되는 문제를 발굴 및 해결 할 수 있는 실전 감각을 익힐 수 있도록 적극 지원함

2. 인력양성 계획 및 지원 방안

2.3 우수 신진연구인력 확보 및 지원 계획

▣ 우수 신진연구인력 확보 및 지원을 위한 대학본부의 발전전략 성립

- 우리 대학은 선택과 집중의 일관된 전략 방향에 입각하여 '특성화' 분야를 선정하여 집중적으로 자원을 배분함으로써 연구와 교육의 경쟁력을 강화하여, 해당 틈새시장인 초연결사회를 위한 문제해결형 특성화 분야에서, 작지만 강한(Small Giant) 세계적 수준의 연구 및 교육의 허브로 발돋움할 수 있도록 집중 육성하고자 하는 의지가 있음
- <KMU 2030+>에서 제시한 5대 발전전략과 대학원의 5대 발전전략을 세움으로써, '초연결형 융복합 교육체계 확립'은 '미래유망분야 발굴・육성'과 '대학인프라 정비・확충,' 그리고 '요구중심 교육체계' 의 혁신 지표 방향을 확립함
- 2020연도 전년 대비 전임교원 수를 51명 증원하여 전임교원 확보율을 75.45% (2020년 기준)로 꾸준히 증가율을 설정하여 계획을 수립하고 있음. 특히, 우수 교원 유치를 위한 제도 개선 계획으로, 신진연구인력 임용 트랙 신설, 국민*스타 교수 임용, 우수 연구자 채용을 위한 연구, 산학협력 업적 기준 신설, 연구 우수 교원 인센티브 & 책임시수 감면, 사업단과 학과간 공동 교수초빙 제도를 시행 진행하고 있음

▣ 우수 신진연구인력 확보 및 지원을 위한 조직 체계 재설정

- 산학연구부총장 (신설): 대학원, 산학협력단, LINC+사업단, 그리고 창업지원단을 산학연구부총장에게 소속시켜 대학원의 연구역량을 극대화하고 이를 실용화・사업화하여 국제 경쟁력을 갖춘 연구중심대학으로 발전시키는 새로운 역할을 부여하고, 이를 통한 신진연구인력 확보와 연구 및 교육역량 강화를 위한 조직과 지원체계를 확보함
- 국민*미네르바 교육원 (신설): 특성화 영역이나 연구집중학과의 교수진이 커리큘럼의 설계를 자문하고, 첨단 융복합 연구주제와 관련된 강의를 통해 산학협력 네트워크를 강화함
- 신진연구인력으로 임용되는 교원을 대상으로 중장기 연구 프로젝트 수행 수월성을 확보하고, 연구 연속성 보장하기 위해 정기평가를 거쳐 우수 연구인력을 전임교원으로 임용하는 제도 도입함

▣ 산학협력 친화형 교원인사제도 운영

▶교원업적평가제도 개편

- 산학협력 실적 반영을 통한 대학 전 교원으로의 확산: 승진·승급·재임용 시 산학협력 관련 점수만으로 승진 등이 가능하도록 산학협력 실적을 100% 대체 인정하고, 특별승진 기준 산학협력점수(연구, 교육, 봉사) 전 분야에서 가능하도록 확대함
- 오픈소스 SW활동을 SCI급 논문실적으로 대체하도록 국제필수 신규 지정함(2016.10.01.)
- 교원업적평가 시 SCI급 논문 1편(100점) 대비 산학협력 실적은 전 계열에 적용 되고, 평가항목별 배점을 모두 동일하게 인정 가능하며, 특히 기술이전(1천만 원)의 경우 SCI급 대비 비율을 73%수준까지 지속적으로 확대함
- K-MOOC 강좌 개발 및 운영 항목, 4차 산업혁명 교과 수업계획서 제출 항목 신설, 수업계획서-동영상 예고편 수록 항목 신설, 선진교수법(FL, PBL 등) 교과목 개발 항목 신설, 팀팀Class 교과목 개발 및 운영 항목 신설, 시민참여활동 교과목 개발 및 운영 항목 신설, 강의개발 및 학습방법혁신 관련 업적항목 등을 신설함(2018.03.01.)
- 교내 융합교과목 프로그램인 팀팀ClassTM 관련 융합연구논문의 장려를 위하여 연구부문 평가항목 배점의 30%를 가산하여 인정함(2018.09.01.)

▣ 연구중심형 연구지원 체계 및 연구지원제도 개선 운영

▶산학협력단 개편

- 연구중심대학으로 도약하기 위한 연구지원 체계 구축을 위해 연구지원 및 산학협력 활성화를 위한 산학협력단 조직 개편함(2015.11.)
- 연구기획, 연구관리 및 성과확산까지 이어지는 전주기적 R&D 관리 기구로서의 역할을 재정립하고 대학의 특성화 역량과 기업의 수요(needs)를 매칭하고 양자 간 관계를 발전시키는 기능을 수행할 수 있도록 기존 2개 부서에서 4개부서로 조직을 개편함

▶연구지원제도 개선

- 연구역량강화 및 활성화를 위한 연구지원제도 개선 및 신규 제도 시행을 위해 아래와 같은 연구지원 제도를 마련하여 운영함
- 학술대회 참가지원에 관한 내규 개정하여(2017.03.01.) 지침으로 시행되던 참가 지원사항을 내규로 규정하고, 참가지역에 따라 지원금을 50만원까지 차등 지급함
- 논문게재료 지원에 관한 내규 개정하여(2017.03.01.) 논문게재료의 효율적 지급을 통한 연구역량강화 및 예산집행의 효율성을 제고하고자 지원대상 학술지를 국내는 한국연구재단 등재(후보)지 이상, 국외는 SCOPUS 이상으로 명확히 규정하고, 지원금을 국내 70만원, 국외 100만원 이내로 세분화하여 운영 중임
- 부설연구소 및 연구원 설립 운영규정 개정하여(2017.03.01.) 학술회의 지원금 기준을 신설함으로써 부설연구소의 학술회의 개최를 활성화 하고자 함
- 연구개발능률성과급 지급 지침 신설하고(2018.03.01.) 교원의 연구 활동 독려 및 우수 연구성과 창출을 위하여 성과급 지급에 대한 지침을 신설하고 매년 산학협력단 간접비에서 평가에 의해 차등 지급함
- 연구책임자 연구활동 지원금 제도 신설하고(2018.12.01.) 연구자의 연구활동을 지원하기 위한 제도 신설함
- 교내 융복합 연구팀 구성을 위한 기획비 지원제도 신설하고(2017.12.) 교내 구성 원간의 융복합 연구 활성화를 위한 기획비 지원함
- 교내 융복합우수연구센터 육성지원사업 재시행하여(2018.04) 이공계열을 중심으로 목표 중심의 집중적이고 유기적인 연구집단을 구성하여 4차 산업혁명에 대비한 창의적인 연구개발 및 인재양성에 전념토록 함으로써 대형국책과제 유치를 위한 기반을 조성하고자 함
- K-LAB 연구소개서 지원사업 신설하고(2019.02.) 우수연구실소개 및 교원의 연구 포트폴리오제작을 지원하는 사업을 운영 중임
- 학부생 연구인턴십 과정(2019.07)은 학부생에게 방학 중 연구실 인턴 경험을 통하여 연구프로젝트에 대한 이해도를 높이고 대학원 진학 등 진로 탐색의 기회를 제공하여, 신진연구자가 우수한 대학원생을 육성하여 연구활성화를 제고하고자 함
- 해외권리화 지원프로그램을 마련하여 우리대한 보유 우수 기술에 대해 연간 상·하 반기로 구분하여 미보완 기술에 대한 재도전 기회를 부여하고 있음
- 시제품 제작 지원사업으로 대학 우수 기술의 상용화 지원을 위한 시제품 제작 지원 프로그램과 우수특허 창출을 위한 특허설계 지원 프로그램 운영하여 대학 우수 기술 확보를 위한 시장 및 동향조사 지원과 유효 기술의 특허 권리화 지원하고 있음

▣ 연구몰입 환경 인프라 구축 및 제도 운영

▶연구지원 제도 개편

- 신진연구자의 연구몰입 환경 조성을 위한 인프라 구축 및 제도를 마련하여 시행하고 있음
- 연구실 및 부설연구소 행정인력 운영방안 마련하여(2017.09.01.) 국가연구개발사업 수행 연구책임자의 행정업무 부담을 최소화하기 위하여 행정 인력 지원하고 있음
- 산학협력단 외부연구비 관리 매뉴얼 제작하여(2018.05.14.) 내・외부 각종 규정 및 서식을 한권으로 통합하여 연구자에게 연구비 신청의 편의성을 제공하고 있음
- 산학협력단 차세대 연구행정시스템 신규 개발 계획을 수립하고(2019.04.) 대학 차세대 시스템 개발과 연계하여 데이터간・업무간・시스템간 정보의 연결성 강화 및 연구자가 연구에만 전념할 수 있는 친 연구시스템 운영 중임

▶미래 지향적 지원체계 운영

- 대학의 혁신비전 및 중장기 발전계획 <KMU Vision 2030+>을 수립하고 우리대학의 교육철학인 공동체정신과 실용주의를 바탕으로 비전을 실현하고 4차 산업혁명 시대가 요구하는 ‘창의적 융합인재’ 양성을 위해 “세상 을 바꾸는 TEAM형 인재 양성 기반구축 및 확산”을 발전목표로 교육・연 구・산학협력의 3대 영역별 혁신전략을 구체적으로 수립함
- 우수한 산업문제 해결을 위한 기술사업화를 위해 교원창업 및 기술사업 통합지원 플랫폼 구축하고 진로 및 취・창업 총괄기구인 “대학일자리본부” 신설하여 진로지도 및 취・창업 지원의 One-stop서비스와 기능적 연계 등을 위해 경력개발지원단과 총장직속 기구인 창업지원단을 총괄하는 대학일자리본부를 신설하여 체계적인 취・창업 지원체계 구축하고, 대학기술지주회사(KMU Holdings) 설립 및 운영하여 대학주도의 기술사업화 및 대학 창업펀드 조성을 위한 자립화 기반을 구축함
- 교원의 창업 및 창업지원 활동 강화를 위해 대학의 기술과 인프라를 기반으로 지속가능한 기업으로의 교원 창업이 이루어질 수 있도록 창업 겸직 규정과 프로세스를 혁신하고, 기술지주회사 및 사업화지원 프로그램을 통하여 신임교원의 창업을 격려할 계획임
- 국민대학교는 매년 본 교육연구단의 업무를 전담하는 행정직원을 지원할 예정이며, 이를 통해 본 교육연구단의 교원과 재학생들이 행정업무에 얽메이지 않고, 자유롭게 연구에 집중 할 수 있도록 운영할 계획임
- 국민대학교는 신진연구인력이 우수한 신입생을 적극 유치할 수 있도록 성곡장학금(수업료 전액), 교수추천우수신입생 장학금(수업료의 50% 지원), 교육조교 장학금 (수업료의 50%), 연구조교 장학금 (연구 조교 A: 수업료의 100%, 연구조교 B: 수업료의 70%) 등 다양한 장학금 지원을 지속할 것임
- 신임교원이 새로운 연구실을 마련하고, 대학원생을 유치를 지원하기 위해 대학원 과목을 학부생이 사전에 이수할 수 있도록 하고, 해당 학생이 석사과정이나 박사과정 진학 시 이수 학기를 단축할 수 있도록 수업 연한 단축 제도를 시행하여, 본교 출신 학생으로 하여금 대학원 진학에 높은 관심을 가질 수 있도록 지원함

▣ 교육연구단의 우수 신진연구인력 확보 및 지원

- 우수 신진연구인력인 박사후 과정생 및 계약교수를 적극적으로 유치하고, 연차에 따라서 2-3명을 단계적으로 채용하여 산학협력 친화와 사업단의 연구 능력을 함양하도록 함
- 신진연구인력의 안정적인 학술 및 연구 활동을 위하여, 연구논문지원사업, Moving Target 인센티브 제도, 연구 우수교원 인센티브 제도 등을 제공하며, 연구활동이 우수한 신진 연구인력에게 연구 및 교육 기회를 확대하여 제공함

3. 참여교수의 교육역량 대표실적

<표 2-1> 해당 산업·사회 문제 해결분야 문제해결을 위한 참여교수의 교육역량 대표실적

<table>
<tr><td rowspan="2">연번</td><td>참여교수명</td><td>연구자등록번호</td><td>세부전공분야</td><td>대학원 교육관련 대표실적물</td><td>DOI번호/SBN/인터넷 주소 등</td></tr>
<tr><td colspan="5">참여교수의 교육관련 대표실적의 우수성</td></tr>
<tr><td rowspan="2">1</td><td>김종성</td><td>10182694</td><td>정보보호</td><td>논문</td><td>https://doi.org/10.1007/s12083-018-0708-3</td></tr>
<tr><td colspan="5">김종성 교수는 2018년 “Forensic Analysis for IoT Fitness Trackers and its Application”라는 제목의 논문을 IF 2.397의 SCIE 논문지 PPNA에 게재했다. Fitness tracker는 사용자의 일상적인 이동거리, 칼로리소모, 심장박동, 수면의 질 등을 측정하기 때문에, 이를 수사 관점에서 사용한다면 용의자의 활동이나 알리바이를 확인하는데 사용 가능하다. 본 논문에서는 모바일기기에 연결되어 데이터를 보여주는 대표적인 fitness tracker인 Xiaomi MI Band2와 Fitbit Alta HR가 남기는 파일 및 데이터를 해석하는 방법을 제공한다. 이는 IoT 시대의 도래에 따라 새롭게 발생하는 데이터의 분석기법을 제시한다는 점에서 의미가 있다. 본 연구의 결과는 IoT 포렌식 소개 교육자료로 활용되고 있다.</td></tr>
<tr><td rowspan="2">2</td><td>박수현</td><td>10056675</td><td>컴퓨터학</td><td>INTERNATIONAL STANDARD</td><td>ISBN 978-2-8322-5372-4</td></tr>
<tr><td colspan="5">2018년 2월 발간된 ISO/IEC 30140-1 (Information technology – Underwater acoustic sensor network (UWASN) – Part 1: Overview and requirements)은 ISO/IEC 30140 시리즈 중 첫 파트로서 수중 음파 센서 네트워크(UWASN)에 대한 일반적인 개요를 제공한다. 전파 가변성의 효과 측면에서 주요 특성을 설명하고 지상망과의 주요 차이점 분석을 제시하고 있다. 또한, UWASN의 특수성을 식별하고 이러한 네트워크에 대한 구체적이고 일반적인 요구사항을 도출하였다. 수중통신 분야에서 세계적으로 처음 도출된 표준화 결과를 대학원 교육에 접목시킴으로서 학생들에게 야기되는 산업·사회 문제를 효과적으로 해결할 수 있는 방안에 대한 학문적/산업적 안목을 증진시켰다.</td></tr>
</table>

<table>
<tr><td rowspan="2">연번</td><td>참여교수명</td><td>연구자등록번호</td><td>세부전공분야</td><td>대학원 교육관련 대표실적물</td><td>DOI번호/SBN/인터넷 주소 등</td></tr>
<tr><td colspan="5">참여교수의 교육관련 대표실적의 우수성</td></tr>
<tr><td rowspan="2">3</td><td>박수현</td><td>10056675</td><td>컴퓨터학</td><td>ICT 표준화전략맵 Ver.2020</td><td>https://www.tta.or.kr/data/reporthosulist_view.jsp?kind_num=5&hosu=2020</td></tr>
<tr><td colspan="5">과기정통부가 2019년 발간한 2020 ICT 표준화전략맵에서 수중통신 분야 전문가로 수중통신 기술 국내외 표준화 전략방향을 제시하였다. 표준화 전략맵은 국내 기업들이 강점을 가진 ICT 기술이 국제표준으로 채택되도록 하기 위한 체계적인 전략으로서 정부 정책 및 민간 표준화 활동의 전략방향을 제시하는 지침서 역할을 하고 있다. 따라서 수중 표준 전문가로서의 역량을 바탕으로 개설한 대학원 교과과정은 수중망의 통신 확장으로 견인될 기술 및 산업적/사회적 문제를 개선할 수 있는 방향을 제시하므로 우수한 교육효과를 도출하였다.</td></tr>
<tr><td rowspan="2">4</td><td>서석충</td><td>10875717</td><td>컴퓨터보안</td><td>논문</td><td>https://doi.org/10.1109/ACCESS.2019.2930986</td></tr>
<tr><td colspan="5">서석충 교수는 2019년 “SCA-Resistant GCM implementation on 8-bit AVR Microcontrollers”라는 제목의 논문을 impact factor가 4.098인 IEEE Access에 게재하였다. 본 논문은 8비트 AVR 마이크로컨트롤러 환경에서 안전한 GCM 구현을 제시한다. SPA/TA를 대비하기 위해 Garbage 레지스터와 ILA를 사용하여 더미 XOR 연산 개념을 소개하고 이를 사용하여 보안 이진체(Binary Field) 곱셈 방법을 제공한다. 또한 GCM 프로세스에서 GHASH 기능을 사용할 때 DPA/CPA를 방지할 수 있는 효율적인 곱셈 마스킹 방법을 제안한다. 8비트 AVR 마이크로컨트롤러에서의 제안된 방법과 실제 구현을 통해 제안된 방법이 기존의 대안을 능가하면서 포괄적인 SCA 보안을 제공함을 보여준다. 본 연구결과를 ‘보안소프트웨어개발’ 강의 교육자료로 사용함으로 GCM 암호 운용 모드를 구현하는 실습을 수행한다.</td></tr>
</table>

<table>
<tr><td rowspan="2">연번</td><td>참여교수명</td><td>연구자등록번호</td><td>세부전공분야</td><td>대학원 교육관련 대표실적물</td><td>DOI번호/SBN/인터넷 주소 등</td></tr>
<tr><td colspan="5">참여교수의 교육관련 대표실적의 우수성</td></tr>
<tr><td rowspan="2">5</td><td>한동국</td><td>10128486</td><td>암호론</td><td>논문</td><td>https://doi.org/10.3390/app8112258</td></tr>
<tr><td colspan="5">한동국 교수는 2018년 “Side Channel Leakages Against Financial IC Card of the Republic of Korea”라는 제목의 논문을 SCIE 논문지 Applied Sciences에 게재했다. 본 논문지의 Impact Factor는 2.217이다. 본 논문은 국내 금융 IC 카드에 사용되는 SEED 암호 알고리즘의 신규 부채널 분석 방법을 제시한다. SEED 암호 알고리즘에 사용되는 혼돈 계층 이후의 확산 계층의 특성을 이용해 낮은 키 복잡도로 키 분석이 가능하다. 신규 부채널 분석 방법을 실제 금융 IC 카드에서 수집한 부채널 파형들을 대상으로 분석을 수행하였다. 본 연구 결과를 ‘디바이스공격론’ 강의 교육자료로 사용함으로써 실제 디바이스를 대상으로부터 부채널 정보를 수집하고 이를 분석하기 위한 실습 도구로 활용한다.</td></tr>
</table>

4. 교육의 국제화 전략

4.1 교육 프로그램의 국제화 계획

▣ 미래사회 정보보안 ‘핵심인재양성’을 위한 국제화 계획 수립

- 기존에 MOU를 체결하였던 인도 최대의 사립대학 VIT University와의 교류를 통해 3명의 교환학생을 유치하였음
- 2015년 영국 QUB (Queen’s University Belfast)와 국제 공동연구 일환으로 국민대학교 수학과 및 금융정보보안학과 학생들이 두 그룹으로 나누어 QUB 장기 방문 및 공동연구 수행하였음
- 원유승, 안현진 (금융정보보안학과) 학생들은 2015년 4월부터 8월까지 (5개월) QUB 방문 및 공동연구 수행, 박애선, 심보연 (수학과, 금융정보보안학과) 학생들은 2015년 9월부터 1월까지 (5개월) QUB 방문 및 공동연구 수행함
- 국제공동연구 결과 암호해독 관련 국제학회 CARDIS 2015, WISA 2015에 공동연구 논문을 발표함
- 외국 대학과의 MOU를 체결하여 초연결사회로 거듭나는 문제를 해결하기 위한 공동 심포지엄을 운영하여 인적, 기술적 교류를 고려하고 있으며, 나아가 본 교육과정을 이수한 외국인 학생 중 우수한 학생을 유치하므로 국제 경쟁력을 강화할 수 있는 연구 환경을 조성할 예정임
- 초연결사회를 대비하여 논리적 사고력과 문제해결력을 신장시키고 우수한 연구 산출물을 획득하기 위하여 대학원생의 학술정보 지원을 강화하고 학위논문 혹은 저널을 외국어로 작성하도록 독려함
- 본 교육연구단의 대학원생들은 외국 학생들과의 교류를 통하여 상당한 수준의 교류 및 국제화 경험 체득이 가능하며 이는 한국 사회의 국제화를 촉진할 것으로 예상됨

▣ 외국 기업 및 연구소와의 교류여건 확보

▶외국 산업체와의 실질적 연구 계획 추진

- 산업통상자원부 주관 국제공동기술개발사업의 ‘딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발’ 연구를 통해 2019년 12월부터 2021년 11월까지 총 3년간 프랑스의 Texplained와 공동연구를 진행 중임. 본 국제 공동연구는 전력 파형 정보를 통해 디바이스 역공학 분야의 연구 분야 중 비정상행위 탐지 연구를 진행함
- 해당 연구 진행 중 연 2회 1달간 프랑스의 Texplained에 직접 연수를 수행하여 디바이스 역공학과 관련하여 실제 디바이스 개발 과정에 참여하는 경험을 제공할 계획임
- 과학기술정보통신부에서 주관하는 ‘한-인도 협력기반조성사업(협력네트워크)’ 과제를 신청하기 위해서 Cyber Physical System 관련 기업과 접촉중임. 지리적 여건으로 인하여 e-mail 및 virtual meeting을 통하여 의견을 교류하며 공동연구 주제를 모색하고 있음
- 외국 연구소에서 인턴으로 근무가 가능할 수 있도록 인턴쉽이 가능한 연구소를 발굴 및 제휴 체결을 시도할 예정임

▣ 외국 대학과의 교류여건 확보

▶외국 대학과의 협력 사례 및 계획

- 싱가포르 난양 기술 대학교(Nanyang Technology University)의 Physical Analysis & Cryptography Engineering (PACE) 소속 원유승 연구팀과 2020년 4월부터 격주 세미나를 통해 교류를 수행하며 연구를 진행함
- 코로나 19로 인해 현재는 세계 최고 물리보안 연구실을 확보하고 있는 PACE 팀과 국민대

학교 금융정보보안학과 부채널분석연구실이 온라인 공동연구 세미나를 수행하고 있지만, 향후 상호 연구원 교류를 통해 각자 보유하고 있는 실험실 공유를 통한 공동연구역량 강화에 합의함

- 2020년 8월, 12월 여름, 겨울 방학 기간 최소 2주 이상의 연구진 상호 방문을 통해 온라인으로 진행되는 공동연구 내용의 실험적 공동 검증 연구를 수행 예정임
- 국민대학교와 상호 교류 체결이 논의된 바 있는 Katholieke University of Leuven (벨기에) Indraprastha Institute of Information Technology (인도), MASSEY University (뉴질랜드) 등의 학교와도 상호 교류를 위한 프로그램을 개발할 예정임
- 해당 상호 교류 체결이 이루어질 경우, 교육연구단 소속 학생들로 하여금 방학기간을 활용하여 해외 학교의 Summer School을 수강할 수 있도록 단기 방문하는 프로그램을 개발하여 파견할 예정임
- 외국 대학과의 교류를 통해서 각자의 주 분야에 대한 고속 구현 기술을 공유하고 공통된 조건에서의 서로 간의 차이점을 분석하거나 다른 환경에서의 고려 사항들을 비교하는 등 각종 환경에서의 장단점을 분석함으로써 확장된 개발 방식을 습득할 수 있음
- 따라서 국제 공동 연구에 참여하는 국내/국외 학자들에 대한 정기적인 세미나 및 실시간 피드백을 활용하여 활발한 의견 교류와 정보 공유를 가능하게 하고 이에 따른 시너지를 기대할 수 있음

▶우수한 해외학자와의 활용을 위한 교류 프로그램 마련

- 국외 유명 논문 저자 혹은 전문가를 초빙하여 국외 연구 동향 및 각종 이슈에 대해 습득할 수 있도록 세미나 개최 예정임
- 해외의 저명 학자를 피인용수가 10회 이상의 논문 저자들로 선정하고, 정보보안 분야의 경력이 5년 이상이며 정보보안 분야에서 지속적으로 연구활동을 진행하고 있는 전문가를 초빙할 예정임
- 국제화 역량 강화를 위한 해외전문가들을 초청하여 5G/6G 유무선 통신, 통신기술 발달로 인한 보안 이슈, 도메인이 확장되고 있는 사물인터넷(IoT)과 관련된 워크숍 및 전문가 초청 강연을 개최할 예정임
- 국제학술대회에 참석한 외국 저명인사를 강연자로 초청하여 해외에 나가지 않고도 우수한 해외 저명 연구자들의 연구결과를 소개받는 방법으로 활용할 것임
- 결과적으로 국제적 인적 네트워크를 형성하여 학술적 정보를 교류하므로 대외적으로 경쟁력을 증진시킬 수 있고, 참여 대학원생들의 연구역량 및 국제화 소양이 강화될 뿐만 아니라 국내 학술 진흥을 도모할 수 있음

▣ 안전한 초연결사회를 위한 문제해결형 전문인력 양성 전략

▶5G/6G 유무선 통신 기술의 국외 교류 및 협력 방안

- 박수현 교수는 지난 2018년 인도를 방문하여 MITS 대학과 교수진 및 학생 교류, 공동 연구 자료 정보 교환, 국제 합동 회의 개최 등의 내용이 포함된 양해각서를 체결하였음

ఇంటర్నెట్ థింగ్స్‌పై అవగాహన పెంచుకోండి

కూక్మిన్ విశ్వవిద్యాలయ అధ్యక్షుడు సోయోహ్యూన్ పార్క్

కడపబలకోట, డిసెంబరు 18:ఇంటర్నెట్ థింగ్స్‌పై అవగాహన పెంచుకోవడంతో దక్షిణ కొరియాకు చెందిన కూక్మిన్ విశ్వవిద్యాలయం ప్రెసిడెంట్ సోయోహ్యూన్ పార్క్ పిలుపునిచ్చారు. అంగళ్లు మిట్ట్ కళాశాలలో జరిగిన అవగాహన సదస్సులో ఆయన మాట్లాడుతూ కొరియాలో ఇంజనీరింగ్ విద్యార్థులకు ఇంటర్న్‌షిప్, ఉద్యోగావకాశాలు ఎప్పుడూ ఉన్నాయన్నారు. అండర్‌వాటర్ కమ్యూనికేషన్ వ్యవస్థపైఇంటర్నెట్ థింగ్స్‌పై మమ్మరంగా పరిశోధనలు జరుగుతున్నాయన్నారు. దీనిపై విద్యార్థులు, అధ్యాపకులు అవగాహన పెంపొందించుకోవాలన్నారు.మిట్స్ ప్రిన్సిపాల్ యువరాజ్ మాట్లాడుతూ కూక్మిన్ విశ్వవిద్యాలయంలో ఇప్పటి విద్యార్థులు ఇంటర్న్‌షిప్‌లో మరిన్ని పాల్గొనే అవకాశాన్ని కల్పించనున్నట్లు తెలిపారు. కొరియాలో సీఎస్‌ఈ, ఈసీఈ విద్యార్థులకు ఉన్న అవకాశాలను తెలియజేశారు. కూక్మిన్ విశ్వవిద్యాలయ ఉపాధ్యక్షురాలు సూయంగ్‌షిన్, ఇంటర్నేషనల్ సెల్ కోఆర్డినేటర్ విజయలక్ష్మి, దీప్లు రామప్రసాదరావు, కపవన్ తదితరులు పాల్గొన్నారు.

సదస్సును ప్రారంభిస్తున్న సోయోహ్యూన్ పార్క్,చిత్రంలో తదితరులు

ఆంధ్రజ్యోతి Wed, 19 December 2018 https://epaper.andhrajyothy.com/c/34990806

SOUTH KOREAN VARSITY TEAM VISITS MITS

EXPRESS NEWS SERVICE
@Tirupati

PROF. Soo Hyun Park, president and Prof. Soo Young Shin, Vice-President of Special Communication Research Centre, Kookmin University, South Korea, visited the Madanapalle Institute of Technology and Science (MITS), Madanapalle, Chittoor district and conducted an interactive session with students and faculty on the campus. Prof. Park, who was the chief guest of the programme, said the purpose of the visit was to organise students internships. Now that the entire world has shrunk into the global village, the students should grab as many opportunities as they can for internships and research collaborations as possible and move ahead, he said.

Prof. Park said special communication research centre of Kookmin University would contributes through research on fundamental issues in underwater sensor networks. The centre aims at developing an applicable underwater technology.

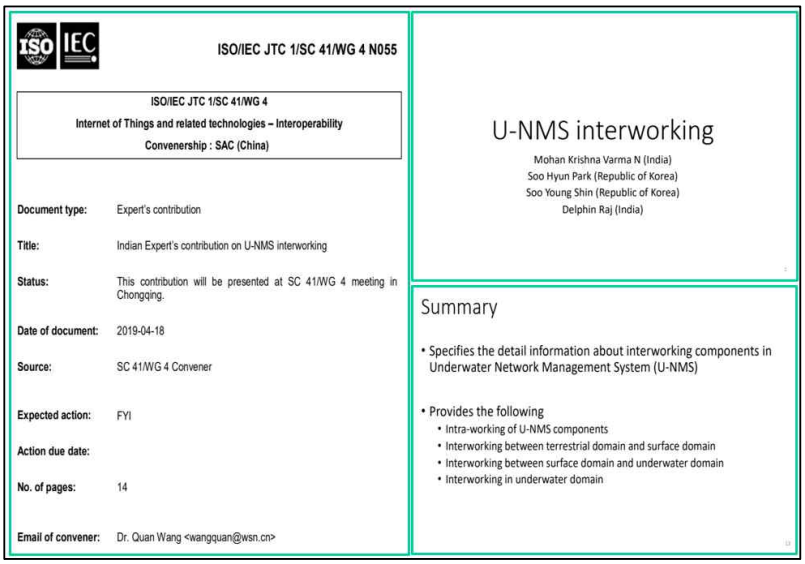
INDIAN EXPRESS Wed, 19 December 2018 epaper.newindianexpress.com/c/34992242

본 교육연구단의 박수현 교수 관련 현지 언론기사

- 인도는 영국의 식민지 결과 영어가 능숙한 인력이 많고, 인도인들의 수리적이고 논리적인 성향은 과학기술을 발달시키는 데 높은 영향을 끼쳤음
- 그러므로 우수한 과학 기술인력 풀을 가지고 있는 인도와 국제적 교류를 통하여 최신과학기술 및 know-how를 습득하므로 산업·사회문제를 해결할 수 있는 선진기술 개발 수준을 제고 할 수 있음
- 인도 통신 산업은 2000년대 이후 빠른 성장세를 보이고 있으며, 인도 정부는 2014년 '디지털 인디아' 이니셔티브를 발표하고 인도의 디지털 사회화 및 경제화를 목표로 설정하면서 4차 산업혁명에 대응하기 위한 정책과 전략을 추진하고 있음
- 모든 도시 내, 도시 간 연결성 강화에 초점을 맞춰 사물인터넷, 와이파이, 모바일 통신기술을 기반으로 하는 산업의 발전에 기여하고 있음
- 최근 신흥시장으로 떠오르고 있는 인도와 해양분야 협력을 위해 수중-IoT(수중통신) 표준 신규 아이템 발굴 및 개발 논의를 거쳐 지난 2019년 5월 개최된 제5차 ISO/IEC JTC 1/SC 41/WG 4에서 "U-NMS Interworking" 주제로 PWI를 발표하였으며 현재 NWIP단계에 진입하였음
- 한국과 인도가 함께 개발하고 있는 "U-NMS Interworking"은 박수현 교수 연구팀에서

발간한 ISO/IEC 30140 시리즈 및 현재 FDIS단계의 ISO/IEC 30142 및 ISO/IEC 30143 국제표준 문서를 기반으로 하고 있음

- 따라서 본 표준 개발 문서의 Scope에 해당하는 U-NMS 구성요소의 내부 작동, 지상과 수중 도메인에서의 상호 작용 네트워크 등의 주제를 다루는 심층 세미나를 정기적으로 인도측 연구자들과 진행할 계획이며, 이를 통해 글로벌 경쟁력을 가지는 수중-IoT 기술혁신 및 참여 대학원생의 국제화 역량을 향상할 수 있을 것임


ISO/IEC JTC 1/SC 41/WG 4 N055

ISO/IEC JTC 1/SC 41/WG 4
Internet of Things and related technologies – Interoperability
Convenership : SAC (China)

Document type:	Expert's contribution
Title:	Indian Expert's contribution on U-NMS interworking
Status:	This contribution will be presented at SC 41/WG 4 meeting in Chongqing.
Date of document:	2019-04-18
Source:	SC 41/WG 4 Convener
Expected action:	FYI
Action due date:	
No. of pages:	14
Email of convener:	Dr. Quan Wang <wangquan@wsn.cn>

U-NMS interworking

Mohan Krishna Varma N (India)
Soo Hyun Park (Republic of Korea)
Soo Young Shin (Republic of Korea)
Delphin Raj (India)

Summary

- Specifies the detail information about interworking components in Underwater Network Management System (U-NMS)
- Provides the following
  - Intra-working of U-NMS components
  - Interworking between terrestrial domain and surface domain
  - Interworking between surface domain and underwater domain
  - Interworking in underwater domain

ISO/IEC 국제표준화 관련 연구 실적

▶자율성장 인공지능 기술의 국제화 및 인적 교류 방안

- 미국 MIT 기계공학과 김상국 교수 연구팀과 국민대 소프트웨어 윤상민 연구팀은 지속적으로 인공지능 기술을 활용한 디자인 프로세스와 관련된 연구를 진행하여 왔음
- 지능형 시스템 분야에서의 설계 및 활용을 위한 디자인 프로세스 정립을 위하여 기존에는 설계자의 주관적인 판단에 의한 하여 이루어졌지만 자율성장 인공지능 기술을 활용하여 다양한 분야에 적용 가능한 프로세스를 정립하고 있음
- 자율성장 인공지능 기술의 활용 및 적용에 대하여 본 교육연구단에서는 다양한 인공지능 모델을 개발하고 MIT 기계공학과에서는 AI for Design과 관련된 프로세스를 정립하고 활용하기 위한 방안을 마련함으로서 지속적인 연구 교류가 이루어지도록 함
- 학생 및 담당 교수가 연 1회 방문하여 관련 논의 및 세미나를 진행할 수 있도록 함

▶자율성장 인공지능 기반 보안 기술의 해외 협력 방안

- 체코 Brno University of Technology는 국민대와의 MOU를 체결하여 지속적으로 교환학생을 파견하고 있으며, IT 분야의 Martin Drahansky 교수는 지능형 시스템을 활용하여 체코 경찰과의 치안 분야의 보안 분야 기술을 개발하고 있음
- 지능형 감시 시스템에서 다양한 환경적 조건과 데이터의 특성에 따른 신뢰성 높은 인공지능 기술의 개발 및 활용과 관련하여 지속적으로 공동 연구 및 인적 교류를 통하여 자율성장 시스템에서의 보안 문제를 해결할 수 있도록 함
- 지능형 시스템의 공격 및 방어 시스템 구축과 관련하여 지속적인 인적 교류 및 워크숍을

통하여 자율 성장 인공지능 기술을 활용한 체코 및 유럽과 한국에서의 사회 문제 해결에 적용할 수 있도록 인적 교류 및 자문할 수 있도록 함

AI 분야 해외 전문가 초빙 프로그램

▣ 산업・사회적 문제 해결을 위한 국제표준화 활동

▶사물인터넷 및 관련기술 국제표준화위원회 ISO/IEC JTC 1/SC 41 활동

- 수중통신을 위한 기술들에 대한 표준화가 진행되고 있음. 하지만 해양에서 발생하는 재난 및 사고 등과 같은 위기를 효과적으로 대응하기 위하여 개발되는 수중통신 기기 및 장비는 특수한 목적성으로 인하여 표준화 진행에 제약이 있음. 따라서 추구하는 목적에 적합한 기술의 표준개발이 절실한 실정임
- 현재 해양통신 또는 IoT 기반 해양 네트워크 기술에 대한 표준화가 공적 국제표준으로 ISO/IEC JTC 1/SC 41 산하에 존재하는 IoT Architecture, IoT Interoperability, IoT Application 분야의 3개의 Working Group (WG) 회의에서 각국의 Experts와의 활발한 토의 및 연구를 통하여 표준화가 개발되고 있으며 인적네트워크 또한 형성되고 있음
- 따라서 본 교육연구단 참여 대학원생들의 국제표준화 회의 참여를 증진시키고 이를 바탕으로 이슈가 되는 산업・사회 문제를 해결하기 위한 국제 기고서를 제출 할 수 있는 역량을 강화시킬 예정임

▶정보보안기술 국제표준화위원회 ISO/IEC SC27 활동

- 국제표준화기구 ISO/IEC SC27은 정보보안 표준화 그룹으로, 5개의 소그룹 WG으로 운영중이며, WG2는 암호 알고리즘의 표준화, WG3는 보안성 평가 방안 표준화를 담당하며, 세계 각국의 암호 전문가들이 매년 2회의 정기 회의를 통해 표준화를 진행함
- 현재 WG2의 국내전문가 수가 WG2의 표준화 프로젝트 수에 비해 현저히 적어, 모든 프로젝트의 진행 상황을 파악하는데 큰 어려움이 있음. 따라서 국내 암호 전문가들의 표준화 프로젝트 기여가 필요한 상황임
- 본 교육연구단은 참여 대학생들의 지속적인 표준화 활동을 장려하여, 표준화 프로젝트에 참여시켜 표준에 대한 이해를 제고시키고, 외국 전문가와의 협업할 수 있는 기회도 제공할 계획임

4. 교육의 국제화 전략

4.2 대학원생 국제공동연구 계획

▣ 국제공동연구를 통한 국제화 계획

▶해외 관련 연구기관과의 공동연구

- 산업통상자원부 주관 국제공동기술개발사업의 ‘딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발’ 연구를 통해 2019년 12월부터 2021년 11월까지 총 3년간 프랑스의 Texplained와 공동연구를 진행 중이다. 본 국제 공동연구는 전력파형 정보를 통해 디바이스 역공학 분야의 연구 분야 중 비정상행위 탐지 연구를 진행 중임
- 해당 연구 진행 중 연 2회 1달간 프랑스의 Texplained에 직접 연수를 수행하여 디바이스 역공학과 관련하여 실제 디바이스 개발 과정에 참여하는 경험을 제공할 계획임
- 싱가포르 난양 기술 대학교(Nanyang Technology University)의 Physical Analysis & Cryptography Engineering (PACE) 소속 원유승 연구팀과 격주 세미나를 통해 교류를 수행하며 연구를 진행하고 있음
- 해당 기관과의 세미나를 통해 연구 결과를 도출하기 위해 연구 주제가 구체화된 경우, 15일 가량 싱가포르에 출장을 통해 직접적인 교류를 추진할 계획임
- 싱가포르 출장 중에는 공동 실험 및 공동 논문 작업 등의 연구활동을 진행할 수 있도록 계획하고 있음

▶박수현 교수의 해외 대학과의 공동연구 내용

- 박수현 교수는 과학기술정보통신부에서 주관하는 ‘한-인도 협력기반조성사업(공동연구)’에 과제를 신청하기 위해서 인도의 Vellore Institute of Technology (VIT)와 Madanapalle Institute of Technology & Science (MITS)의 소속 교수진과 접촉 중임

기간	내용
2020.12.16.-2020.12.31.	국민대학교 선발 인원 1인 Vellore Institute of Technology 방문
	연구주제 : 자연재해 및 재난 조기경보 공동 연구
	연구목표: 첨단 빅데이터 분석기법 확보

<Vellore Institute of Technology 방문 계획>

기간	내용
2021.08.10.-2021.08.24.	Vellore Institute of Technology 연구원 1인 방문
	연구주제 : 자연재해 및 재난 조기경보 공동 연구
	연구목표 : 상황인지 기반 IoS 지능형 서비스 기술 확보

<국민대학교 방문 계획>

- 지리적 여건으로 인하여 e-mail 및 virtual meeting을 통하여 의견을 교류하며 공동연구 주제를 모색하고 있으며, 본 교육연구단의 핵심 기회로 활용할 예정임
- 현재 연구 기획 단계로 삶의 질 향상을 위하여 자동화 및 환경 관리가 필수적으로 요구되는 상수원 종합관리를 고려한 ‘자연재해 및 재난 조기경보’ 주제를 고려중임
- 본 연구를 통하여 실시간으로 수중 센서에서 수집되는 방대한 데이터를 첨단 빅데이터 분석기법을 활용하여 분석 가능하며, 그 결과를 해양환경 관제센터에 전송하므로 기름 유출 등과 같은 재난에 대한 조기경보를 실시할 수 있음
- 이를 통하여 인도와 한국 전역의 해양영역에서 관리자가 사용할 수 있는 정책 시스템 설

계가 가능하며, 이해관계자에게는 IoS(Internet of Service) 제공이 가능할 것으로 사료됨
- 국제공동연구를 수행하며 우수한 연구 결과를 도출하기 위하여 참여 대학원생들에게 세미나를 통한 이론·기술 강의 및 효과적인 연구수행을 위한 인도 출장비 및 관련 비용을 지원하는 것을 고려하고 있음
- 인도와의 국제공동연구 수행을 통하여 협력연구 및 과학기술 협력기반 강화를 넘어서 국제적 소양을 갖춘 인재 육성도 가능할 것으로 예상됨

▶이옥연 교수의 해외 대학과의 공동연구 내용

- 본 교육연구단의 이옥연 교수는 과학기술정보통신부의 정보통신기획평가원(IITP)으로부터 정보보안핵심원천기술개발사업(R&D)의 일환으로 'IoT 장비 펌웨어 보안성 검증 기술개발' 국제공동연구 과제를 수행 중이며, 미국 University of Florida 대학의 FICS (Florida Institute for Cybersecurity Research)와 EYL사(Everywhere in Your Life)와 함께 2018년 4월부터 IoT(Internet of Things) 시스템의 고도화로 인해 악성코드, 랜섬웨어, 분산 서비스 거부와 같은 다양한 사이버 공격 대응기술이 중요한 관심사가 되고 있는 IoT 펌웨어 장비에 대한 보안성 검증 통합 프레임워크 개발에 대한 국제 공동연구를 진행하고 있으며, 암호 장비 및 모듈 개발 기술을 지속적으로 공동 개발할 계획임
- 이처럼 해외 기업과 산학 공동 과제를 진행하게 됨에 따라 본 사업단은 미국 실리콘 밸리를 비롯해 세계 유수한 전문업체와 교류할 수 있도록 연구 협약 체결을 꾸준히 추진하여 산학 협동 과정의 기회를 지속하여 늘려갈 계획이며, 석·박사 졸업생으로 하여금 정보보안 기술 역량을 창업으로 이끌어내도록 독려함은 물론 이를 발판으로 향후 졸업생이 세계적 연구 기관이나 업체에 진출할 수 있도록 이끌 계획임

▶한동국 교수의 해외 대학과의 공동연구 내용

- 싱가포르 난양 기술 대학교(Nanyang Technology University)의 Physical Analysis & Cryptography Engineering (PACE) 소속 원유승 연구팀과 2020년 4월부터 격주 온라인 세미나를 통해 교류를 수행하며 연구를 진행하고 있음
- PACE 팀과 2021년 1월~2월 겨울 방학 기간에 각 2주 이상 상호 기관 방문 통해 Cold-Boot Attack 연구주제와 Machine Learning 기반 상용 IC카드 분석 연구주제로 직접적인 교류를 추진할 계획임.

기간	내용
2021.01.10.-2021.01.30.	국민대학교 선발 인원 2인 난양기술대학교 방문
	연구주제 : IoT 기기에 대한 Cold-Boot Attack 공동 연구
	연구목표: 고등 물리보안 취약성 검증 최신 기술 확보

<난양 기술 대학교 방문 계획>

기간	내용
2021.02.10.-2021.02.25.	난양기술대학교 PACE 연구원 2인 방문
	연구주제 : ML기반 상용IC카드 분석 공동 연구
	연구목표 : 상용스마트디바이스 신규 취약성 탐지 기술 확보

<국민대학교 방문 계획>

▶해외 연구기관 및 대학에 단기 또는 장기 파견

- 한 학기(단기) 또는 두 학기 이상(장기) 기간 동안 협정체결 해외학교에서 수학하는 교환학생 프로그램 개발을 통해 본 교육연구단의 대학원생이 국제공동연구를 수행할 수 있도록 지원할 계획임
- 정기적인 세미나 및 실시간 양방향 아이디어 공유를 통해 새로운 아이디어를 제시하고 선택된 아이디어에 대한 전체적 공유가 완료되면 독립 환경 여부를 판단할 수 있도록 지도할 예정임
- 독립적인 환경에서 진행할 경우 주기적으로 또는 연구 단계별로 진행 상황을 공유하고 이슈를 해결할 수 있도록 지도할 계획임
- 온라인을 통한 단순 연구 주제 및 목표, 자료 공유와는 다르게 오프라인 교류는 연구실 환경과 자원을 공유하고 실시간으로 의견 피드백이 가능하여 더욱 더 긴밀하게 협동이 가능하므로, 이를 통해 효율 높은 연구 성과를 기대할 수 있음
- 정기적으로 해외 유수 연구원을 초빙하여 특강 또는 단기강좌를 통한 국제공동연구 수행할 수 있도록 지도할 계획임

Ⅲ. 연구역량 영역

1.2연구업적물

① 참여교수 대표연구업적물의 적합성과 우수성

<표 3-2> 최근 5년간 참여교수 대표연구업적물 실적

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자 등록번호</th><th>이공계열/ 인문사회계열</th><th>전공분야
세부전공분야</th><th>실적 구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="8">1</td><td rowspan="8">강주성</td><td rowspan="8">10127144</td><td rowspan="8">이공계열</td><td rowspan="4">수학

확률과정론</td><td rowspan="8">저널논문</td><td>Yongjin Yeom, Ju-Sung Kang</td><td></td></tr>
<tr><td>Probability distributions for the Linux entropy estimator</td><td rowspan="3"></td></tr>
<tr><td>Discrete Applied Mathematics</td></tr>
<tr><td>241, 87-99</td></tr>
<tr><td>2/2</td><td>URL입력</td></tr>
<tr><td>2018</td><td rowspan="2">https://doi.org/10.1016/j.dam.2016.07.019</td></tr>
<tr><td>https://doi.org/10.1016/j.dam.2016.07.019</td></tr>
<tr><td colspan="7">Linux 및 임베디드 시스템과 모바일 장치의 여러 운영체제에서 LRNG가 널리 사용되지만, LRNG의 설계 근거는 불분명하다. 경험적 엔트로피 분석에 따르면 LRNG에 의해 계산된 추정 엔트로피가 경험적 빈도수에 기반한 엔트로피보다 낮다. LRNG의 출력 난수는 엔트로피 소스에 의해 완전히 결정되므로, 잡음원에서 수집된 엔트로피의 양을 정확히 추정하는 것이 매우 중요하다. 본 논문에서는 랜덤한 이벤트 시간에 대한 확률 모델을 구성한 다음 첫 번째, 두 번째 및 세 번째 시간 차이에 대한 확률 분포를 정확하게 도출한다. LRNG에서 엔트로피를 추정하는 데 사용되는 이러한 차이의 최소 절댓값에 대한 확률 분포를 도출한다. 본 연구 결과는 일반적인 랜덤한 시간 차이로부터 생성된 잡음원에서 엔트로피가 수집되는 경우 엔트로피가 정확하게 추정되지 않아 발생하는 안전성 문제를 완화하는데 기여한다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="8">2</td><td rowspan="8">강주성</td><td rowspan="8">10127144</td><td rowspan="8">이공계열</td><td rowspan="4">수학

확률과정론</td><td rowspan="8">저널논문</td><td>Hojoong Park, Yongjin Yeom, and Ju-Sung Kang</td><td></td></tr>
<tr><td>A Lightweight BCH Code Corrector of TRNG with Measurable Dependence</td><td rowspan="3"></td></tr>
<tr><td>Security and Communication Networks</td></tr>
<tr><td>2019</td></tr>
<tr><td></td><td>URL입력</td></tr>
<tr><td>2019</td><td rowspan="2">https://doi.org/10.1155/2019/9684239</td></tr>
<tr><td>chttps://doi.org/10.1155/2019/9684239</td></tr>
<tr><td colspan="7">대부분의 코드 후처리 기법은 편향된 입력 비트가 독립적일 때 출력 비트의 편향성(bias)을 줄이는 주제에 관해 연구되었으므로, 본 논문에서는 출력 비트의 의존성에 집중하고, 새로운 척도인 의존성 정도(degree of dependence)를 정의한다. 이론적 분석 결과 및 시뮬레이션 결과를 통해 의존성 정도가 입력 비트의 편향성과 관련이 있다는 사실을 얻었다. 또한, BCH 코드 후처리 기법은 작은 코드 크기로 인해 IoT, 임베디드 및 모바일 장치와 같은 경량 환경에 적용할 수 있다. 따라서 제안하는 BCH 코드 후처리 기법은 TRNG(True Random Number Generator)의 후처리 요소로서 경량 환경에 적용할 수 있고, 출력 비트 간의 의존성은 입력 비트의 편향성에 따라 제어할 수 있다. 본 논문의 결과는 경량 환경에서 엔트로피 소스를 효율적으로 관리하는데 이용될 수 있다.</td></tr>
</table>

연번	참여교수명	연구자등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
3	강주성	10127144	이공계열	수학 확률과정론	저널논문	박호중, 강주성, 염용진	
						진난수발생기용 난수성 검정 방법 AIS.31에 대한 확률론적 분석 및 보안성 평가 적용 방법	
						정보보호학회논문지	
						26(1), 49-67	
							URL입력
						2016	https://doi.org/10.13089/JKIISC.2016.26.1.49
						https://doi.org/10.13089/JKIISC.2016.26.1.49	
	본 논문은 진난수발생기(TRNG, True Random Number Generator)의 통계적 난수성을 평가하는 대표적인 방법 중 독일 BSI의 AIS.31의 통계적 검정들을 일반화한 결과를 도출한다. AIS.31 평가 기준의 목적은 온라인 검정으로, 진난수발생기의 작동 중에 내부난수의 완전붕괴를 검출한다. 온라인 검정을 오프라인 검정에 그대로 적용하는 것은 어렵고, 임베디드, 모바일 환경 등의 장비별 특성에 따른 다양한 잡음원으로부터 추출된 정보를 입력으로 하는 진난수발생기 출력 수열의 난수성 평가 방법을 획일적으로 적용하는 것은 바람직하지 못하다. 따라서 본 논문에서는 유의수준과 표본수열의 길이에 따른 검정 통과 기준을 제시함으로써 AIS.31을 일반화한다. 또한, AIS.31에서 정확히 기술하지 않은 검정의 반복 시행 결과들에 대해 신뢰구간 개념을 적용한 최종 통과 기준을 제안하고, 적절한 시뮬레이션을 통하여 본 논문의 분석 결과에 대한 유효성을 확인한다. 본 논문의 결과는 2017년에 제정되고 2018년에 개정된 TTA 표준문서인'소프트웨어 환경에서의 잡음원 엔트로피 검증 알고리즘(TTAK.KO-12.0306/R1)'에서 참조되고 있다.						

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="9">4</td><td rowspan="8">김동찬</td><td rowspan="8">11579260</td><td rowspan="8">이공계열</td><td rowspan="4">수학</td><td rowspan="8">학술대회논문</td><td>Jaeheon Kim, Je Hong Park, Dong-Chan Kim, and Woo-Hwan Kim</td><td></td></tr>
<tr><td>Complete Addition Law for Montgomery Curves</td><td rowspan="3"></td></tr>
<tr><td>ICISC 2019</td></tr>
<tr><td></td></tr>
<tr><td rowspan="4">암호론</td><td></td><td>URL입력</td></tr>
<tr><td>2019</td><td rowspan="2">https://doi.org/10.1007/978-3-030-40921-0_16</td></tr>
<tr><td>https://doi.org/10.1007/978-3-030-40921-0_16</td></tr>
<tr><td colspan="7">일반적으로 타원곡선군의 덧셈은 입력값에 따라 다른 연산식을 사용한다. 그런데 이 방식은 암호 구현 시 조건확인 과정이 반드시 포함되어야 하기에 연산 효율성 저하가 발생한다. 따라서 입력값의 조건이 없는 완전덧셈에 대한 연구가 학계에 많은 관심을 받았다. 최근 몇 년간 주요 타원곡선에 대한 완전덧셈식이 발표되었다. 본 논문은 DH키공유 알고리즘에 사용하는 몽고메리 타원곡선에 대한 효율적인 완전덧셈식을 제시하는 논문이다.</td></tr>
<tr><td rowspan="9">5</td><td rowspan="8">김동찬</td><td rowspan="8">11579260</td><td rowspan="8">이공계열</td><td rowspan="4">수학</td><td rowspan="8">저널논문</td><td>Dong-Chan Kim, Dae San Kim</td><td></td></tr>
<tr><td>Poset weight enumerators</td><td rowspan="3"></td></tr>
<tr><td>Advanced Studies Contemporary Mathematics</td></tr>
<tr><td></td></tr>
<tr><td rowspan="4">암호론</td><td></td><td>URL입력</td></tr>
<tr><td>2017</td><td rowspan="2">http://jangjeonopen.or.kr/public/upload/1495045679-ascm27-2-(7).pdf</td></tr>
<tr><td>http://jangjeonopen.or.kr/public/upload/1495045679-ascm27-2-(7).pdf</td></tr>
<tr><td colspan="7">일반적으로 오류정정부호는 해밍거리 개념을 사용한다. 하지만 부호의 효율성을 높이기 위해 다양한 거리개념을 적용하는 시도가 있다. 본 논문은 Poset 거리 기반 부호의 무게셈자를 제안한다. 또한 고차원 부호의 무게셈자와 Tutte 다항식과의 연관성도 함께 제시한다.</td></tr>
</table>

연번	참여교수명	연구자 등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
6	김동찬	11579260	이공계열	수학 암호론			
							URL입력
	-						
7	김종성	10182694	이공계열	컴퓨터학 정보보호	저널논문		
						How to Decrypt PIN-Based Encrypted Backup Data of Samsung Smartphones	
						Digital Investigation	
						26, 63-71	
							URL입력
						2018	https://doi.org/10.1016/j.diin.2018.05.006
						https://doi.org/10.1016/j.diin.2018.05.006	
	스마트폰은 이미 현대인의 필수품이 되었으며, 잠재적인 디지털증거가 발견될 수 있는 유력한 기기이기 때문에 디지털 포렌식 수사에 있어서 가장 먼저 조사해야 될 대상이다. 하지만 스마트폰이 망가지거나 압수가 불가능한 경우에는 스마트폰 정보를 저장해 둔 백업파일을 분석해야 하지만, 백업파일은 벤더사에서 제공하는 프로그램을 통해 암호화되어 있기 때문에 그 내용을 확인할 수 없다. 본 논문에서는 삼성 스마트폰의 백업프로그램을 역공학을 통해 분석하여 그 암호알고리즘의 동작과정을 분석하고 그 플로우 차트를 제공하여 포렌식 수사 시 사용할 수 있게 한						

연번	참여교수명	연구자등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
	다. IF 1.771의 SCIE 논문지 Digital Investigation에 게재되었다.						
8	김종성	10182694	이공계열	컴퓨터학 정보보호	저널논문	Hangi Kim, Myungseo Park, Jaehyung Cho, Jihun Kim, Jongsung Kim	
						Weaknesses of Some Lightweight Blockciphers Suitable for IoT Systems and Their Applications in Hash Modes	
						Peer-to-Peer Networking and Applications	
						13(2), 489-513	
							URL입력
						2019	https://doi.org/10.1007/s12083-019-00734-2
						https://doi.org/10.1007/s12083-019-00734-2	
	블록암호 기반 해시함수인 12개의 PGV 모델, MDC-2, HIROSE는 모두 기반 블록암호가 안전할 때 해시함수로서의 안전성이 증명된다. 하지만 이들 해시함수는 취약한 키 스케줄을 갖는 블록암호를 기반으로 한다면 공격될 수 있다. 본 논문에서는 확산효과가 약한 키 스케줄을 갖는 블록암호 Midori-128, LS-design (Fantomas), GOST, 12라운드 축소 AES-256의 연관키 혹은 선택키 차분성질을 제시하고, 이 성질들을 12개의 PGV 모델, MDC-2 또는 HIROSE에 대한						

연번	참여교수명	연구자등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
	충돌쌍 공격으로 전이시키는 방법을 소개한다. 또한, PRINT와 Midori-64에 대한 불변 부분공간 공격이 해시함수의 충돌쌍 공격으로도 전이될 수 있음을 최초로 보인다. 이는 IoT 환경에서 사용하는 경량 블록암호 기반의 해시함수를 선택할 때, 적절한 확산효과를 갖는 키 스케줄을 사용하는 블록암호를 사용해야 함을 뜻한다. IF 2.397의 SCIE 논문지 PPNA에 게재되었다.						
9	김종성	10182694	이공계열	컴퓨터학 정보보호	저널논문	Serim Kang, Soram Kim, Jongsung Kim	
						Forensic Analysis for IoT Fitness Trackers and its Application	
						Peer-to-Peer Networking and Applications	
						13, 564-573	
							URL입력
						2018	https://doi.org/10.1007/s12083-018-0708-3
						https://doi.org/10.1007/s12083-018-0708-3	
	Fitness tracker는 사용자의 일상적인 이동거리, 칼로리소모, 심장박동, 수면의 질 등을 측정하기 때문에, 이를 수사 관점에서 사용한다면 용의자의 활동이나 알리바이를 확인하는데 사용 가능하다. 본 논문에서는 모바일기기에 연결되어 데이터를 보여주는 대표적인 fitness tracker인 Xiaomi MI Band2와 Fitbit Alta HR가 남기는 파일 및 데이터를 해석하는 방법을 제공한다. 이는 IoT시대의 도래에 따라 새롭게 발생하는 데이터의 분석기법을 제시한다는 점						

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="2"></td><td rowspan="7"></td><td rowspan="7"></td><td rowspan="7"></td><td rowspan="7"></td><td rowspan="7"></td><td></td><td></td></tr>
<tr><td rowspan="5"></td><td rowspan="3"></td></tr>
<tr><td></td></tr>
<tr><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td rowspan="2"></td></tr>
<tr><td></td></tr>
<tr><td colspan="7">에서 의미가 있다. IF 2.397의 SCIE 논문지 PPNA에 게재되었다.</td></tr>
<tr><td rowspan="9">10</td><td rowspan="9">박수현</td><td rowspan="9">10056675</td><td rowspan="9">이공계열</td><td rowspan="5">컴퓨터학</td><td rowspan="9">저널논문</td><td>Mohan Krishna Varma N, Kalyani M, Soo-Young Shin, Soo-Hyun Park</td><td></td></tr>
<tr><td>Underwater spray and wait routing technique for mobile ad-hoc networks</td><td rowspan="3"></td></tr>
<tr><td>Indian Journal of Geo Marine Sciences</td></tr>
<tr><td>48(10), 1648-1655</td></tr>
<tr><td></td><td>URL입력</td></tr>
<tr><td rowspan="4">컴퓨터학</td><td>2019</td><td rowspan="2">http://nopr.niscair.res.in/handle/123456789/51147</td></tr>
<tr><td>http://nopr.niscair.res.in/handle/123456789/51147</td></tr>
<tr><td colspan="7">수중 모바일 애드혹 네트워크는 출발지에서 목적지까지 end-to-end 경로가 존재하지 않는 간헐적인 네트워크다. 이러한 문제를 극복하기 위해서 지연-허용 네트워크(DTN)가 좋은 해결책으로, 본 논문에서는 SaW(Spray and Wait) 라우팅 기법을 검토한다. SaW에서 소스 및 릴레이 노드는 이동 노드를 나타내며, 대상 노드로 데이터를 전송하려고 한다. 이를 바탕으로 수중 모바일 애드혹 네트워크를 위한 수중 SW(USaW) 라우팅에 기초한 복제품을 제안한다. USaW에서 소스 노드는 표면 하단에 고정되며, 수중 센서 노드는 센서 데이터를 복제하여 발생하는 릴레이 노드에</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="2"></td><td rowspan="7"></td><td rowspan="7"></td><td rowspan="7"></td><td rowspan="7"></td><td rowspan="7"></td><td></td><td></td></tr>
<tr><td rowspan="5"></td><td rowspan="5"></td></tr>
<tr><td></td></tr>
<tr><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td rowspan="2"></td></tr>
<tr><td></td></tr>
<tr><td colspan="8">최대 데이터 복사본을 제공한다. 일반적으로 릴레이 노드는 수중 환경의 센서 노드에 비해 데이터 전송 능력이 높다. 본 논문에서는 기존 SW 및 라우팅 프로토콜과 비교한 전달 비율, 네트워크 처리량, 에너지 소비량, 엔드 투 엔드 지연, 패킷 손실률에 대한 USaW의 성능을 분석한다.</td></tr>
<tr><td rowspan="8">11</td><td rowspan="8">박수현</td><td rowspan="8">10056675</td><td rowspan="8">이공계열</td><td rowspan="4">컴퓨터학</td><td rowspan="8">저널논문</td><td>Delphin Raj K M, Sun-Ho Yum, Eunbi Ko, Soo-Young Shin, Jung-Il Namgung and Soo-Hyun Park</td><td></td></tr>
<tr><td>Multi-Media and Multi-Band Based Adaptation Layer Techniques for Underwater Sensor Networks</td><td rowspan="3"></td></tr>
<tr><td>Applied Sciences</td></tr>
<tr><td>9(3187), 1-24</td></tr>
<tr><td rowspan="4">컴퓨터학</td><td></td><td>URL입력</td></tr>
<tr><td>2019</td><td rowspan="2">https://doi.org/10.3390/app9153187</td></tr>
<tr><td>https://doi.org/10.3390/app9153187</td></tr>
<tr><td colspan="8">수중통신 시스템은 주변 소음, 주파수 선택성, 다중 경로 및 도플러 이동과 같은 열악한 채널 조건에서 작동한다. 효과적으로 데이터를 수집하고 전송하기 위해, 본 논문에서는 다중매체/다중대역 기반의 적응 계층 기술을 제안한다. 데이터는 센서 노드에서부터 시작하여 여러 채널을 통한 계층적 방식으로 지표면 게이트웨이까지 전송된다. 수중환경에서 강력하고 신뢰할 수 있는 통신을 제공하기 위해, 적응 계층은 다중대역/다중매체 접근법을 사용하여 데이터를 전송한다. 따라서 본 논문에서는 주파수 대역을 분할하기 위해 기존의 대역분할기법을 사용하며, 수중에서</td></tr>
</table>

연번	참여교수명	연구자등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
	의 음파, 가시광선통신(VLC), 적외선(IR) 신호 등 다양한 매체를 통해 신호를 전달하는 '매체 선택 메커니즘'을 제안한다. 채널 선택 메커니즘에는 두 가지 단계가 포함된다. 첫 번째는 맨해튼 방법을 사용하여 근거리 및 원거리 노드의 거리를 찾는 것이고, 두 번째는 다양한 매체를 선택하기 위한 매체 선택 및 데이터 전송 알고리즘이다.						
12	박수현	10056675	이공계열	컴퓨터학 컴퓨터학	저널논문	Mukhridinkhon Ibragimov, Jae-Hoon Lee, Muppalla Kalyani, Jung-il Namgung, Soo-Hyun Park, Okyeon Yi, Chang Hwa Kim, Yong-Kon Lim	
						CCM-UW Security Modes for Low-band Underwater Acoustic Sensor Networks	
						Wireless Personal Communications	
						89, 479–499	
							URL입력
						2016	https://doi.org/10.1007/s11277-016-3283-z
						https://doi.org/10.1007/s11277-016-3283-z	
	본 논문에서는 보안 알고리즘에 더불어 메커니즘을 송신/삭제해 달라는 요청에 근거한 '수중 미디어 액세스 제어 프로토콜'을 간략하게 설명한다. 이는 데이터 기밀성, 신뢰성 및 재생 공격 보호를 제공하기 위해 제안되는 것이다. 이 프로토콜은 고급 암호화 표준/기관, 연구기관, 연구소, 학교의 블록 암호 알고리즘에 기반한 수중 음향 통신용 CCBC-MAC(CCM*) 모드에서 수정된 형태의 카운터, 즉 수중 CCM-UW 모드에 대한 암호 블록 체인-메시지 인증 코						

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="2"></td><td colspan="7">드(CBC-MAC)를 가진 카운터를 포함한다. CCM-UW 보안 메커니즘은 수중 음향 센서 네트워크(UWASN)에 적합하며 보안 강도, 에너지 소비량 및 전송 시간이 다른 6가지 보안 수준을 제공한다. 본 논문의 결과는 에너지 효율성과 전송 시간 단축이라는 측면에서 이 프로토콜이 UWASN에 대해 실행 불가능한 것은 아님을 보여준다.</td></tr>
<tr><td rowspan="2">13</td><td rowspan="2">서석충</td><td rowspan="2">10875717</td><td rowspan="2">이공계열</td><td rowspan="2">컴퓨터학
컴퓨터보안</td><td rowspan="2">저널논문</td><td>Seog Chung Seo, HeeSeok Kim</td><td></td></tr>
<tr><td>SCA-Resistant GCM implementation on 8-bit AVR Microcontrollers
IEEE Access 7
103961-103978

2019
https://doi.org/10.1109/ACCESS.2019.2930986</td><td>URL입력
https://doi.org/10.1109/ACCESS.2019.2930986</td></tr>
<tr><td colspan="7">본 연구에서는 8비트 AVR 마이크로컨트롤러 환경에서 안전한 GCM 구현을 제시한다. 제안된 구현은 SPA/TA 뿐만 아니라 DPA/CPA를 고려하여 포괄적인 SCA 보안을 제공한다. SPA/TA를 대비하기 위해 Garbage 레지스터와 ILA를 사용하여 더미 XOR 연산 개념을 소개하고 이를 사용하여 보안 이진체(Binary Field) 곱셈 방법을 제공한다. 또한 GCM 프로세스에서 GHASH 기능을 사용할 때 DPA/CPA를 방지할 수 있는 효율적인 곱셈 마스킹 방법을 제안한다. 8비트 AVR 마이크로컨트롤러에서의 제안된 방법과 실제 구현을 통해 제안된 방법이 기존의 대안을 능가하면서 포괄적인</td></tr>
</table>

연번	참여교수명	연구자등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
	SCA 보안을 제공함을 보여준다. 국제 저명 저널이며 impact factor가 4.098인 IEEE Access에 게재되었다.						
14	서석충	10875717	이공계열	컴퓨터학 컴퓨터보안	저널논문	Seog Chung Seo, Hwajeong Seo	
						Highly Efficient Implementation of NIST-compliant Koblitz Curve for 8-bit AVR-based Sensor Nodes	
						IEEE Access 6	
						67637-67652	
							URL입력
						2018	https://doi.org/10.1109/ACCESS.2018.2878777
						https://doi.org/10.1109/ACCESS.2018.2878777	
	지금까지 NIST 기준 곡선에 대한 여러 ECC 구현이 8비트 센서 노드에 제공되었다. 그러나 대부분 NIST에서 권장하는 112비트 보안 수준을 제공하지 않는다. 일부 작업은 112비트 이상의 보안 수준을 제공하지만 리소스가 제한된 센서 노드에서 제대로 실행되도록 성능 개선이 필요했다. 본 연구에서는 무선 센서 네트워크의 센서 노드에 일반적으로 사용되는 8비트 AVR 마이크로컨트롤러를 위한 NIST K-233 곡선을 통해 ECC를 효율적으로 구현하는 방법을 제시한다. 곱셈에 필요한 레지스터를 줄이는 새로운 다항식 곱셈 기술을 제공하고 8비트 AVR 기능을 고려한 제곱과						

연번	참여교수명	연구자등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
	감산 알고리즘을 최적화 하였다. 결과적으로 NIST K-233 곡선보다 고속 버전과 고안전도 버전으로 두 가지 ECC 구현물을 제공한다. 국제 저명 저널이며 impact factor가 4.098인 IEEE Access에 게재되었다.						
15	서석충	10875717	이공계열	컴퓨터학 컴퓨터보안	저널논문	Seog Chung Seo, Taehong Kim, Seokhie Hong	
						Accelerating Elliptic Curve Scalar Multiplication over GF(2^m) on Graphic	
						Elsevier Journal of Parallel and Distributed Computing	
						75, 152-167	
							URL입력
						2015	https://doi.org/10.1016/j.jpdc.2014.09.001
						https://doi.org/10.1016/j.jpdc.2014.09.001	
	IT 기술의 발달로 BYOD 시대가 되면서 사람들은 적어도 하나 이상의 모바일 장치들을 이용하ㅕ 다양한 인터넷 기반 IT 서비스를 제공받고 있다. PC를 통하여 서버에 접속하여 서비스를 제공받던 에전과는 달리 현재는 개인 모바일 장치를 통하여 서버에 접속하여 서비스를 제공받기 때문에 서버에서 서비스를 제공해야 하는 장치의 수가 크게 증가하였다. 서버에서 사용자 장치들에게 안전한 서비스를 제공해주기 위해서는 안전한 세션을 생성해야 하며 이는 공개키 암호 알고리즘을 기반으로 한다. 따라서 서버에서는 많은 수의 공개키 암호 연산을 빠르고 효율적으로 수행						

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="2"></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="7">할 필요가 있다. 본 연구에서는 서버 환경에서 GPU를 통하여 차세대 공개키 암호인 타원곡선 암호 연산을 효율적으로 수행할 수 있는 방법을 제시한다. impact factor가 1.819인 Elsevier Journal of Parallel and Distributed Computing에 게재되었다.</td></tr>
<tr><td rowspan="2">16</td><td rowspan="2">윤상민</td><td rowspan="2">10701285</td><td rowspan="2">이공계열</td><td rowspan="2">컴퓨터학
인공지능</td><td rowspan="2">저널논문</td><td>Jungwoo Choi, Heeryon Cho, Jinjoo Song, Sang Min Yoon</td><td></td></tr>
<tr><td>SketchHelper: Real-time Stroke Guidance for Freehand Sketch Retrieval
7 IEEE Trans. Multimedia
21, 2083-2092

2019
https://doi.org/10.1109/TMM.2019.2892301</td><td>URL입력
https://doi.org/10.1109/TMM.2019.2892301</td></tr>
<tr><td colspan="7">본 논문은 Image retrieval등 다양한 분야에서 응용될 수 있는 freehand sketch에 대한 연구이다. Sketch를 기반으로 하는 영상 복원 방법들은 정형화되고 완성된 밑그림을 요구한다. 하지만 많은 사용자들이 이와 같은 밑그림을 그릴 수 없기 때문에 딥러닝을 이용하여 사용자가 그은 획으로 의도한 밑그림을 예측하고 이를 위한 다음 획을 추천해서 밑그림에 익숙하지 않은 사용자도 손쉽게 정형화된 밑그림을 완성할 수 있도록 도와준다.Impact Factor: 5.452, 분야별 상위 5%이내</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="8">17</td><td rowspan="7">윤상민</td><td rowspan="7">10701285</td><td rowspan="7">이공계열</td><td rowspan="3">컴퓨터학

인공지능</td><td rowspan="7">저널논문</td><td>Hyeong Jae Hwang, Gang-Joon Yoon, Sang Min Yoon</td><td></td></tr>
<tr><td>Optimized Clustering Scheme-Based Robust Vanishing Point Detection</td><td rowspan="3"></td></tr>
<tr><td>IEEE Trans. Intelligent Transportation System</td></tr>
<tr><td>21, 199-208</td></tr>
<tr><td></td><td>URL입력</td></tr>
<tr><td>2020</td><td rowspan="2">https://doi.org/10.1109/TITS.2018.2890364</td></tr>
<tr><td>https://doi.org/10.1109/TITS.2018.2890364</td></tr>
<tr><td colspan="7">본 논문은 자율 주행 등 영상 분석을 위해 사용되는 Vanishing Point에 관한 연구이다.
영상 기반 깊이 정보를 획득하기 위하여 영상으로부터 Vanishing point 후보군을 찾고 Sphere Domain임을 이용하여 강건한 후보군을 찾고 최적화 하기 위한 기법을 제안하는 방법으로서 , 인공지능 기반 자동 소실점 검출 및 활용과 관련된 기술을 개발하였다.
Impact Factor: 5.744, 분야별 상위 5%이내</td></tr>
<tr><td rowspan="8">18</td><td rowspan="7">윤상민</td><td rowspan="7">10701285</td><td rowspan="7">이공계열</td><td rowspan="3">컴퓨터학

인공지능</td><td rowspan="7">저널논문</td><td>Jinjoo Song, Gangjoon Yoon, Kwangsoo Hahn, Sang Min Yoon</td><td></td></tr>
<tr><td>Subspace Clustering via structure-enforced Dictionary Learning</td><td rowspan="3"></td></tr>
<tr><td>Elsvier Journal of Neurocomputing</td></tr>
<tr><td>362, 1-10</td></tr>
<tr><td></td><td>URL입력</td></tr>
<tr><td>2019</td><td rowspan="2">https://doi.org/10.1016/j.neucom.2019.07.025</td></tr>
<tr><td>https://doi.org/10.1016/j.neucom.2019.07.025</td></tr>
<tr><td colspan="7">고차원의 데이터들은 차원의 저주와 같은 본질적인 문제를 갖고 있다.
본 논문은 고차원의 데이터를 여러 개의 작은 Subspace들의 집합으로 표현 될 수 있다는 관점을 이용해서 구조화 된 PCA 기반의 dictionary learning으로 고차원의 데이터를 여러 개의 subspace로 나누고 군집화 한다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="8">19</td><td rowspan="8">염용진</td><td rowspan="8">10090653</td><td rowspan="8">이공계열</td><td rowspan="4">수학</td><td rowspan="8">저널논문</td><td>Taeill Yoo, Ju-Sung Kang, and Yongjin Yeom</td><td></td></tr>
<tr><td>Recoverable Random Numbers in an Internet of Things Operating System</td><td rowspan="3"></td></tr>
<tr><td>Entropy</td></tr>
<tr><td rowspan="2">19(3)</td></tr>
<tr><td rowspan="4">해석학</td><td></td><td>URL입력</td></tr>
<tr><td>2017</td><td rowspan="2">https://doi.org/10.3390/e19030113</td></tr>
<tr><td>https://doi.org/10.3390/e19030113</td></tr>
<tr><td colspan="7">본 논문은 Google이 개발한 IoT 운영체제인 Brillo에서 사용하는 Linux 난수발생기(LRNG)의 동작을 분석하여 700바이트의 난수의 엔트로피가 단지 약 43비트임을 보여준다. 본 논문에서는 부팅 시 동작하는 특징을 관찰하였다. 첫 번째 특징은 부팅 시 입력 풀의 엔트로피 카운터가 192비트 미만이어서 불충분한 엔트로피를 가진다는 것이고, 두 번째는 잡음원 입력 순서와 난수 출력 순서가 일정하여 동일한 패턴을 가진다는 것이다. 이러한 특징을 사용하여 부팅 시 생성되는 700바이트의 난수를 90% 성공 확률로 복구할 수 있음을 보여준다. 즉, 700바이트의 난수의 엔트로피가 약 43비트임을 보여준다. 운영체제의 부팅 시 생성된 초기 난수는 민감한 보안 매개 변수에 사용되기 때문에, 본 논문의 결과는 암호 시스템에 대한 실제 공격에 적용할 수 있다.
SCIE, IF=2.419(2018 Journal Impact Factor, 출처: Web of Science)</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="8">20</td><td rowspan="8">염용진</td><td rowspan="8">10090653</td><td rowspan="8">이공계열</td><td rowspan="4">수학</td><td rowspan="8">저널논문</td><td>Yongjin Yeom, Ju-Sung Kang</td><td></td></tr>
<tr><td>Probability distributions for the Linux entropy estimator</td><td rowspan="3"></td></tr>
<tr><td>Discrete Applied Mathematics</td></tr>
<tr><td rowspan="4">해석학</td><td>241, 87-99</td></tr>
<tr><td>2/2</td><td>URL입력</td></tr>
<tr><td>2018</td><td rowspan="2">https://doi.org/10.1016/j.dam.2016.07.019</td></tr>
<tr><td>https://doi.org/10.1016/j.dam.2016.07.019</td></tr>
<tr><td colspan="7">본 논문은 Linux 난수발생기(LRNG)에서 사용하는 엔트로피 추정기의 수학적 모델을 제안한다. 경험적 엔트로피 분석에 따르면 LRNG에 의해 계산된 추정 엔트로피가 경험적 빈도수에 기반한 엔트로피보다 낮다. LRNG의 출력 난수는 엔트로피 소스에 의해 완전히 결정되므로, 잡음원에서 수집된 엔트로피의 양을 정확히 추정하는 것이 매우 중요하다. 본 논문에서는 랜덤한 이벤트 시간에 대한 확률 모델을 구성한 다음 첫 번째, 두 번째 및 세 번째 시간 차이에 대한 확률 분포를 정확하게 도출한다. 그리고 LRNG에서 엔트로피를 추정하는 데 사용되는 이러한 차이의 최소 절댓값에 대한 확률 분포를 도출한다. 본 연구 결과는 일반적인 랜덤한 시간 차이로부터 생성된 잡음원에서 엔트로피가 수집되는 경우 엔트로피가 정확하게 추정되지 않아 발생하는 안전성 문제를 완화하는데 기여한다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="8">21</td><td rowspan="8">염용진</td><td rowspan="8">10090653</td><td rowspan="8">이공계열</td><td rowspan="4">수학</td><td rowspan="8">저널논문</td><td>Yongjin Yeom, Dong-Chan Kim, CHung Hun Baek, and Junbum Shin</td><td></td></tr>
<tr><td>Cryptoanalysis of the Obfuscated Round Boundary Technique for Whitebox Cryptography</td><td rowspan="3"></td></tr>
<tr><td>SCIENCE CHINA-INFORMATION SCIENCES</td></tr>
<tr><td rowspan="4">해석학</td><td>63(3)</td></tr>
<tr><td></td><td>URL입력</td></tr>
<tr><td>2020</td><td rowspan="2">https://doi.org/10.1007/s11432-019-9883-9</td></tr>
<tr><td>https://doi.org/10.1007/s11432-019-9883-9</td></tr>
<tr><td colspan="7">본 논문은 RBO-WBAES(10, 500)라는 AES의 화이트박스 구현에 대한 키 복구 공격을 구성한다. 2018년 Xu et al.은 난독화된 라운드 경계 기법(obfuscated round boundary technique)이라는 새로운 설계 근거를 제안하였고, 이는 테이블에서 각 라운드를 식별하는 것을 방해하여 구조로부터 키 정보를 추출하는 것을 어렵게 한다. 하지만, 본 논문에서는 SAS와 SASAS 구조의 차이점을 분석하여 RBO-WBAES에 대한 키 복구 공격을 제시한다. 또한, 룩업 테이블을 사용한 화이트박스 구현은 필연적으로 SAS 구조를 가진 큰 크기의 테이블을 사용하기 때문에, 본 연구 결과를 통해 테이블에 숨겨진 키 정보를 추출할 수 있다.
SCI, IF=2.731(2018 Journal Impact Factor, 출처: Web of Science)</td></tr>
</table>

연번	참여교수명	연구자등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
22	이옥연	10056884	이공계열	컴퓨터학 유무선통신보안	저널논문	Hyunki Kim, Jaehoon Lee, Okyeon Yi	
						Proposal of Piecewise Key Management Design Considering Capability of Underwater Communication Nodes	
						Journal of Computational and Theoretical Nanoscience	
						23(12), 12729-12733	
							URL입력
						2017	https://doi.org/10.1166/asl.2017.10888
						https://doi.org/10.1166/asl.2017.10888	
	본 논문은 수중 센서에 의해 생성된 모든 데이터에 보안을 적용하기 위해 수중 보안 통신을 진행하는 엔티티 간 키 관리 방법 및 요구사항을 제안한다. 무선 센서 네트워크 인프라에서는 다수의 센서로부터 데이터를 모아 전송하는 중간노드와 상위노드의 수가 많지 않고 각 개체의 크기가 작지 않으며 일반적으로 기기의 성능이 보장되기 때문에 질 좋은 통신과 잘 정의되어 있는 보안을 적용할 수 있다. 하지만 노드의 수가 많아 기기의 값이 저렴해야 하고 그로 인해 상위 노드만큼의 성능이 보장되지 않는 센서 단말같은 하위 노드 등은 중간노드와 통신을 할 때 질 좋은 통신을 사용하기 어렵다. 따라서 무선 센서네트워크의 일종인 수중 통신에서 이룰 수 있는 전반적인 네트워크 구조를 제시하고 각 노드 간, 각 부분에서 보안을 적용해야 할 부분과, 보안요구사항을 제시한다.						

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="8">23</td><td rowspan="8">이옥연</td><td rowspan="8">10056884</td><td rowspan="8">이공계열</td><td rowspan="4">컴퓨터학

유무선통신보안</td><td rowspan="8">저널논문</td><td>Hansaem Wi, Chan-Guk Jang, Jaehoon Lee, Okyeon Yi</td><td></td></tr>
<tr><td>Suggestion SSL-VPN for Traffic Signal Control System</td><td rowspan="3"></td></tr>
<tr><td>Advanced Science Letters</td></tr>
<tr><td>23(12), 12725-12728</td></tr>
<tr><td></td><td>URL입력</td></tr>
<tr><td>2017</td><td rowspan="2">https://doi.org/10.1166/asl.2017.10887</td></tr>
<tr><td>https://doi.org/10.1166/asl.2017.10887</td></tr>
<tr><td colspan="7">본 논문은 교통신호제어시스템의 보안을 위해 SSL-VPN을 제안한 논문이다. 또한 SSL-VPN의 구현과 SSL-VPN을 적용하기 위한 구현 환경에 대해서도 설명한다. 이는 지능형 교통 시스템이 빠르게 개발됨에 따라, 교통신호제어시스템의 통신 방법은 모바일 네트워크 및 공용 네트워크를 사용하는 폐쇄망에서 3G/LTE 와 같은 이동통신으로 변화하고 있는 현시점에 필수적인 요소이다. 이에 따라 변경된 교통신호제어시스템은 데이터 감시, 데이터 수정 등과 같은 위협에 노출될 수 있기 때문에 End-To-End 보안을 적용할 수 있는 SSL-VPN을 교통신호 제어시스템에 적용하여 논문에서 제시한 보안 위협을 방지한다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="8">24</td><td rowspan="8">이옥연</td><td rowspan="8">10056884</td><td rowspan="8">이공계열</td><td rowspan="4">컴퓨터학

유무선통신보안</td><td rowspan="8">저널논문</td><td>Chan-Kuk Jang, JaeHoon Lee, Okyeon Yi</td><td></td></tr>
<tr><td>Encryption scheme in portable electric vehicle charging infrastructure: Encryption scheme using symmetric key</td><td rowspan="3"></td></tr>
<tr><td>International Conference on Computer Applications and Information Processing Technology (CAIPT)</td></tr>
<tr><td>17650166</td></tr>
<tr><td></td><td>URL입력</td></tr>
<tr><td>2017</td><td rowspan="2">https://doi.org/10.1109/CAIPT.2017.8320674</td></tr>
<tr><td>https://doi.org/10.1109/CAIPT.2017.8320674</td></tr>
<tr><td colspan="8">본 논문은 휴대용 EV 충전 인프라가 보다 빨리 보급되기 위해서 보안 서비스의 제공이 필요하다는 점을 강조하면서 기존 서비스에 보안을 제공함과 동시에 안전한 EV 충전 시스템을 구축하는데 비용과 암호화 속도가 전체 서비스 유지를 위해 큰 문제가 아니라는 것을 보여준 논문이다.</td></tr>
<tr><td rowspan="8">25</td><td rowspan="8">최은미</td><td rowspan="8">10116354</td><td rowspan="8">이공계열</td><td rowspan="4">컴퓨터학

컴퓨터학</td><td rowspan="8">저널논문</td><td>Eunmi Choi</td><td></td></tr>
<tr><td>A basis of spatial big data analysis with map-matching system</td><td rowspan="3"></td></tr>
<tr><td>Journal of Cluster Computing</td></tr>
<tr><td>20, 2177–2192</td></tr>
<tr><td></td><td>URL입력</td></tr>
<tr><td>2017</td><td rowspan="2">https://doi.org/10.1007/s10586-017-1014-1</td></tr>
<tr><td>https://doi.org/10.1007/s10586-017-1014-1</td></tr>
<tr><td colspan="8">디지털 운행 기록계는 대부분의 국내 상업용 차량에 사전 설치되어 있으며 안전한 운전 및 연료 소비 추정치와 같은 에코 드라이빙 지표를 분석하는 데 매우 유용하다. 다수의 GPS 위치 정보를 올바르게 분석하려면 공간 내 위치 데이터와 디지털 도로 네트워크 데이터가 정확히 일치하는 링크를 찾아야 한다. 본 연구진은 일반적으로 사용되는 맵-매칭 기술을 사용하여 GPS좌표의 도로 정보를 미리 알아냈으나, 맵-매칭 기술은 대량의 데이터를 빠르고 정확하</td></tr>
</table>

연번	참여교수명	연구자등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
	게 탐색하기 위해 많은 추가적인 수정이 필요로 한다. 본 연구에서는 공간 인덱스, 긴 링크 정점 분할, 속도 필터링, 방위각 필터링 및 맵 일치 가중치 논리로 Geohash를 사용하여 향상된 맵-매칭 로직을 적용했으며, HBase와의 빅 데이터 맵-매칭을 위한 분산 분석 환경을 구축하고 구현했다. 본 논문에서는 Hadoop MapReduce 메커니즘에서 맵-매칭 로직을 사용하여 공간 분석 시스템 성능을 향상시켰다.						
26	최은미	10116354	이공계열	컴퓨터학 컴퓨터학	저널논문	Eunmi Choi	
						Big data pre-processing methods with vehicle driving data using MapReduce techniques	
						Journal of Supercomputing	
						73(7), 3179-3195	
							URL입력
						2017	https://doi.org/10.1007/s11227-017-2014-x
						https://doi.org/10.1007/s11227-017-2014-x	
	빅 데이터 분야에서는 전처리가 필수적이지만 사례 대한 연구가 크게 부족했다. 본 논문에서는 빅 데이터 전처리 방법을 연구하고 제안한다. 보다 정확한 분석을 통해 전처리 방법을 평가하기 위해 DTG (Digital Tachograph) 데이터를 사용했다. 우리는 1년에 걸쳐 6198대의 운전 차량에 대한 DTG 데이터를 얻었다. 범위 필터링, 무의미한 값 제외, 변수에서 필터 비교, 통계 기법 적용 및 드라이빙 패턴 찾기의 5가지 전처리 방법을 연구했다. 또한 Hadoop 에						

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="3"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="7">코 시스템을 사용하여 MapReduce 프로그램을 개발하고 사전 처리 분석을 수행하기 위해 빅 데이터를 배포했다. 전처리 단계를 통해 오류를 포함한 DTG 감지 데이터 포인트의 비율이 최대 27.09%임을 확인했다. 기존의 무차별 대입 방식에 비해 71.1%의 추가 감지 효과가 있었다. 또한 간단한 범위의 오류 전처리를 통해 탐지하기 어려운 이상치 데이터 포인트를 잘 탐지 할 수 있음을 확인했다.</td></tr>
<tr><td rowspan="8">27</td><td rowspan="8">최은미</td><td rowspan="8">10116354</td><td rowspan="8">이공계열</td><td rowspan="4">컴퓨터학

컴퓨터학</td><td rowspan="8">저널논문</td><td>Eunmi Choi</td><td></td></tr>
<tr><td>A comprehensive evaluation of availability and operational cost for a virtualized server system using stochastic reward nets</td><td rowspan="3"></td></tr>
<tr><td>Journal of Supercomputing</td></tr>
<tr><td>74, 224-279</td></tr>
<tr><td></td><td>URL입력</td></tr>
<tr><td>2018</td><td rowspan="2">https://doi.org/10.1007/s11227-017-2127-2</td></tr>
<tr><td>https://doi.org/10.1007/s11227-017-2127-2</td></tr>
<tr><td colspan="7">본 논문에서는 확률 보상 보상망 (SRN)을 사용하여 m 개의 가상화 된 서버로 구성된 클러스터 모델을 제안한다. 전체 시스템의 전체 구성에 중점을 두었으며 모델링에서는 서버 간의 세부 상호 작용을 고려했으며, 고가용성을 위해 대기 기술, 가상 머신 실시간 마이그레이션 및 VM 장애 조치 기술이 통합되어 있다. 물리적 서버 및 VM의 단순화된</td></tr>
</table>

연번	참여교수명	연구자등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
	장애 및 복구 동작을 고려했다. 다양한 SRN 모델은 시스템의 전체 가용성을 향상시키는 기술이 차례로 통합된 다양한 사례 연구를 기반으로 개발된다. SSA (steady-state availability), SSA의 민감도 분석, 다운 타임 비용 및 운영 비용 분석 등 중요한 관심 지표로 모델에 대한 포괄적인 분석을 수행했다. 본 논문에서는 운영 비용을 쉽게 계산할 수 있도록 SRN에 포함된 보상 기능을 사용할 것을 제안한다. 그리고 데이터 센터에서 가상화 시스템의 시스템 조정 및 구성, 실제로 클라우드 컴퓨팅에 대한 분석 기반을 제공한다.						
28	한동국	10128486	이공계열	수학 암호론	저널논문	Yoo-Seung Won, Soung-Wook Choi, Dong-Won Park, Dong-Guk Han	
						Security of Constant Weight Countermeasures	
						ETRI Journal	
						39(3), 417-427	
							URL입력
						2017	https://doi.org/10.4218/etrij.17.0116.0876
						https://doi.org/10.4218/etrij.17.0116.0876	
	상용 암호화 장비는 부채널 분석에 내성을 갖도록 설계되어야 한다. 이를 위해 많은 종류의 대응기법들이 제시되었는데, 본 논문은 그중 하나인 constant weight 대응기법에 대한 안전성 분석을 진행하였다. 부채널 정보 누출 모델의 계수를 정규 분포에 따라 선택함으로써 실제 파형과 유사한 시뮬레이션 파형을 이용해 기존의 constant weight						

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="2"></td><td rowspan="7"></td><td rowspan="7"></td><td rowspan="7"></td><td rowspan="7"></td><td rowspan="7"></td><td></td><td></td></tr>
<tr><td></td><td rowspan="4"></td></tr>
<tr><td></td></tr>
<tr><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td rowspan="2"></td></tr>
<tr><td></td></tr>
<tr><td colspan="7">대응기법들에 대한 안전성 검증을 수행하였다. 그 결과, 기존에 제시된 대응기법들에 취약성이 존재하며 bitwise correlation power analysis를 통해 적은 수의 파형으로 비밀 키가 도출됨을 확인하였다. USIM이나 금융 IC 카드 등의 상용 장비에 부채널 대응기법을 적용하기 위해 기존의 constant weight 대응기법을 사용하는 것은 부채널 분석 취약점을 온전히 제거하지 못함을 시사하였다. SCIE급 저널이며 impact factor가 1.116인 ETRI Journal에 게재하였다.</td></tr>
<tr><td rowspan="8">29</td><td rowspan="8">한동국</td><td rowspan="8">10128486</td><td rowspan="8">이공계열</td><td rowspan="4">수학</td><td rowspan="8">저널논문</td><td>Bo-Yeon Sim, Junki Kang, Dong-Guk Han</td><td></td></tr>
<tr><td>Key Bit-Dependent Side-Channel Attacks on Protected Binary Scalar Multiplication</td><td rowspan="3"></td></tr>
<tr><td>Applied Sciences</td></tr>
<tr><td rowspan="4">8(11), 2168-2187</td></tr>
<tr><td rowspan="4">암호론</td><td>URL입력</td></tr>
<tr><td>2018</td><td rowspan="2">https://doi.org/10.3390/app8112168</td></tr>
<tr><td>https://doi.org/10.3390/app8112168</td></tr>
<tr><td colspan="7">공개키 암호 알고리즘인 ECC에 사용되는 이진 스칼라 곱셈은 부채널 분석에 취약함이 알려져 있다. 특히 단일 부채널 정보 내에서 패턴을 구분하는 단순 부채널 분석만으로도 키가 도출될 수 있다. 따라서 분기문에 따른 패턴 제거, 중간값에 따른 통계적 특성 제거, 데이터 간 관계성 제거 등을 목적으로 한 다양한 대응기법들이 제시되었다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>연구자등록번호</th><th>이공계열/인문사회계열</th><th>전공분야
세부전공분야</th><th>실적구분</th><th>대표연구업적물 상세내용</th><th>증빙</th></tr>
<tr><td colspan="7">대표연구업적물의 적합성과 우수성</td></tr>
<tr><td rowspan="3"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td></td><td></td></tr>
<tr><td></td><td rowspan="6"></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="8">본 논문에서는 기존의 대응기법들이 여전히 부채널 분석 관점에서의 취약점을 갖고 있음을 보였다. 널리 사용되는 공개 소프트웨어 라이브러리인 mbedTLS와 OpenSSL에서 사용하는 알고리즘에 본 논문에서 제시하고 있는 취약점이 존재하며 하드웨어로 구현된 Montgomery–López–Dahab ladder 알고리즘이 취약함을 보였다. 공개키 암호 알고리즘이 통신 분야에서 널리 사용됨을 견주어 보아, 본 논문에서 제시하고 있는 취약점은 파급력이 크다. 국제 저명 저널이며 impact factor가 2.217인 Applied Sciences에 게재되었다.</td></tr>
<tr><td rowspan="7">30</td><td rowspan="7">한동국</td><td rowspan="7">10128486</td><td rowspan="7">이공계열</td><td rowspan="4">수학

암호론</td><td rowspan="7">저널논문</td><td>Yoo-Seung Won, JongHyeok Lee, Dong-Guk Han</td><td></td></tr>
<tr><td>Side Channel Leakage Against Financial IC Card of the Republic of Korea</td><td rowspan="3"></td></tr>
<tr><td>Applied Sciences</td></tr>
<tr><td>8(11), 2258-2274</td></tr>
<tr><td></td><td>URL입력</td></tr>
<tr><td>2018</td><td rowspan="2">https://doi.org/10.3390/app8112258</td></tr>
<tr><td>https://doi.org/10.3390/app8112258</td></tr>
<tr><td colspan="8">본 논문은 국내 금융 IC 카드에서 표준으로 사용하고 있는 SEED 암호 알고리즘에 대한 신규 부채널 분석 기법을 제시하였다. SEED 암호 알고리즘의 G 함수의 특성을 이용하여 기존의 분석 기법의 키 추정량보다 현저히 낮은 키 추정량으로 분석이 가능함을 보였다. 기존의 부채널 분석 방법들은 혼돈 계층의 출력값을 대상 중간값으로 사용하는</td></tr>
</table>

연번	참여교수명	연구자등록번호	이공계열/인문사회계열	전공분야 세부전공분야	실적구분	대표연구업적물 상세내용	증빙
	대표연구업적물의 적합성과 우수성						
	분석법을 주로 사용하였다. 하지만 본 논문에서 제시하는 방법은 혼돈 계층 이후에 따라오는 확산 계층의 특성을 이용하는 방법을 제시한다. 국내 금융 IC 카드가 사용하고 있는 SEED 암호 알고리즘에 대해 효율적인 부채널 분석 방법을 제시함에 따라, 보다 수준 높은 안전성 테스트를 수행하는 데 이바지하고 있다. 국제 저명 저널이며 impact factor가 2.217인 Applied Sciences에 게재되었다.						

② 참여교수 특허, 기술이전, 창업 실적의 우수성

<표 3-3> 최근 5년간 이공계열 참여교수 특허, 기술이전, 창업 실적

<table>
<tr><th rowspan="2">연번</th><th>참여
교수
명</th><th>연구자
등록번호</th><th>전공
분야</th><th>실적
구분</th><th>특허, 기술이전, 창업 상세내용</th><th>증빙</th></tr>
<tr><td></td><td></td><td>세부
전공
분야</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="6">특허, 기술이전, 창업 실적의 우수성</td></tr>
<tr><td rowspan="6">1</td><td rowspan="5">강주성</td><td rowspan="5">10127144</td><td rowspan="3">수학</td><td rowspan="5">특허</td><td>염용진, 강주성, 배민영, 유동창, 유태일</td><td></td></tr>
<tr><td>다중 엔트로피 풀 지원 난수 발생기</td><td></td></tr>
<tr><td>대한민국</td><td>URL입력</td></tr>
<tr><td rowspan="2">확률과정론</td><td>10-1872329</td><td rowspan="2">https://patents.google.com/patent/KR101872329B1/ko</td></tr>
<tr><td>2018.06.22</td></tr>
<tr><td colspan="6">본 발명은 내부 상태 크기 변화를 필요로 하는 환경에서 난수발생기의 전면 재설계 없이 간편하게 풀 크기를 확장 및 축소할 수 있는 다중 엔트로피 풀 지원 난수발생기에 관한 것이다. 발명한 난수발생기는 난수 처리부와 난수 입출력 래퍼부(wrapper unit)로 구성되어 있다. 난수 처리부는 독립적인 내부상태를 기초로 주어진 입력 잡음원에 대해 난수를 출력하는 복수의 난수 발생부들을 포함한다. 난수 입출력 래퍼부는 난수 생성 과정에서 상기 복수의 난수 발생부들 중 특정 난수 발생부를 선택하여 입력 잡음원을 제공하고, 난수 출력 과정에서 상기 특정 난수 발생부로부터 출력된 특정 난수를 출력한다. 본 발명은 내부 상태를 확장하여 재구축 시 기존 설계 함수를 재사용 가능하여 높은 경제성을 갖는다. 또한, 다중 엔트로피 풀 지원에 있어서, 모든 입력 잡음원의 값을 알아내야만 잡음원의 입력 순서와 난수 출력에 사용될 풀의 순서를 알 수 있게 하여 안전성을 향상시킬 수 있다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여
교수
명</th><th>연구자
등록번호</th><th>전공
분야

세부
전공
분야</th><th>실적
구분</th><th>특허, 기술이전, 창업 상세내용</th><th>증빙</th></tr>
<tr><td colspan="6">특허, 기술이전, 창업 실적의 우수성</td></tr>
<tr><td rowspan="6">2</td><td rowspan="5">강주성</td><td rowspan="5">10127144</td><td rowspan="2">수학</td><td rowspan="5">특허</td><td>강주성, 염용진, 박호중</td><td></td></tr>
<tr><td>경량 난수 헬쓰 테스트 장치</td><td></td></tr>
<tr><td rowspan="3">확률과정론</td><td>대한민국</td><td>URL입력</td></tr>
<tr><td>10-1981623</td><td rowspan="2">https://patents.google.com/patent/KR20190049283A/ko</td></tr>
<tr><td>2019.05.17</td></tr>
<tr><td colspan="6">발명한 장치는 엔트로피 소스로부터 엔트로피를 입력받는 엔트로피 입력부와 상기 입력받은 엔트로피에 관하여 비모수적 순열 검정을 통한 경량 IID 테스트를 수행하여 상기 엔트로피 소스를 검정하는 엔트로피 소스 검정부를 포함한다. 엔트로피 소스 검정부는 IID 가설을 검증하기 위해 랜덤 수열의 카이제곱 통계량을 계산하고, 이를 특정 기준과 대소 비교하여 상대적으로 큰 그룹, 동일 그룹 및 상대적으로 작은 그룹으로 구성된 3개의 그룹들로 분류한다. 그런 다음, 계산된 카이제곱 통계량이 상기 3개의 그룹들로 오차 범위 내에서 균등하게 분배되지 않은 경우에는 랜덤 수열의 IID 가설을 검정 실패로 판정한다. 발명한 장치는 난수 출력 전에 온-더-플라이(on-the-fly) 방식으로 엔트로피 소스를 검정할 수 있다. 본 발명은 기존 테스트 방법보다 적은 데이터로 랜덤 수열의 IID 가설을 효과적으로 검정할 수 있다는 이점이 있다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여
교수
명</th><th>연구자
등록번호</th><th>전공
분야</th><th>실적
구분</th><th>특허, 기술이전, 창업 상세내용</th><th>증빙</th></tr>
<tr><td></td><td></td><td>세부
전공
분야</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="6">특허, 기술이전, 창업 실적의 우수성</td></tr>
<tr><td rowspan="6">3</td><td rowspan="5">박수현</td><td rowspan="5">10056675</td><td rowspan="3">컴퓨터학</td><td rowspan="5">특허</td><td>염선호, 남궁정일, 신수영, 박수현</td><td></td></tr>
<tr><td>하이브리드 수중무선통신 장치 및 그 통신 방법</td><td></td></tr>
<tr><td>대한민국</td><td>URL입력</td></tr>
<tr><td rowspan="2">컴퓨터학</td><td>10-2041432</td><td rowspan="2">https://patents.google.com/patent/KR102041432B1/ko</td></tr>
<tr><td>2019</td></tr>
<tr><td colspan="6">본 발명은 적어도 하나의 수중무선통신매체를 선택하여 효과적으로 수중무선통신을 수행할 수 있게 한다. 다수의 수중환경 데이터를 검출하는 단계; 외부로부터 수신된 데이터 및 내부에서 생성된 데이터를 이용하여 외부 수신장치로 전송하고자 하는 전송패킷을 생성하는 단계; 상기 생성된 전송패킷의 헤더를 분석하여 상기 전송패킷이 우선순위를 요구하는 긴급패킷인지를 판단하는 단계; 상기 전송패킷이 긴급패킷이면 현재 가용가능한 모든 수중무선통신매체를 통해 상기 긴급패킷을 전송하도록 하고 긴급패킷이 아니면 상기 검출된 수중환경 데이터를 바탕으로 상기 전송패킷에 대한 통신장애요소가 있는지를 판단하는 단계; 상기 판단결과 통신장애요소가 없으면 상기 전송패킷이 고속통신을 요구하는지를 판단하는 단계; 및 상기 전송패킷이 고속통신을 요구하는 경우 기설정된 거리 내에 상기 전송패킷을 수신가능한 수신장치가 존재하는지 확인하여 존재하면 상기 전송패킷을 가시광 통신매체로 전송하는 단계를 포함한다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여
교수
명</th><th>연구자
등록번호</th><th>전공
분야</th><th>실적
구분</th><th>특허, 기술이전, 창업 상세내용</th><th>증빙</th></tr>
<tr><td></td><td></td><td>세부
전공
분야</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="6">특허, 기술이전, 창업 실적의 우수성</td></tr>
<tr><td rowspan="5">4</td><td rowspan="5">박수현</td><td rowspan="5">10056675</td><td rowspan="3">컴퓨터학</td><td rowspan="5">특허</td><td></td><td></td></tr>
<tr><td>수중 사물인터넷 장치에서의 Ｐ２Ｐ 기반 서비스 디스커버리 방법 및 그 수중 사물인터넷 장치</td><td></td></tr>
<tr><td>대한민국</td><td>URL입력</td></tr>
<tr><td rowspan="2">컴퓨터학</td><td>10-1801061</td><td rowspan="2">https://patents.google.com/patent/KR101801061B1/ko</td></tr>
<tr><td>2017</td></tr>
<tr><td colspan="6">본 발명은 사물인터넷(IoT) 통신장치에서 P2P 기반으로 이기종의 네트워크상에 제공하는 다양한 응용서비스를 검색 및 접근 가능하도록 하는 수중 사물인터넷 장치에서의 P2P 기반의 서비스 디스커버리 방법 및 그 수중 사물인터넷 장치에 관한 것이다. 본 발명에 따른 P2P 기반의 서비스 디스커버리 방법을 적용한 수중 사물인터넷 장치는, 지상 또는 수중 통신 프로토콜을 이용하여 지상 사물인터넷 장치 또는 다른 수중 사물인터넷 장치와 통신을 수행하는 수중 사물인터넷 프로토콜부; 상기 수중 사물인터넷 프로토콜부와 통신하며 서비스 디스커버리를 수행하기 위한 P2P 오버레이 네트워크를 형성하고 서비스 검색요청에 따라 서비스 검색을 수행하여 서비스 검색결과를 응답하는 서비스 디스커버리 기능부; 및 상기 수중 사물인터넷 프로토콜부와 상기 서비스 디스커버리 기능부 간의 통신을 위한 인터페이스를 처리하는 교차계층인터페이스부를 포함한다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여
교수
명</th><th>연구자
등록번호</th><th>전공
분야

세부
전공
분야</th><th>실적
구분</th><th>특허, 기술이전, 창업 상세내용</th><th>증빙</th></tr>
<tr><td colspan="6">특허, 기술이전, 창업 실적의 우수성</td></tr>
<tr><td rowspan="6">5</td><td rowspan="5">염용진</td><td rowspan="5">10090653</td><td rowspan="3">수학

해석학</td><td rowspan="5">특허</td><td>염용진, 김상필, 유태일, 김나영, 주왕호, 강주성</td><td></td></tr>
<tr><td>LEA 블록암호의 화이트박스 암호 구현 장치 및 방법</td><td></td></tr>
<tr><td>대한민국</td><td>URL입력</td></tr>
<tr><td>10-1623503</td><td rowspan="2">https://patents.google.com/patent/KR101623503B1/ko</td></tr>
<tr><td>2016</td></tr>
<tr><td colspan="6">본 발명은 암호키를 포함한 암호 알고리즘을 다수의 테이블로 구성하여 암호 알고리즘의 소스코드나 메모리 영역의 조사 등을 통해 암호키를 찾는 것을 원천적으로 막을 수 있는 LEA 블록암호의 화이트박스 암호 구현 장치 및 방법을 제공하기 위한 것이다. 평문 입력부는 인코딩된 평문을 입력받고 암호문 출력부는 상기 라운드 함수부에서 처리된 출력값 중 모든 라운드 키에 대한 라운드 함수부 수행이 완료되어 출력되는 결과값인 인코딩 암호문을 출력한다. 본 발명에 따른 LEA 블록암호의 화이트박스 암호 구현 장치 및 방법은 암호키를 하드웨어 토큰에 저장하지 않고도 암호키의 해킹이나 탈취로부터 방어할 수 있다. 또한, 금융거래 등에 사용되는 암호모듈의 구현시 난독화 기술과 함께 사용되면 안전성을 크게 강화할 수 있는 효과가 있다.</td></tr>
</table>

연번	참여 교수 명	연구자 등록번호	전공 분야 / 세부 전공 분야	실적 구분	특허, 기술이전, 창업 상세내용	증빙
	특허, 기술이전, 창업 실적의 우수성					
6	염용진	10090653	수학 / 해석학	기술이전	염용진, 강주성	
					암호알고리즘 실행과정에서의 암호키 보호기술	
					이니텍	URL입력
					30,000(천원)	
					2016.10.07	
	화이트박스 암호는 암호 소프트웨어에 대한 완전한 접근을 할 수 있고 실행되는 환경에 대한 모든 조작이 가능한 화이트박스 공격자가 있는 경우에도 안전하게 암호키를 숨기면서 암호 기능을 제공하는 기술이다. 종래의 화이트박스 암호화 기술은 높은 안전성을 구현하고자 하는 경우 테이블의 크기가 지나치게 커지기 때문에 사물인터넷이나 모바일 기기를 위한 경량 환경에 적합하게 구현하기 어려운 단점이 있다. 따라서 본 연구단은 이러한 문제를 해결하기 위해 발명한 경량 블록암호인 LEA의 화이트박스 구현 장치 및 방법과 화이트박스 LEA 프로그램을 이니텍에 기술이전하였고, 이를 통해 이니텍에서 개발하는 금융 서비스 관련 제품의 안전성을 강화하는 데 기여하였다.					

<table>
<tr><th rowspan="2">연번</th><th>참여
교수
명</th><th>연구자
등록번호</th><th>전공
분야</th><th rowspan="2">실적
구분</th><th>특허, 기술이전, 창업 상세내용</th><th>증빙</th></tr>
<tr><th>세부
전공
분야</th></tr>
<tr><td colspan="7">특허, 기술이전, 창업 실적의 우수성</td></tr>
<tr><td rowspan="6">7</td><td rowspan="5">윤상민</td><td rowspan="5">10701285</td><td rowspan="2">컴퓨터학</td><td rowspan="5">특허</td><td>윤상민, 최정우</td><td></td></tr>
<tr><td>스케치 기반의 영상표절 검사 방법 및 장치</td><td></td></tr>
<tr><td rowspan="3">인공지능</td><td>대한민국</td><td>URL입력</td></tr>
<tr><td>10-2058393</td><td rowspan="2">https://patents.google.com/patent/KR102058393B1/ko</td></tr>
<tr><td>2019</td></tr>
<tr><td colspan="6">본 발명은 스케치 기반의 영상표절 검사 방법 및 장치에 관한 것으로 사용자 영상을 수신하는 사용자 영상 수신부, CNN(Convolution Neural Network, 합성곱 신경망) 기반의 영상 분류를 통해 상기 사용자 영상에 관한 특정 영상 카테고리와 영상 특징을 검출하는 영상 특징 검출부, 검출된 상기 영상 특징을 해시 코드화하여 영상 해시 코드(Hash Code)를 생성하는 해시 코드화부 및 상기 특정 영상 카테고리에 있는 적어도 하나의 해당 학습 영상의 해시 코드 각각으로부터 상기 영상 해시 코드와 가장 유사한 유사 학습 영상을 결정하여 표절 검사를 수행하는 표절 검사 수행부를 포함한다. 따라서, 본 발명은 사용자가 입력한 영상을 인식하여 표절여부를 검사할 수 있다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여
교수
명</th><th>연구자
등록번호</th><th>전공
분야</th><th rowspan="2">실적
구분</th><th rowspan="2">특허, 기술이전, 창업 상세내용</th><th rowspan="2">증빙</th></tr>
<tr><th>세부
전공
분야</th></tr>
<tr><td colspan="7">특허, 기술이전, 창업 실적의 우수성</td></tr>
<tr><td rowspan="6">8</td><td rowspan="5">윤상민</td><td rowspan="5">10701285</td><td rowspan="3">컴퓨터학</td><td rowspan="5">특허</td><td>윤상민, 원용욱</td><td></td></tr>
<tr><td>순환 신경망 기반 네트워크 패킷의 위험요소 분석 방법, 이를 수행하는 순환 신경망 기반 네트워크 패킷의 위험요소 분석 장치</td><td></td></tr>
<tr><td rowspan="3">인공지능</td><td>대한민국</td><td>URL입력</td></tr>
<tr><td>10-1927100</td><td rowspan="2">https://patents.google.com/patent/KR101927100B1/ko</td></tr>
<tr><td>2019</td></tr>
<tr><td colspan="6">본 발명은 순환 신경망 환경에서 네트워크 패킷의 위험 요소를 분석하고 이에 대한 방어 체계를 구축하기 위하여 딥러닝 기반의 네트워크 환경 구성 및 순환 신경망 환경에서의 네트워크 패킷의 위험 요소를 분석할 수 있다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여
교수
명</th><th>연구자
등록번호</th><th>전공
분야</th><th rowspan="2">실적
구분</th><th>특허, 기술이전, 창업 상세내용</th><th>증빙</th></tr>
<tr><th>세부
전공
분야</th></tr>
<tr><td colspan="7">특허, 기술이전, 창업 실적의 우수성</td></tr>
<tr><td rowspan="6">9</td><td rowspan="5">이옥연</td><td rowspan="5">10056884</td><td rowspan="3">컴퓨터학</td><td rowspan="5">특허</td><td>이옥연, 송행권, 황누리, 안현정, 윤승환, 김현기, 장찬국</td><td></td></tr>
<tr><td>사물인터넷 기반의 DUSS(Different Units Same Security) 장치</td><td></td></tr>
<tr><td>대한민국</td><td>URL입력</td></tr>
<tr><td rowspan="2">유무선통신보안</td><td>10-1938312</td><td rowspan="2">https://patents.google.com/patent/KR101938312B1/ko</td></tr>
<tr><td>2019</td></tr>
<tr><td colspan="6">본 발명의 일 실시예는 IoT(Internet of Things) 센서와 운영 서버 간 통신에 있어서 보안을 강화한 사물인터넷 기반의 DUSS(Different Units Same Security) 장치를 제공하고자 한다. 본 발명의 일 실시예는 센서 데이터의 보안 레벨에 따라 미들웨어를 바이패스 하도록 암호화를 수행하여 센서 데이터의 중요도에 따라 통신 보안을 강화시킬 수 있는 사물인터넷 기반의 DUSS 장치를 제공하고자 한다.</td></tr>
</table>

<table>
<tr><th rowspan="2">연번</th><th>참여
교수
명</th><th>연구자
등록번호</th><th>전공
분야</th><th>실적
구분</th><th>특허, 기술이전, 창업 상세내용</th><th>증빙</th></tr>
<tr><td>세부
전공
분야</td></tr>
<tr><td></td><td colspan="6">특허, 기술이전, 창업 실적의 우수성</td></tr>
<tr><td rowspan="6">10</td><td rowspan="5">한동국</td><td rowspan="5">10128486</td><td rowspan="3">수학</td><td rowspan="5">특허</td><td>박찬일, 이옥연, 안현진, 원유승, 심보연, 김호연, 이예림</td><td></td></tr>
<tr><td>중간값 평균기법을 이용한 부 채널 분석 성능 향상방법</td><td></td></tr>
<tr><td>대한민국</td><td>URL입력</td></tr>
<tr><td rowspan="2">암호론</td><td>10-1589185</td><td rowspan="2">https://patents.google.com/patent/KR101589185B1/ko</td></tr>
<tr><td>2017</td></tr>
<tr><td colspan="6">본 발명은 중간값 평균기법을 이용한 부 채널 분석 성능 향상방법에 관한 것이다. 본 발명에 따른 중간값 평균기법을 이용한 부 채널 분석 성능 향상방법은 암호 알고리즘 입력정보가 랜덤 평문인지 여부를 판단하는 단계(S100); 암호 알고리즘에 따른 중간값을 구성하는 단계(S200); 중간값에 따른 소비 전력 집합을 분류하는 단계 (S300); 및 집합 별 소비 전력 평균 기법을 적용하는 단계(S400);를 포함한다. 본 발명에 따르면, 본 발명에 따르면, 종래의 상관 전력 분석이 평균 기법에 의해 분석이 불가능한 문제를 해결하고, 중간값으로 분류한 파형에 대한 평균을 취함으로써 향상된 부 채널 분석 결과를 얻을 수 있다.</td></tr>
</table>

1.2 연구업적물
③ 연구의 수월성을 대표하는 연구업적물 (최근 10년)

<표 3-4> 최근 10년간 참여교수의 해당 산업·사회 문제 해결분야 대표연구업적물

〈표 3-4〉 최근 10년간 참여교수의 해당 산업·사회 문제 해결분야 대표연구업적

연번	대표업적물 설명
1	▶ 산업·사회 문제 해결을 위한 미국 특허 등록 - 최은미 교수와 그 연구팀은 2017. 3. 21 일자로 미국 특허 US 9,600,541 B2를 등록하였으며, 이는 “Method of Processing and Analysing Vehicle Driving Big Data and System Thereof” 의 발명의 명칭이 된 특허임 - 이 특허는 대한민국특허청 공개특허공보로 출원번호 10-2014-0053389 및 공개번호 10-2015-0126155 로 특허 등록된 “운행기록 빅데이터 처리 및 분석 방법” 발명의 명칭으로 된 특허임 - 본 특허는, 차량으로부터 수집된 로우 데이터(raw data)의 운행기록 데이터를 정제(refine)하는 단계와, 상기 정제된 운행기록 데이터에 근거하여 통계 데이터를 획득하는 단계, 및 상기 정제된 운행기록 데이터 및 상기 획득된 통계 데이터 중 적어도 하나에 근거하여 마이닝 분석을 수행하는 단계를 포함하는, 운행기록 빅데이터 처리 및 분석 방법이 제공됨 - 차량의 운행에 대한 빅데이터를 기반으로 산업·사회 문제 해결을 진행하였으며, 이에 대한 연구 활동과 다양한 빅데이터 처리 분석 연구 결과와 알고리즘으로 해결을 추구하였음 - 정보통신산업진흥원사업 IT/SW 창의연구과정 (기술개발형)에서 디지털 운행기록계 빅데이터 분석 기술 연구를 진행하면서 차량에서 수집된 빅데이터를 기반으로 빅데이터 처리 및 분석을 통하여 그 연구 방법과 결과를 도출함. - 본 연구는 중국 특허도 OA 접수 보고되어 현재 특허 출원 및 심사 절차를 진행하고 있음 - 입력된 센싱 데이터는, 차량의 주행거리, 주행시간, 데이터 획득주기, 데이터 획득일시, 속도, 분당 엔진 회전수, 브레이크 신호, 위치, 방위각 및 가속도 필드에 대한 레코드를 포함하는, 운행기록 빅데이터 처리 및 분석을 진행함 - 연구 활동으로 이용한 통계 데이터는, 운행 통계 데이터와 성향 통계 데이터를 포함하고, 운행 통계 데이터는, 일주행거리, 총 주행 시간, 평균 속도, 최고 속도, 및 최고 분당 엔진 회전수 필드에 대한 레코드를 포함하고, 성향 통계 데이터는, 과속 횟수, 위험과속 횟수, 장기과속 횟수, 급가속 횟수, 급감속 횟수, 급출발 횟수, 급정지 횟수, 앞지르기 횟수, 진로변경 횟수, 급회전 횟수, 공회전 횟수, 및 고 분당 엔진 회전수 횟수 필드에 대한 레코드를 포함하는, 운행기록 빅데이터 처리 및 분석 방법임 - 기술보증기금 서부기술혁신센터를 통하여 2014년에 출원한 유사한 분야의 특허인 “DTG 빅데이터 처리 및 분석시스템“에 (등록번호 10-1601034) 대하여 기술이전에 대한 문의를 국민대학교 산학협력단에 요청하였으며, 기술혁신센터의 기술보증에 따라서 ㈜나오소프트에서 기술이전을 하였음

2	▶ 산업·사회 문제 해결을 위한 유럽 특허 등록: Contact-type Apparatus and Method for Inspecting Side Channels of Smartcard - 한동국 교수는 부채널 분석의 국내 전문가로 활동하며, 물리적 보안을 요구하는 다양한 보안 기기에 대해 안전성 검증 역량 발전에 기여함 - 2019년 3월 ‘Contact-type Apparatus and Method for Inspecting Side Channels of Smartcard’ 라는 발명 명칭으로 유럽 특허를 등록함 - 본 발명은 스마트카드의 접촉식 부채널 검사 장치에 연산 증폭기를 사용하여 접촉식 부채널 검사의 분석 성능을 향상시킬 수 있는 방법을 제시함 - 스마트카드는 금융IC카드, 모바일폰, 전자 여권 등 다양한 분야에서 범용적으로 사용되는 보안 기기임 - 개인정보를 다룬다는 점과 실생활에 널리 사용된다는 점으로 스마트카드는 물리적인 공격에 대해 내성을 가져야 함 - 부채널 분석은 스마트카드 내에서 암호 알고리즘이 동작 중일 때 발생하는 소비 전력, 수행 시간, 전자파 방출 등을 관측 데이터로 사용함 - 기존의 부채널 정보 수집 장비들은 전압강하용 저항을 사용하였는데, 본 저항값을 증가시키면 스마트카드가 오작동을 유발할 위험이 있고 감소시키면 측정된 부채널 정보에 부가되는 외부 노이즈가 많다는 문제점이 존재함 - 본 발명은 연산 증폭기를 사용하여 스마트카드의 전압 변화 스펙트럼을 확장시켜 전력 분석 성능을 향상시킬 뿐만 아니라 스마트카드에 인가되는 공급 전압을 정전압으로 유지하여 오동작을 유발하지 않게 함 - 또한, 수집된 부채널 정보에서 노이즈가 감소함에 따라 분석 범위의 집약적인 선택이 가능하여 분석 시간이 감소함 - 따라서 본 유럽 특허를 통해 더욱 정밀하게 부채널 정보의 수집이 가능하고 물리적 보안을 요구하는 보안 기기에 대한 강력한 안전성 검증이 가능함 - 부채널 분석 관련하여 유럽 특허를 등록함에 따라 유럽 위주의 부채널 분석 기술 선도에서 경쟁할 수 있는 유리한 교두보를 확보함 - 날로 늘어나는 IoT 기기 등의 물리적 보안을 요구하는 보안 기기들에 대한 안전성 검증 기술을 선도할 수 있을 것으로 기대됨

3	▶ 국제표준화 위원에서 ISO/IEC 국제표준화 활동을 통한 산업연계 표준 발간 - 박수현 교수는 ISO/IEC JTC 1/SC 41 (사물인터넷 및 관련기술)에서 한국전문가로 활동하며, PL(Project Leader)을 맡아 ISO/IEC 30140-3 (Information technology-Underwater acoustic sensor network (UWASN)-Part 3: Entities and interfaces)을 IS(International Standard)로 발간하므로 수중-IoT 발전에 기여함 - 2018년 7월 발간된 ISO/IEC 30140-3 (Information technology-Underwater acoustic sensor network (UWASN)-Part 3: Entities and interfaces)은 세계 최초로 수중음파통신 분야에서 제정된 국제표준인 ISO/IEC 30140 시리즈의 일부로서 수중 음파 센서 네트워크(UWASN)간의 상호운용성을 지원하는 일반 요구사항, 참조 아키텍처 및 고급 인터페이스 지침을 제공함 - UWASN의 물리적 엔티티(entity)를 네트워크, 어플리케이션 도메인으로 나누어 제시하고 있으며, 각 계층의 기능적 엔티티를 구분하고 그 역할을 정의함 - UWASN 인프라를 구축할 때 고려해야 하는 공통 인터페이스를 물리적 엔티티 및 기능적 엔티티로 분류하여 기술함 - 바다는 무한한 가능성을 지닌 미개척지로 EU, 중국, 미국, 일본 등 주요국은 이미 해양수산업을 미래 성장동력으로서 전략적으로 육성하고 있음 - 우리나라는 삼면이 바다로 둘러싸여 있어 풍부한 자원을 보유하고 있음에도 불구하고 국내 해양산업의 경우 침체가 장기화되고 핵심기술 부족으로 인하여 부가가치 창출에 어려움을 겪고 있는 실정 - 따라서 본 국제표준의 발간을 통해 해양환경 보호, 수중·항만 보안 등의 여러 목적을 위한 다양한 기기와 통신할 수 있는 하나의 계기가 수중에도 마련되었음 - 그뿐만 아니라 4차 해양산업혁명의 산업·사회적 문제를 수중-IoT 기술 발달로 해결 가능할 것으로 여겨지며, 수중통신 글로벌 시장에서 경쟁할 수 있는 유리한 교두보를 확보함 - 또한, 6G 이동통신으로의 기술 발달 및 IoT 시대가 본격적으로 열리며 가속화되고 있는 초연결사회의 데이터 확장 및 정보보안 이슈 해결을 위한 기초연구 역할을 함 - 6G 기술의 발전은 대표적인 통신 음영 영역으로 여겨지던 수중에서도 통신을 가능하게 하므로 환경적 제약으로 인한 음파를 사용한 제한적인 통신의 한계도 뛰어넘을 것으로 예상됨 - 본 국제표준에서 다루고 있는 음파 기반 네트워크를 확장 적응하여 연구 및 개발시 6G가 접목된 Underwater IoT 구축 및 실현 가능성이 증가될 것으로 예측됨

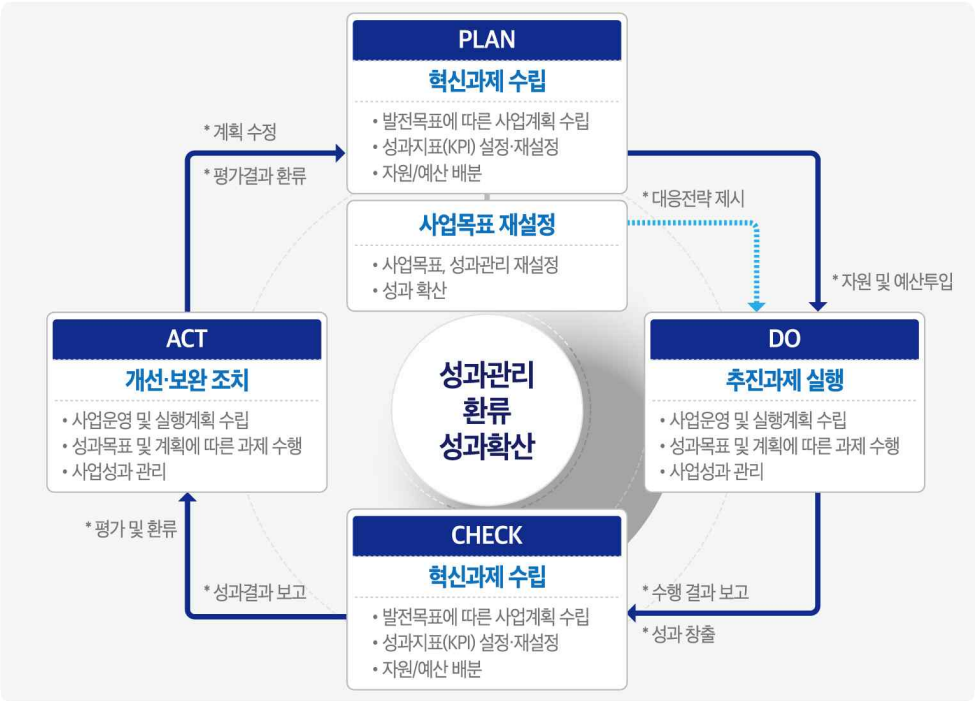
1. 참여교수 연구역량

1.3 교육연구단의 연구역량 향상 계획

▣ 산업사회문제 해결에 초점을 맞춘 연구 성과관리 체계 조성

▶미래 지향적 지원체계 운영

- 대학의 혁신 비전 및 중장기 발전계획 <KMU Vision 2030+>을 수립하고 우리 대학의 교육철학인 공동체 정신과 실용주의를 바탕으로 비전을 실현하고 4차 산업혁명 시대가 요구하는 '창의적 융합인재'를 양성하기 위하여 "세상을 바꾸는 TEAM형 인재 양성 기반구축 및 확산"을 발전목표를 세우고 교육·연 구·산학협력의 3대 영역별 혁신전략을 구체적으로 수립함
- 교원의 창업 및 창업지원 활동 강화를 위해 대학의 기술과 인프라를 기반으로 지속 가능한 기업으로의 교원 창업이 이루어질 수 있도록 창업 겸직 규정과 프로세스를 혁신하고, 기술지주회사 및 사업화 지원프로그램을 통하여 신임교원의 창업을 격려함



연구성과 관리 및 연구성과 확산을 위한 환류체계

▶사회문제 공유 및 해결방안 마련을 위한 정기 워크숍 및 세미나 시행

- 사회에서 발생하는 문제에 대한 공유 및 해결방안 마련을 위해 정기적으로 워크숍을 개최하여 기업, 연구소, 학계 연구자들과 교류함
- 대학원생이 이론적 기반을 공고히 하여 IT 응용서비스 정보보안 관련 연구자로서 창의적인 인재가 될 수 있도록 최신 연구 결과를 파악할 수 있는 정기 공개 세미나를 시행함
- 최신 연구 동향 및 각종 이슈에 대해 습득할 수 있도록 국내외 유명 논문 저자 또는 연구소 및 기업체의 전문가 특강을 시행함
- 피인용수가 높은 논문의 저자 또는 정보보안 분야의 경력이 5년 이상인 정보보안 분야에서 지속적으로 연구활동을 진행하고 있는 전문가를 초빙함

▶창의적 연구 환경 조성

- 교육연구단 소속연구원 전용공간 구축 및 연구 장비 지원을 통해 연구원 간 원활한 의사

소통 및 장비의 효율적 활용이 이루어질 수 있도록 유도함
- 국내·외 전문가 초청 강연 세미나 및 심포지엄 개최하여 전공 분야 최신 연구주제 집중 특강 및 교수/국내외전문가/대학원생 간 3자 간담회 등을 통해 연구 활동과 학문에 대한 다양한 경험과 열정을 공유함으로써 대학원생에게 미래가 요구하는 과학 인재로 성장할 기회를 제공함
- GitHub를 통하여 개발한 정보보안 기술 및 자율 성장 인공지능 모델을 공개하여 관련 연구 분야의 활성화 및 사회적 문제 해결에 기여하고, 다양한 연구자들과의 교류를 활성화 할 수 있도록 지원함

▶국제 표준화 활동 지원
- 초연결시대가 현실화되면서 신기술 또는 새로운 산업에 대한 국제표준을 선점하기 위한 각국의 준비가 시작된 만큼, 사물인터넷 국제표준화를 수행하는 ISO/IEC JTC 1/SC 41(사물인터넷 및 관련 기술) 회의에 정기적으로 참여할 수 있도록 재정적으로 지원함
- 안전한 초연결사회를 위한 문제해결형 정보보안 관련 선진 연구 개발 동향을 파악 및 현장에서 실무 경험을 체득할 수 있는 기회를 제공함

▣ 연구 업적물의 질적 우수성 향상 방안

▶수월성에 중점을 둔 학위취득 평가 방법 도입
- 연구 업적물의 질적 향상을 위해 해당 연구 분야 상위 20% 이내 학술저널 논문 또는 학술대회 논문 1편 이상 또는 상위 40% 2편 이상을 학위 취득요건으로 함
- 논문 출판 실적 외에 논문 심사 위원회에서 학위대상자의 창의성, 문제해결 능력 및 전공 분야 전문가 자질 등을 종합적으로 판단하여 졸업 자격을 결정함.

▶교비대응자금 20%를 활용하여 우수 연구 업적에 대한 성과보수 부여
- 학술 활동 결과물의 질적 향상 동기부여를 위해 학술저널에 출판된 논문 저자에 대한 성과보수를 지급함. 학술저널의 IF(피인용지수)를 기준으로 연구 결과의 우수성을 판단하여 성과보수 차등 지급할 계획임
- 대학원생을 대상으로 IF 2.0 이상 학술저널 출판 논문에 대해서는 편당 최대 100만 원을, IF 2.0 미만 학술저널 출판 논문에 대해서는 편당 최대 50만 원을 기준으로 논문 저자 수에 따라 지급함
- 학술논문 출판 외에도 USENIX, S&P, ACM CCS, CHES, CRYPTO, ASIACRYPT, EUROCRYPT, FSE 등 정보보안 분야 유명 국제 학술대회 발표 논문을 우수한 실적으로 판단하고 해당 결과에 대한 성과보수를 지급할 계획임
- 유명 국제 학술대회에 발표한 논문에 대해서는 대학원생을 대상으로 편당 최대 50만원을 기준으로 논문 저자 수에 따라 나눠 지급함
- 상기 해당하는 학술저널 또는 학술대회에 논문이 선정되지 않은 대학원생에게도 출판 또는 발표 논문 수가 기준 초과 시 꾸준한 학술 활동 동기를 부여하기 위해 성과보수를 지급할 계획임
- 해당 기준은 석사과정 또는 박사과정(석박사통합과정 포함)에 따라 기준을 달리 적용함
- 석사과정 대학원생은 학술대회 5편 또는 학술저널 2편 이상 작성한 경우 10만 원의 성과보수를 제공하며, 박사과정 대학원생은 (석박사통합과정 대학원생 포함) 학술대회 10편 또

는 학술저널 5편 이상 작성 시 10만 원의 성과보수를 제공함
- 최우수 학술저널 또는 학술대회에 논문을 100% 게재한 대학원생에게 수업연한을 한 학기 단축할 수 있는 혜택을 제공함
- 학술 활동을 목적으로 한 출장(학술대회, 경진대회 등)에서 우수한 성적을 얻을 수 있도록 차기 해외 연수 또는 해외 저명 학회 참가를 지원하여 격려할 계획임
- 연구개발능률성과급 지급 지침 신설하고(2018.03.01.) 교원의 연구 활동 독려 및 우수연구 성과 창출을 위하여 성과급 지급에 대한 지침을 신설하고 매년 산학협력단 간접비에서 차등 지급함

▣ 산학 공동 연구 및 연수를 통한 연구 역량 향상 방안

▶프랑스 하드웨어 보안기업 Texplained 연수 추진

- 연 1회 2달간의 프랑스 하드웨어 보안기업 Texplained에 직접 연수를 수행하여 디바이스 역공학과 관련하여 실제 디바이스 개발 과정에 참여하는 경험을 제공하고, 성과보수 해당자에 대해 먼저 우선순위를 부여함

▶싱가포르 난양 기술 대학교와의 공동 연구 진행

- 싱가포르 난양 기술 대학교(Nanyang Technology University)의 우수 보안 연구팀인 Physical Analysis & Cryptography Engineering (PACE) 팀과 공동 연구를 진행함
- 원활한 국제 공동 연구가 진행될 수 있도록 교류를 위해 발생하는 항공 운임 및 체류비용을 본교 국외 출장 기준으로 지원함. 성과보수 해당자에 대해 먼저 우선순위를 부여함

▶체코 Brno University of Technology와의 정기 교류 워크숍 진행

- 체코 Brno University of Technology와의 지속적인 인적 교류 및 워크숍을 통해 자율성장 인공지능 기술을 활용한 체코의 사회문제 해결에 적용할 수 있도록 인적 교류를 진행함

▶미국 MIT와의 정기적 연구 교류

- MIT 기계공학과 김상국 교수 연구팀과의 인적 교류를 자율성장 인공지능 모델에 대한 디자인 구성 및 활용 방안에 대한 자문으로 활용함

▶국제 공동 연구 프로그램 개발

- 국민대학교와 상호 교류 체결이 논의된 바 있는 Katholieke University of Leuven (벨기에), Indraprastha Institute of Information Technology (인도), MASSEY University (뉴질랜드) 등의 학교와도 상호 교류를 위한 프로그램을 개발할 예정임
- 이러한 프로그램을 통해 교육연구단 소속 대학원생이 방학 기간을 활용하여 해외 대학의 Summer School과 같은 교육프로그램에 참여할 수 있도록 함
- 외국 대학과의 교류를 통해서 각자의 주 분야에 대한 고속 구현 기술을 공유하고 공통된 조건에서의 서로 간의 차이점을 분석하거나 다른 환경에서의 고려 사항들을 비교하는 등 각종 환경에서의 장단점을 분석함으로써 확장된 개발 방식을 습득할 수 있음
- 따라서 국제 공동 연구에 참여하는 국내/국외 학자들에 대한 정기적인 세미나 및 실시간 피드백을 활용하여 활발한 의견 교류와 정보 공유를 가능하게 하고 이에 따른 시너지를 기대할 수 있음

▣ 연구몰입 환경 구축 및 연구 지원제도 운용

▶연구 지원제도 개편

- 연구자의 연구몰입 환경 조성을 위한 인프라 및 제도를 아래와 같이 마련하여 시행함
- 연구실 및 부설 연구소 행정인력 운영방안 마련하여(2017.09.01.) 국가연구개발사업 수행 연구책임자의 행정업무 부담을 최소화하기 위하여 행정인력 지원함
- 산학협력단 외부연구비 관리 설명서 제작하여(2018.05.14.) 내・외부 각종 규정 및 서식을 한 권으로 통합하여 연구자에게 연구비 신청의 편의성을 제공함
- 산학협력단 차세대 연구행정시스템 신규 개발 계획을 수립하고(2019.04.) 대학 차세대 시스템 개발과 연계하여 데이터 간・업무 간・시스템 간 정보의 연결성 강화 및 연구자가 연구에만 전념할 수 있는 친 연구시스템 운영함
- 연구역량 강화 및 활성화를 위한 연구지원제도 개선 및 신규 제도 시행을 위해 아래와 같은 지원제도를 마련하여 운영함
- 학술대회 참가 지원에 관한 내규 개정하여(2017.03.01.) 지침으로 시행되던 참가 지원사항을 내규로 규정하고, 참가지역에 따라 지원금을 50만 원까지 차등 지급함
- 논문게재료 지원에 관한 내규 개정하여(2017.03.01.) 논문게재료의 효율적 지급을 통한 연구역량 강화 및 예산집행의 효율성을 높이고자 지원대상 학술지를 국내는 한국연구재단 등재(후보)지 이상, 국외는 SCOPUS 이상으로 명확히 규정하고, 지원금을 국내 70만 원, 국외 100만 원 이내로 세분화하여 운영함
- 시제품 제작 지원사업으로 대학 우수 기술의 상용화 지원을 위한 시제품 제작 지원프로그램과 우수특허 창출을 위한 특허 설계 지원프로그램 운영하여 대학 우수 기술 확보를 위한 시장 및 동향조사 지원과 유효 기술의 특허 권리화를 지원함
- 사업 참여 대학원생의 연구성과가 제고될 수 있도록 참여 대학원생에 대한 본교 기숙사(생활관) 입주 우선 배정을 요청함
- 대학원 주요 장학제도인 ‘교수추천 우수 신입생 장학금’(수업료의 50% 감면), ‘교육조교 장학금’(수업료의 50% 감면), ‘연구조교 및 산학협력 조교 장학금’ (수업료의 70% 또는 100% 감면), ‘이공계 전일제 박사과정 장학금’(수업료 100% 감면) 등을 배정할 시, BK21 FOUR 교육연구단장이 학과장을 역임하므로, BK21 FOUR 사업 참여 대학원생을 먼저 배정함
- 본 사업개시 학기부터 ‘BK21 FOUR 장학금’을 신설하여 본 사업에 참여하는 전일제 재학생을 대상으로 ‘정부 장학금’을 받지 못하는 대학원생에 대해 우리 대학 대응자금을 재원으로 하여 별도로 장학금을 지원할 예정이며, 본 장학금에 대한 대상자 선발 권한은 전적으로 교육연구단장에게 부여함
- 해외 우수 대학원생 유치를 위한 ‘해외 우수연구인력 유치 지원사업’ 운영을 위하여 석사과정 1년, 박사과정 2년, 석・박사통합과 정 3년간 등록금 전액과 기숙사비의 50%, 매월 60만 원의 생활비를 지원하는 제도를 바탕으로, 본 교육연구단에 우수한 해외 대학원생 유치 노력을 지속할 예정임

▶교원 업적평가 제도 개편

- 산학협력 실적 반영을 통한 대학 전 교원으로의 확산: 승진·승급·재임용 시 산학협력 관련 점수만으로 승진 등이 가능하도록 산학협력 실적을 100% 대체 인정하고, 특별승진 기준 산학협력점수(연구, 교육, 봉사) 전 분야에서 가능하도록 확대함

- 오픈소스 SW 활동을 SCI급 논문실적으로 대체하도록 국제필수 신규 지정함(2016.10.01.)
- 교원업적평가 시 SCI급 논문 1편(100점) 대비 산학협력 실적은 전 계열에 적용되고, 평가 항목별 배점을 모두 동일하게 인정 가능하며, 특히 기술 이전(1천만 원)의 경우 SCI급 대비 비율을 73% 수준까지 지속해서 확대함

▶창업 지원제도 운영

- 교육연구단은 국내 주요 액설러레이터 (CCVC 밸류업센터, 아산나눔재단 정주영 창업센터 등과 기협의)와 협력하여 자질이 우수한 학생이나 팀에게 학내 보육 수준을 넘어선 창업 멘토링 제공과 세계 시장 진출 지향형 보육 환경을 지원함
- 성과나 실적이 우수한 참여 교수와 대학 동문들이 (가칭) 국민엔젤펀드를 결성하여 자금 지원을 실행함으로써, 현재 모태펀드(한국벤처투자)나 아산나눔재단 등이 운영하는 엔젤 매칭펀드 등과 연계하여 학생들의 연구와 학업을 지원함

▣ 우수 대학원생 확보 방안

▶우수 학부생에게 대학원 진학 장려

- ‘학부 연구생’ 제도 시행을 통해, 학부생들이 BK 교육연구단의 연구 프로젝트에 참여하여 정보보안 분야의 관심을 유도하고, 책임감과 전문성을 갖춘 학생으로 육성함
- 학부생을 대상으로 대학원 연구실별 성과 및 연구내용을 소개하고 진학 관련 고민 및 궁금증에 대해 해소할 수 있도록 수시 상담을 진행함
- 우수한 신입생을 적극적으로 유치하기 위해 성곡 장학금 (수업료 전액), 교수추천 우수 신입생 장학금 (수업료의 50% 지원), 교육 조교 장학금 (수업료의 50%), 연구조교 장학금 (연구조교 A: 수업료의 100%, 연구조교 B: 수업료의 70%) 등 다양한 장학금 지원을 늘려, 인재 확보와 연구 기회와 질 높은 교육환경을 제공함

▶연구공간 지원

- 교육연구단의 원활한 연구수행을 위하여 산학협력관에 교육연구단장 또는 사업 참여 교수의 요청에 따라 연구공간을 마련하여 지원함

2. 산업·사회에 대한 기여도

2.1 산업·사회문제 해결 기여 실적

▣ 강주성 교수

▶난수발생기에 대한 안전성 분석 연구 진행

- 염용진 교수와 공동으로 가장 널리 사용되는 Linux 의사 난수발생기의 엔트로피 추정 방법을 최초로 이론적으로 증명함
- 이 결과를 이용하면 암호 시스템과 암호모듈에서 사용되는 Linux 의사 난수발생기 엔트로피 추정 시 발생할 수 있는 안전성 문제를 완화할 수 있으며, 이 연구 결과는 SCI급 국제 논문지에 게재됨

▶경량 환경에서 엔트로피 소스를 효율적으로 관리하는 BCH 코드 기반 후처리 기법 개발

- 이 기법으로 경량 환경에서 사용되는 난수발생기의 안전성 문제를 완화할 수 있으며, 이 연구 결과는 SCIE급 국제 논문지에 게재됨

▶난수발생기 구조, 엔트로피 평가 방법 등에 관한 국내 특허 6건 등록과 1건의 기술이전

- 이 평가 방법은 정보보안제품 보안성평가의 정확성과 효율성 향상에 기여함

▶KIST 양자정보연구단과 양자난수발생기 공동연구 진행하여 국내 특허 2건 등록

- 이 연구결과는 양자 통신을 기반으로 하는 암호키 생성 효율성 향상과 사용자 인증의 안전성 강화에 기여함

▶화이트박스 암호 연구를 진행하여 국내 특허 2건 등록과 기술이전 2건

- 염용진 교수와 공동으로 개발한 화이트박스 암호 기술은 금융 등의 산업에서 화이트박스 암호 기술 적용 제품의 안전성을 강화하는 데 기여함

-

▣ 김동찬 교수

▶ISO/IEC SC27 WG2 한국대표 전문가로 활동하며, ISO/IEC 29192-2:2019 프로젝트를 주도

- 국제 표준 기구 ISO/IEC의 SC27(Information security, cybersecurity and privacy protection)은 정보보안 관련 표준 분야로, 5개의 WG(Working Group) 중 WG2는 암호 알고리즘 표준 그룹이며, 세계 각국의 암호 전문가들이 매년 2회의 정기 회의를 통해 우수 암호 알고리즘의 표준화를 추진함
- SC27 WG2 국내전문위원인 김동찬 교수는 2016년부터 WG2의 한국대표 전문가로 활동 중이며, 최근 주저자로 국내 경량 블록암호 LEA의 국제표준화(29192-2:2019)를 주도함

▶국가보안기술연구소와 공동연구를 진행하여 사용자 인증 및 키공유 알고리즘에 사용하는 타원곡선 암호 완전덧셈식 도출

- 타원곡선 암호는 현재 사용자 인증 및 키공유에서 가장 많이 사용하는 암호임
- 국가보안기술연구소와 공동연구를 진행하여 DH 키공유에 사용하는 몽고메리 타원곡선의 완전덧셈식을 도출함. 이는 국제암호학회 ICISC 2019에서 발표됨

▶화이트박스 암호 기술이전 2건

- 화이트박스 암호는 고도화되고 있는 소프트웨어 분석기법에도 안전하도록 설계한 암호 보호 장치임
- 염용진 교수와 공동으로 개발한 화이트박스 암호 기술은 금융 등의 산업에서 화이트박스 암호 기술 적용 제품의 안전성을 강화하는 데 기여함

▣ 김종성 교수

▶주요 랜섬웨어 정밀 분석

- 2017년부터 랜섬웨어 연구를 시작하여 MyRansom, Donut, LooCipher에 대한 복호화 방안을 개발함

- 이외에도 WannaCry, CryptoShield, Erebus, CERCER, Revenge, hermes, Rapid, Clop, Phobos, JCry, Maze 등의 랜섬웨어를 분석하여 추가적인 분석이 가능하도록 함
- 메모리분석, 암호 알고리즘 취약점 공격 등 여러 가지 기법을 적용하여 주요 랜섬웨어 복호 방법 개발함. 개발한 도구는 랜섬웨어로 인한 피해를 최소화 하는데 기여함
- 논문 실적: 정보보안학회논문지 2건, 디지털 포렌식연구 1건, 정보보안학회 학술지 1건

▶포렌식 기법을 이용한 주요 애플리케이션 취약점 발견

- 포렌식 수사에서 스마트폰은 디지털 용의자 행동을 분석하고, 디지털 증거를 수집하는데 유용한 기기임
- 스마트폰 탑재 애플리케이션에는 사용자 설정에 따라, 혹은 자동으로 암호화 또는 직렬화 되어 저장하는 데이터가 존재하는데 이는 디지털수사에 귀중한 정보가 됨
- LG 갤러리, 말랑말랑톡카페, Surespot, 카카오톡(iOS), 후스콜, 컬러노트, 소모임 등의 애플리케이션에서 사용하는 암호화 알고리즘과 그 취약점을 밝혀냄
- 최근 삼성, 화웨이, LG, SONY 스마트폰 백업 파일의 암호화 알고리즘과 그 취약점을 밝혀내었고, 백업파일 복호 방법을 제시하여 디지털 포렌식 수사에 기여함
- 논문실적: 국제저널 DI 3건, 정보보안학회논문지 1건, 디지털 포렌식연구 2건, 특허실적: 국내특허 1건 등록

▶시스템로그 분석 도구 개발

- 시스템로그는 일반적으로는 이해하기 힘들고 어떤 행동으로 인해 발생되었는지를 구체적으로 알기가 쉽지 않아 디지털 포렌식 수사 시에 특정 로그가 어떤 행동을 의미하는지 파악할 수 있도록 사전연구가 필요함
- Windows, iOS, 안드로이드 등에서 제공하는 시스템로그를 분석/정규화하여, 디지털 포렌식 관점에서의 활용방안 연구 및 분석도구를 개발하였음
- 논문실적: 정보보안학회논문지 1건, 디지털 포렌식연구 4건, 특허실적: 국내특허 3건 등

▶블록암호 기반 해시함수의 새로운 공격기법 제시

- 2019년 블록암호 기반 해시함수의 연관키 차분성질을 이용한 공격기법을 발표하였고, 이는 IoT환경에 적합한 경량 블록암호 기반 해시함수는 취약할 수 있음을 시사함
- 논문 실적: 국제저널 PPNA 1건, 국제저널 MTAP 1건

▣ 박수현 교수

▶M2M/IoT(사물인터넷) 환경용 지능형 디바이스 플랫폼 설계 방안 기술이전

- 2015년 2월 M2M/IoT(사물인터넷) 환경에서 다양한 통신 인터페이스를 지원하는 지능형 디바이스 플랫폼 제작 기술의 Know-how를 ㈜클린웨어에 500만원에 기술이전 함
- 이를 통해 해당 기업은 스마트 홈 IoT 장치개발이 가능하게 됨

▶국제표준(ISO/IEC) 제안/제정을 통한 수중통신 표준 분야 선도

- 표준화 대상기술 분야에서 리더십을 가지고, 주도적으로 국제규격(ISO/IEC) 및 국내 단체규격을 위한 제안/제정을 수행하여 수중통신 표준 분야를 선도하고 있음
- ISO/IEC JTC 1/SC 41에서 Project Leader로 활동하며 4건의 ISO/IEC 30140 시리즈 국제표준 문서(Information technology-Underwater acoustic sensor network (UWASN)-Part 1: Overview and requirements, Information technology-Underwater acoustic sensor network (UWASN)-Part 2: Reference architecture, Information technology-Underwater Acoustic Sensor Network (UWASN)-Part 3: Entities and interfaces, Information technology-Underwater Acoustic Sensor Network (UWASN)-Part 4: Interoperability)를 발간하고,

ISO/IEC 30142, 30143 표준문서 개발을 진행함

▶ICT표준전략맵 참여를 통한 국제 표준화 전략 제시

- ICT 표준전략맵의 수중통신 전문가로서 참여하여 국제 표준화 대응 전략을 제시함
- 수중과 같은 특수 도메인을 포괄하는 IoT 표준그룹으로서의 확장성을 위한 네트워크를 수립함

▣ 서석충 교수

▶다양한 환경에서의 보안 취약점 분석 및 대응방안 제시

- 보안 정보의 안전을 보장하는 것이 정보보안 분야에서의 산업·사회문제 해결 방향성이라고 할 수 있으며, 수많은 연구를 통해 다양한 환경에서 취약점을 분석하고 그에 따른 대응방안을 연구함
- 정보누수 분석을 통한 비침투분석 안전성 조기 검증 방법을 연구한 사례의 세부 내용은 테스트벡터 기반의 부채널 안전성 조기 검증 기술을 연구한 것임
- 컴파일 설정에 따른 부채널 취약점을 분석하고 그에 따른 대응방안 구현기술을 연구한 실적이 존재함

▶양자 컴퓨팅 환경을 위한 암호키 설정 방법의 최적화 구현 기술 제시

- 현재 사용하는 암호는 양자 컴퓨터를 사용해서 공격할 수 있기 때문에, 이 공격을 무력화하는 포스트 양자 암호키 설정 방법의 최적화 구현 기술에 대한 연구를 진행 중임
- 본 연구는 국가보안기술연구소 등과 활발하게 교류하며 관련 연구를 수행중이며, 상기 제시한 연구 이외에도 다양한 보안적 이슈에 대한 대응 기술 개발 혹은 대응 기술 최적화 연구에 대한 결과를 논문화하여 각종 학술지에 게재함

▣ 윤상민 교수

▶디자인 및 영상 유사도 검색 및 표절 시스템 개발 및 특허 등록

- 디자인의 저작권 보호 및 침해와 관련하여 기준이 모호하여 사회적 문제가 발생하는 가운데, 인공지능 기반 디자인 패턴의 유사성 검증 및 정량적 평가 기준을 마련할 수 있는 디자인 및 영상 유사도 검색 및 표절 시스템 개발을 통하여 해외학술지 발표 및 특허 등록을 수행하였음

▣ 염용진 교수

▶난수발생기에 대한 안전성 분석 연구 진행

- 강주성 교수와 공동으로 가장 널리 사용되는 Linux 의사 난수발생기의 엔트로피 추정 방법을 최초로 이론적으로 증명함
- 이를 결과를 이용하면 암호 시스템과 암호모듈에서 사용되는 Linux 의사 난수발생기 엔트로피 추정 시 발생할 수 있는 안전성 문제를 완화할 수 있음
- 이 연구 결과는 SCI급 국제 논문지에 게재됨

▶경량 환경에서 엔트로피 소스를 효율적으로 관리하는 BCH 코드 기반 후처리 기법 개발

- 이 기법으로 경량 환경에서 사용되는 난수발생기의 안전성 문제를 완화할 수 있음
- 이 연구 결과는 SCIE급 국제 논문지에 게재됨

▶난수발생기 구조, 엔트로피 평가 방법 관련 국내 특허 6건 등록, 1건의 기술이전, TTA 표준문서 제정 및 개정

- 이 평가 방법은 정보보안제품 보안성평가의 정확성과 효율성 향상에 기여함
- 또한 이 연구 결과를 기반으로 하여 2건의 TTA 표준문서를 제정 및 개정하였고, 이는 국내 암호모듈 개발업체와 시험기관에서 난수발생기의 안전성을 분석 및 평가하는 방법으로

활용함

▶KIST 양자정보연구단과 양자난수발생기 공동연구 진행하여 국내 특허 2건 등록

- 이 연구결과는 양자 통신을 기반으로 하는 암호키 생성 효율성 향상과 사용자 인증의 안전성 강화에 기여함

▶화이트박스 암호 관련 국내 특허 4건 등록 및 기술이전 2건

- 최근 수요가 늘어나는 화이트박스 암호에 관한 연구를 통해 국내 특허 4건 등록 및 기술이전 2건 진행함
- 이는 금융 등의 산업에서 화이트박스 암호 기술이 적용된 제품의 안전성을 강화하는 데 기여함
- 김동찬 교수, 삼성전자와 공동연구를 진행하여 Xu et al.이 제안한 화이트박스 암호 분석에 성공하여 SCI급 논문에 게재됨

▣ 이옥연 교수

▶소프트웨어 암호모듈 KMULiB 개발 및 보급

- 개발한 소프트웨어 암호모듈 KMULiB는 2016년 국가정보원에서 검증받아 다양한 IoT 장비에 적용하여 군의 CCTV, 정수장의 센싱 데이터 등 다양한 행정기관의 정보통신망에 보안조치에 이바지함

▶KMULiB 탑재 가상사설망 제품 DUSSYL, DUSSVPN 총 2종 개발

- 2017년 KMULiB을 탑재한 가상사설망 제품 DUSSYL과 최초 개발하였고, 2018년 DUSSVPN을 개발하여 정보보안제품 평가인증 수행규정에 근거한 평가기관이 공통평가기준(CC)버전 3.1 R2와 공통평가방법론(CEM) 버전 3.1 R2를 적용하여 평가받음
- 이를 통해 철도청, 경찰청 등 다양한 기관에 VPN을 적용하여 각 통신간 End to End 보안을 제공하고 있음

▶교통신호제어기 표준 내 통신보안규격 설계

- 2018년 경찰정에서 발행한 교통신호제어기 표준의 통신보안규격을 설계함
- 이 통신보안규격을 제정함으로 인해 교통안전 핵심시절인 교통신호 제어기 및 중앙관제시스템을 해킹 등 외부 침입으로부터 방어할 수 있으며 도로환경에서 국민의 생명과 재산을 보호할 수 있음
- 이것의 의미는 무분별한 보안 장비의 사용으로 인해 호환성이 무력화되어 시설관리 체계가 와해됨으로써 야기되는 각종 사회적 비용을 감소시키는 데 기여함

▶군 드론 안전성 검증

- 최근 드론이 군의 핵심기술로 인식되고 있으나 드론 비행 제어 기술이 대부분 오픈 소스에 기반을 두고 있어 안전성에 대한 검증이 요구되고 있음
- 따라서 다양한 하드웨어, 펌웨어를 기반으로 한 IoT 장비에서의 보안을 적용한 연구 결과를 바탕으로 2019년부터 군이 개발 및 제작한 암호를 탑재한 드론의 데이터 기밀성, 무결성, 사용자 인증 등 안전성을 검증하는 것에 기여하고 있음

▶한국전력공사 전력연구원과 공동으로 스마트그리드용 검증필암호모듈 개발

- 한국전력공사 전력연구원과 공동으로 2016년 3월과 2017년 11월에 스마트그리드용 검증필암호모듈(CM-112-2021.03, CM-132-2022.11) 개발에 성공하여, 2016년 2,500억 규모의 200만 가구 및 2017년 3,000억원 규모의 300만 가구용 지능형전략망의 AMI 보급사업이 재개될 수 있어, 관련 국내 정보보안 산업 및 전력산업 발전에 기여함

▶IoT, 스마트미터 등 6G에 포함될 수 있는 다양한 환경에서 보안 서비스 개발

- IoT, 스마트미터 등 6G에 포함될 수 있는 다양한 환경에서 보안 서비스 개발을 위한 다수의 암호 및 보안 라이브러리 기술 및 개발, KCMVP 검증 실적, 상용화에 기여함
- 주요 개발 및 상용화 실적은 다음과 같음
  - 공공시설용 이동 영상감시의 무선 데이터 기밀성 보장 WiFi 장비 개발 및 상용화
  - 문화재 시설 감시를 위한 Wi-Fi 무선통신 영상감시의 장비 개발 및 상용화
  - 시내버스 탑재 카메라를 통한 주정차위반 단속영상용 LTE 장비 개발 및 상용화
  - 지자체 CCTV용 방범 영상정보 Wi-Fi 무선 전송장비 개발 및 상용화
  - 기상청 관측소 감시영상 및 기상센서 정보 무선용 LTE 보안장비 개발 및 상용화

▣ 최은미 교수

▶산학 중심 연구 주도

- 위담바이오와 테크나인의 최근 창업한 회사와의 긴밀한 연구 협력을 진행하면서, 학생들에게 창업에 대한 경험과 기술이전 추구를 도모하는 연구할 수 있도록 진행하고 있음.
- 위담바이오 회사와는 룰 기반한 Expert System과 온톨로지 관련된 시스템, 전문가 도메인의 정보를 시스템적인 구조와 IT 기술로 응용화하는 연구를 진행하고 있음
- 테크나인 회사와는 IoT 환경에서 수집하는 빅데이터에 대한 연구를 진행하고 있으며, 블록체인의 기술을 응용 서비스화 하는 연구 활동을 진행하고 있음

▣ 한동국 교수

▶Mifare 카드 복제 가능 취약점 제기

- 2016년 공공기관 및 호텔 등에서 출입 통제를 위해 Mifare 카드가 수 분 내에 복제 가능하다는 취약점을 제기함
- 이는 보안이 취약한 카드를 기반으로 한 출입 통제 시스템에 대한 취약점이 존재함을 시사함

▶블록 암호 알고리즘 SEED용 효율적 부채널 분석 기법 제시

- 2018년 국내 금융 IC 카드에 사용되는 블록 암호 알고리즘 SEED에 대한 보다 효율적인 부채널 분석 방법을 제시. 이는 기존의 금융 IC 카드 안전성 테스트에서 고려하고 있지 않은 부채널 분석 방법을 제안함으로써 금융 IC 카드에서 발생할 수 있는 개인정보 탈취 문제를 방지하는데 기여함

▶주요 양자내성암호 부채널 공격 취약성 분석

- 2016년부터 최근까지 Ring-LWE 기반 암호 알고리즘, 다변수 기반 서명 알고리즘, 부호기반 암호 알고리즘 등의 양자내성암호 알고리즘에 대한 신규 부채널 분석 방법들을 제안함으로써 양자 컴퓨터의 개발로 대두된 공개키 암호 알고리즘의 취약성에 대한 문제 해결에 기여하고 있음

▶산업통상자원부 주관 국제공동기술개발사업 수행 예정

- 2019년 12월부터 2021년 11월까지 총 3년간 산업통상자원부 주관 국제공동기술개발사업의 ‘딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발’ 연구를 수행하고 있으며, 이를 통해 머신러닝 기술과 부채널 분석 기술을 접목하여 자동화된 이상행위 탐지 도구를 개발하여 국가 산업을 보호할 것으로 기대함

▶백도어 탐지 기술 개발

- 마이크로프로세서별(예, AVR, MSP, ARM) 부채널 정보 특성이 어떻게 차등화 되는지 연구하여 다양한 환경에 유연하게 적용 가능한 이상행위 탐지 도구를 개발. 전 세계적으로 문제가 되고 있는 백도어를 탐지하여 국가 산업 보호에 기여함

2. 산업·사회에 대한 기여도

2.2 산업·사회문제 해결 기여 계획

▣ 참여교수별 산업·사회문제 기여 계획

▣ 강주성 교수

▶암호학적 난수발생기의 안전성과 효율성 분석 기술 연구

- 정보보안시스템에서 난수발생기는 암호 키(key)와 암호파라미터 그리고 암호 프로토콜에서 사용하는 각종 파라미터와 난수 등의 생성 시에 반드시 사용되어야 하는 핵심 요소임
- 안전하지 않은 난수발생기 사용과 잘못된 사용으로 인한 보안시스템과 암호 프로토콜의 취약점 발견 사례가 빈번하게 보고되고 있음
- 암호학적 난수발생기의 안전성은 입력되는 잡음원의 엔트로피에 의존하기 때문에 사용되는 잡음원에 대한 엔트로피를 최대한 정확하게 추정할 수 있는 기술이 필수적임
- 확률론 및 통계학과 기존 엔트로피 평가 방법을 분석한 결과를 기반으로 미지의 분포에 대한 IID 판정법과 기존 평가 방법이 다루지 못한 데이터에 대한 새로운 엔트로피 평가 방법을 연구하고 개발할 예정임
- 개발된 결과는 난수발생기의 취약성으로 발생할 수 있는 산업·사회적 피해를 최소화하는데 기여할 수 있을 것으로 기대함

▶정보보안프로토콜 설계 및 안전성 분석 기술 연구

- 암호 알고리즘을 이용한 개인식별, 메시지 인증, 디지털 서명 등의 보안 기능을 만족시키기 위하여 안전성이 검증된 정보보안프로토콜 기술의 적용이 필수적임
- 산업계에서는 효율성 문제 해결에 중점을 둔 나머지 안전성이 검증되지 않은 정보보안프로토콜을 적용한 제품을 출시하여 보안사고로 이어지는 사례가 빈번히 발생함
- 정보보안프로토콜 설계 시 외부 공격자 뿐만 아니라 내부 공격자와 제3의 신뢰기관(TTP)에 의한 프라이버시 침해 문제까지 고려할 수 있어야 함
- 다양한 공격 관점에 저항을 갖는 정보보안프로토콜 기술을 개발하고 이를 교육함으로써 산업계에서 안전한 정보보안프로토콜 기술의 사용이 정착하는 토대를 마련하고자 함

▣ 김동찬 교수

▶안전한 암호알고리즘 개발 연구 및 표준화 활동

- 암호알고리즘의 산업계 활용 및 국제적 통용을 위해서는 표준화가 필수적이며, 대표적인 국제 표준 기구 ISO/IEC의 SC27(Information security, cybersecurity and privacy protection)은 정보보안 관련 표준 분야로, 5개의 WG(Working Group) 중 WG2는 암호 알고리즘 표준화 그룹이며, 매년 2회의 정기 회의를 통해 우수 암호 알고리즘의 표준화를 진행함
- 본 교수는 SC27 WG2 국내전문위원으로 활동하여 2016년부터 WG2의 한국대표로 참여하고 있으며, 또한, 직접 개발한 경량블록암호 LEA를 2016년 가을 회의에서 국제표준으로 제안, 3년 6개월 간의 표준화 작업을 거쳐 2019년 11월 표준(29192-2:2019)으로 제정됨
- 국제표준으로 제정된 LEA는 기존에 알려진 공격방법들에 내성을 가지며 산업계 defacto 표준인 AES보다 더욱 빠르게 동작하는 것으로 알려져 있어, 산업계 뿐만 아니라 국제적으로도 활용될 가능성이 큼
- 지속적인 경량 암호 개발연구 및 국제표준화 추진을 통하여 해당 암호알고리즘을 사용하는 보안 제품의 안전성을 제고하고 국산 보안제품의 해외 진출의 토대를 마련하고자 함

▶양자내성암호 개발 연구 및 표준화 활동

- 양자컴퓨터의 개발로 기존 공개키 암호시스템의 안전성이 위협받고 있으며 이에 대한 대비로서 미국 표준기관인 NIST에서는 양자내성암호에 대한 공모를 진행 중임
- 향후 양자내성암호에 대한 개발을 진행할 예정이며, 지속적인 국제표준화 활동을 통해 양자내성암호 국제표준 최신 동향 파악 및 개발한 양자내성암호의 국제표준화 작업을 추진할 예정임
- 안전하고 효율적인 양자내성암호 개발 및 표준화 활동을 통하여 양자컴퓨터 개발에 대비한 안전한 암호시스템을 준비하고 국제적인 우위를 달성하고자 함

▣ 김종성 교수

▶신규 랜섬웨어에 대한 복호화 연구 및 기계학습을 통한 분석 방법 연구

- 랜섬웨어는 사용자 데이터를 암호화하여 금품을 요구하는 악성코드의 일종으로서 5SS5C, Crysis/Dharma, Ryuk, Nemty 등의 신규 랜섬웨어가 지속적으로 유포되어 사용자의 데이터 안전성을 위협하고 있는 실정임
- 신규 랜섬웨어에 대한 구현적 취약점 분석과 복호화가 가능성을 연구하고, 기계학습기법을 접목하여 바이러스, 랜섬웨어와 같은 악성코드 탐지를 자동화하고자 함
- 본 연구결과는 랜섬웨어를 포함한 악성코드로 인한 기업 및 사용자의 피해를 최소화 할 수 있을 것으로 기대됨

▶스마트폰 포렌식 기법 연구

- 스마트폰에 설치된 앱 내에는 사용자의 설정에 따라, 혹은 자동으로 암호화되어 저장되는 데이터가 존재하며 이는 디지털수사에 귀중한 정보가 될 수 있음
- ProntonMail, SteganographyX plus, SteganoG, Telegram, BBM-Enterprise, slack, discord 등의 스마트폰 앱에서 사용하는 암호화 알고리즘을 디지털 포렌식 관점에서 효율적으로 분석하는 연구를 수행하고자 하며, 본 연구결과는 스마트폰에 대한 디지털 포렌식에 활용되어 정확한 디지털수사를 가능하도록 할 것으로 기대함

▶딥러닝 기반의 블록암호 분석기법 연구

- 기존의 통계적 블록암호 분석기법은 큰 계산복잡도로 인해 실용성이 제한되므로, 딥러닝 기반의 새로운 블록암호 분석기법을 연구하여 현실적인 계산복잡도를 달성함
- 본 연구결과는 개발된 블록암호 알고리즘의 안전성 평가 시 유용하게 활용될 수 있을 것으로 기대됨

▣ 박수현 교수

▶수중 네트워크 기반 기술 연구

- 현재 상용화되고 있는 5G를 넘어, 6G로 진화되고 있는 이동통신은 wireless coverage에 수중 도메인을 포함하는 논의가 본격화되고 있음
- 즉, 지상 및 수중간 도메인의 사물인터넷이 만드는 ‘초연결사회’에서 실용화 가능한 통신기술의 필요성으로 인해, 이에 적합한 수중 네트워크 기술 연구가 활성화될 전망임
- 6G가 Underwater IoT에 적용될 시 핵심기술로서 cell-free 네트워크, VLC (Visible Light Communication) 활용, 분산된 학습 기법을 이용한 오류 검출, 수중망 내 BBU(Base Band Unit) Pool과 RRH(Remote Radio Head) 기반 정의 등과 같은 요소의 고려가 필요하며, 이에 대한 지속적인 연구를 수행할 예정임
- 본 연구 결과는 6G 시대에 IoT 초연결사회를 구축하는 핵심기술로서 활용될 수 있을 것

으로 기대함

▶DSC(Dynamic Service Composition)와 IoS(Internet of Service)에 대한 융합기술 연구

- 6G 통신환경에 도래함에 따라 클라우드 서비스와 IoS를 통합하는 연구의 중요성이 커짐
- 특수 도메인 IoT와 결합된 서비스 네트워크 개발을 위해 중앙집중식 서버 환경에서의 클라우드 기반 가변 서비스로서 제공되고 있는 DSC와 IoS기술을 적용하여 특수영역을 포함하는 도메인에서 만나는 사물과의 상호작용이 가능하도록 연구 개발을 진행할 예정임
- 2020년부터 임베디드 환경에서 DSC, IoS 지원이 가능한 네트워크 플랫폼 연구를 수행하고 있는 Veea Inc.(미국)와 협력하여 해당 플랫폼이 적용된 수상, 수중 DSC 서비스 네트워크 모델을 개발하기로 협의함
- 이 결과를 통해 항만, 선박의 고가용성 네트워크 확보와 가변 자율 의사결정 서비스 네트워크를 동시에 제공하여 해당 비즈니스 도메인에서 오랜 기간 지적된 비효율성의 문제를 해결하고 신규 산업 창출 등이 가능할 것으로 기대함

▣ 서석충 교수

▶암호알고리즘에 대한 소프트웨어 최적화 연구

- 동일한 암호알고리즘도 소프트웨어 구현방법에 따라 수배에서 수십배의 성능 차이가 발생할 수 있으며, 산업계에서 널리 활용되기 위해서는 효율성이 보장되어야 함
- 수학적 최적화 방법과 함께 다양한 IoT 장치 및 병렬 컴퓨팅 환경의 특성을 활용한 소프트웨어 암호 최적화 방법론 연구를 수행하고자 함
- 본 연구결과를 통하여 개발된 최적화된 암호 소프트웨어는 다양한 보안시스템에서 활용되어 효율적으로 사용자 데이터에 대한 프라이버시를 제공할 수 있을 것으로 기대함

▶동형암호 소프트웨어/하드웨어 통합 설계 연구

- 2020년 1월 데이터 3법 개정안이 국회를 통과함에 따라 기업에서 가명정보개념을 도입하여 사용자 데이터를 가공하여 활용할 수 있게 됨
- 동형암호는 사용자 데이터가 암호화된 상태에서 다양한 연산을 수행할 수 있기 때문에 사용자 프라이버시를 제공하면서 다양한 서비스가 가능하다는 장점이 있으나, 연산속도가 매우 느림
- 국외의 경우 MS, IBM을 필두로 하드웨어 암호설계를 통해 동형암호의 성능을 고속화하는 연구를 수행 중
- 본 연구단에서는 소프트웨어와 하드웨어의 최적화방법을 함께 고려하는 암호연산기 설계를 연구하고자 함
- 개발된 결과는 데이터 3법 하에서 사용자들이 안심하고 사용할 수 있는 다양한 서버스가 가능하도록 하며 클라우드 컴퓨팅 환경에서도 효율적으로 사용될 수 있을 것으로 기대함

▣ 염용진 교수

▶난수발생기 안전성 분석 및 국내표준화 추진

- 난수발생기에 대한 안전성을 분석한 연구 결과를 기반으로 국가보안기술연구소와 협력하여 TTA 표준문서인 ‘운영체제별 잡음원 수집 및 응용 지침(TTAK.KO-12.0235/R1)’과 소프트웨어 암호모듈에 사용되는 잡음원 시험 평가 지침(TTAK.KO-12.0341)’을 2020년 내에 개정을 주도할 계획이며, 개정된 2건의 표준문서는 한국 암호모듈 검증제도(KCMVP)에서 가이드문서로 활용될 계획임

- 개정된 TTAK-KO-12.0235/R1 표준문서를 이용하여 암호모듈 개발업체에서는 안전한 난수발생기 구현이 가능하며, TTAK.KO-12.0341 표준문서는 시험기관에서 잡음원의 엔트로피 평가 절차 가이드 문서로 활용될 예정임
- 암호학적 난수발생기의 안전성 분석에 대한 지속적인 연구와 표준화 활동을 통하여 안전한 난수발생기 사용에 대한 토대를 마련하고자 함

▶양자내성암호에 대한 고속구현 기술 연구

- NIST는 양자 컴퓨팅 시대에도 안전성을 보장받을 수 있는 양자내성암호에 대한 표준화 공모사업 진행 중이며, 2022년에 표준화 초안을 준비할 예정임
- 2019년 1월에 26건의 2차 후보 알고리즘으로 선정되었으며 대부분 기존에 사용하는 암호알고리즘과 연산 측면에서 상이한 구조를 가짐
- 암호알고리즘이 산업계에서 활용되기 위해서는 안전성 뿐만 아니라 계산 효율성도 보장되어야하기 때문에, 2차 후보 알고리즘의 일부를 구현 효율성 관점에서 분석하고자 함
- 본 연구 결과는 향후 국가/공공기관뿐만 아니라 산업계에서 NIST의 표준화된 양자내성암호 도입 시, 고속구현 기술에 대한 기반연구로 활용될 것으로 기대함

▣ 윤상민 교수

▶인공지능 기술에서의 데이터 및 모델 연구

- 딥러닝 기술의 발전으로 인하여 다양한 분야와 산업계에서 인공지능을 활용한 지능형 시스템 개발에 관한 관심이 크게 증가하고 있으므로, 딥러닝을 비롯한 다양한 인공지능 기술에 대한 데이터 및 모델에 관한 연구를 수행하고자 함
- 연구결과는 인공지능 기술에 대한 이해를 증진시켜 산업계의 다양한 서비스 창출에 활용될 수 있을 것으로 기대함

▶인공지능 기술에서의 데이터 및 모델 연구

- 인공지능 환경에서 데이터의 중요성이 날로 높아지는 상황에서, 데이터의 오류 및 모델의 오류는 사람과 사람, 사람과 기기, 기기와 기기 간의 소통 문제로 이어질 수 있음
- 또한, 인공지능 기술의 허점을 이용하여 해킹을 시도하는 사례가 늘어남에 따라 인공지능 기술의 안정성 및 시스템에 대한 신뢰성에 의문이 제기되고 있는 실정임
- 다양한 딥러닝 모델을 기반으로 소프트웨어적 관점에서 자율성장 및 방어체계를 분석하여 지능형 시스템에 대한 신뢰성 확보 및 다양한 분야에 적용할 수 있는 연구를 수행하고자 함
- 개발된 기술을 오픈 소스로 제공함으로써 관련 기술이 산업계에서 유용하게 활용될 수 있을 것으로 기대함

▣ 이옥연 교수

▶국가 주요 기반시설 보안기술 연구

- 교통망과 같은 국가 주요 기반시설에서는 국내 CC인증을 받은 정보보안제품 사용이 필수적이므로, 교통신호 통합 DB센터를 5G를 적용한 DB센터와 연동할 수 있도록 보안 규격에 맞는 보안통신 SSL VPN을 적용할 예정임
- 또한, 군이 개발 및 제작한 암호를 탑재한 드론을 분석하여 드론의 프로세서, 메모리, 운영체제 또는 펌웨어 등의 유통 과정 및 제조과정에서 생길 수 있는 피해에 대해 대비하며 안전한 공급망을 확보할 계획임

▶6G 환경에서의 암호기술 연구

- 6G에 연결될 수 있는 저사양의 IoT 장치, 임베디드 장치, 고성능 PC와 같이 다양한 성능을 가진 기기에서의 암호기술의 가용성에 대해 연구함으로써 6G를 활용한 다양한 융합서비스에 사용될 수 있도록 할 예정임
- 또한, 양자난수 기술 등 최신의 보안기술을 적극 수용하여 높은 보안강도의 제공 및 가용성을 보장할 수 있는 플랫폼을 개발하고 이러한 기술의 증진을 토대로 융합보안 시장을 선도할 수 있는 연구결과와 전문인력 양성으로 기여할 계획임
- 이와 같이 6G에서의 암호기술에 대해 연구함으로써 기존 산업 혁신 및 신지능 서비스 활성화, 초연결·초신뢰의 안전한 미래 디지털 생태계 구축 및 국가 지능화를 통한 산업 경쟁력의 재도약을 이룰 수 있을 것으로 기대함

▣ 최은미 교수

▶인공지능과 보안시스템의 융합연구

- 다양한 인공지능 기술과 다양한 응용 및 보안시스템을 융합하는 것에 대한 요구가 증가하고 있으며, 인공지능 기술 분야에서 Expert System과 머신 러닝 분야의 응용 어플리케이션 개발 연구를 수행하고자 함
- 특히, 금융정보보안 기술을 적용할 시스템 설계와 응용 어플리케이션 개발에 있어서, 블록체인 기술을 적용하는 응용 비즈니스 모델 도출을 연구 진행 중임
- 또한, 빅데이터 처리를 위한 대용량기반 구조와 클라우드 기반 기술을 분산 정보 지능화의 응용 시스템으로 개발하는 방안을 지속적으로 연구 진행 중임
- 본 연구의 결과는 인공지능기술과 보안기술을 융합함으로써 인공지능 기술의 안전한 활용과 인공지능을 통한 보안문제를 해결하는데 기여할 수 있을 것으로 기대함

▣ 한동국 교수

▶양자내성암호에 대한 부채널분석 안전성 연구

- NIST 양자내성암호 공모가 현재 진행 중이며 부채널분석에 대한 안전성은 중요한 선정기준이며, 양자내성암호 공모에 제출된 다양한 암호 알고리즘에 대한 이론적 부채널분석 취약점 및 구현 이후의 발생 가능한 취약점을 파악하는 연구를 수행하고자 함
- 본 연구결과는 양자내성암호를 선정하는 주요기준으로 활용될 수 있으며 또한, 양자컴퓨팅 시대에 사용될 양자내성암호의 안전성을 높여 다양한 서비스 창출이 가능할 것임

▶암호디바이스에 대한 실질적인 부채널분석 안전성 연구

- 최근 부채널 대응기법이 적용된 암호알고리즘을 암호장치에 탑재할 때 커플링 효과 등의 구현적 취약점이 발생할 수 있음이 제기되어 이를 해결할 수 있는 방안을 연구하고자 함
- 또한, 기계학습을 활용하여 기존의 높은 복잡도로 제한되었던 다양한 부채널분석 방법들의 한계를 극복하는 연구를 진행할 예정임
- 2019년 12월부터 2021년 11월까지 3년간 산업통상자원부 주관 국제공동기술개발사업의 ‘딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발’ 연구 수행할 예정임
- 레이저, 전자파, 전압 글리치 등을 사용하는 준침입 공격을 이용하여 인증 우회 등에 대한 문제가 제기되고 있으며, 이러한 준침입 공격에 대한 다양한 대응방법 연구를 수행하여 개인 정보 탈취 문제를 해결하고자 함

3. 연구의 국제화 현황 및 계획

3.1 참여교수의 국제적 학술활동 참여 실적 및 현황

▣ 참여교수별 국제적 학술활동 참여 실적

▶강주성 교수

- 미국 NIST의 SP 800-90B의 Non-IID 잡음원에 대한 엔트로피 평가 방법 중 가장 소요 시간이 긴 MultiMCW 엔트로피 추정 방법을 Python 및 C 언어로 고속 구현하고 효율성을 분석한 결과는 그 우수성을 인정받아 AINS 2017에서 Best Paper Award를 수상함

▶김동찬 교수

- 국제 표준화 기구 ISO에서 2016년부터 SC27 WG2 한국 대표 전문가로서 활동하고 있으며, 최근 경량 블록암호 표준인 29192-2:2019 주 저자로 3년 6개월 동안 표준화 작업을 수행하였음
- 2016년부터 국제 암호학회 ICISC의 프로그램 위원으로 활동 중이며, 2017년에는 프로그램 위원장을 역임하면서 ICISC 2017 논문집을 편찬함(eBook ISBN 978-3-319-78556-1)

▶김종성 교수

- 국제 저명 디지털 포렌식 워크숍 DFRWS가 주최한 DFRWS Forensic Challenge에서 2018년 2위, 2019년 1위를 각각 입상함
- 두 대회는 IoT Forensic Challenge라는 주제로 진행되어 주어진 디지털 증거들을 기반으로 용의자를 지목하고 그 근거를 제시하는 방식으로 디지털 포렌식 첼린지 대회를 통한 연구의 실효성을 입증함
- 한국정보보안학회 산하 디지털 포렌식연구회가 주최한 국제 Tech Contest 논문부문에서 2018년 2위, 2019년 1위를 각각 입상함
- 2018년에는 피트니스 밴드에서 얻을 수 있는 정보를 분류, 데이터 추출 방법 및 포렌식 활용 방안을 제시함
- 2019년에는 암호화된 삼성 스마트폰 백업 파일에 대한 복호화 방안을 제시하여 결과가 각각 채택되었음
- 국제학술대회 PlatCon 2018 프로그램 위원장직을 수행했으며, Applied Soft Computing, Wireless Personal Communications 등 다수의 SCI(E) 저널 특집호 에디터로 활동하였음
- Applied Soft Computing, Wireless Personal Communications 등 다수의 SCI(E) 저널 특집호 에디터로 활동하고 있음

▶박수현 교수

- 수중분야 최대 학술교류 네트워크로서 유명 대학과 기관이 참여하는 WUWNet 2018 학술대회에서 기술력을 인정받아 기술의 상세설계에 대한 높은 관심을 받았음
- 또한, 국제학술대회 ICGHIT 2019에서 다이버를 위한 실시간성과 신뢰성이 담보되는 네트워크 기술에 대한 개념, 프로토타입의 개발 및 실험 결과를 발표하였으며, 우수논문으로 선정되는 결과를 도출하였음
- IoUT 환경에서의 RESTful 데이터 접근 및 처리 방법의 구현과 검증을 위한 국제 공동연구로서 핀란드 SAVONIA 대학과의 협업을 성공적으로 수행하여 UWASN 국제 표준화 제정에 우호적인 전문가 네트워크를 구축하였음
- 이러한 국제 수준의 수중 통신분야 전문 연구자와의 적극적인 인적 교류를 바탕으로 현재까지 ISO/IEC JTC 1/SC 41에서 4건의 IS 발간을 성공적으로 완료하였고, 추가적으로 2건의

표준안이 국제표준으로 승인되어 2020년 IS 발간을 앞두고 있음
- 2019년 중국 CQUPT 캠퍼스에서 개최된 Internet of Things Technology and Standards Summit Forum에서 “Current Technologies of Underwater IoT and Standardization” 주제 발표를 하였음

▶염용진 교수
- 암호화에 필수적인 난수를 생성하는 기법에 관한 실험적 분석 연구로 GPU에서 생성되는 잡음원으로부터 추출되는 엔트로피의 양을 측정하고 분석한 연구 결과는 그 우수성을 인정받아 PlatCon’15에서 Best Paper Award를 수상함
- 미국 NIST의 SP 800-90B의 Non-IID 잡음원에 대한 엔트로피 평가 방법 중 가장 소요 시간이 긴 MultiMCW 엔트로피 추정 방법을 Python 및 C 언어로 고속 구현하고 효율성을 분석한 결과는 그 우수성을 인정받아 AINS 2017에서 Best Paper Award를 수상함

▶윤상민 교수
- Sensors 국제학술지 편집위원으로 컴퓨터 비전 분야에서 대용량의 데이터를 기반으로 한 사람의 자세 추정 및 추적과 관련된 분야에서의 심사 및 위원으로 활동하고 있음

▶이옥연 교수
- ICISC2018 (International Conference on Information Security and Cryptology) 국제학술대회의 운영위원으로 국제교류에 참여함
- WISA2018 (World conference on Information Security Applications) 운영위원장으로 국제학술대회를 주최하고 국제교류를 선도함
- CSA-CUTE2018 (Advances in Computer Science and Ubiquitous Computing) 국제학술대회의 운영위원으로 참여하여 국제교류에 참여함
- ICUFN2018 (International Conference on Ubiquitous ad Future Networks) 국제학술대회의 운영위원으로 참여함
- Platcon2019 (International Conference on Platform Technology and Service) 국제학술대회의 운영위원으로 참여함
- WISA2019 (World conference on Information Security Applications) 국제학술대회에 운영위원으로 참여함

▶최은미 교수
- 국제학술대회 BIGDAS 2017 에서 “An Oriental Medical Recommendation System Architecture based on OWL Ontology with ARC2 Library” 의 논문에 대하여 Best Paper Award를 수상함
- 국제학술대회 CUTE 2016 에서 “An Evaluation of Availability, Reliability and Power Consumption for a SDN Infrastructure using Stochastic Reward Net” 의 논문에 대하여 Best Paper Award를 수상함
- 국제학술대회 BIGDAS and ICDIM 2015에서 “A GPS Trajectory Map-Matching Mechanism with DTG Big Data on the HBase System” 의 논문에 대하여 Best Paper Award를 수상함
- Dependability Engineering, Chapter of Stochastic Reward Net-based Modeling Approach

for Availability Quantification of Data Center Systems, pp61-83, ISBN 978-1-78923-258-5, DOI: 10.5772/intechopen.74306, 2018 국제 저술 활동 공동 저자로 활동함
- JIPS (Joural of Information Processing Systems) 국제학술지 편집위원으로 활동함(~2018)
- CUTE2019 (International Conference on Ubiquitous Information Technologies) 운영위원으로 활동함
- BIGDAS2019 (International Conference on Big Data Applications and Services) 운영위원으로 활동함
- ICBDSC2020 (International Conference on Big Data and Smart Computing) 좌장으로 활동함

▶한동국 교수
- 2016년 국제 저명 학술대회 Conference on Cryptographic Hardware and Embedded Systems 2016 (CHES 2016)에서 진행된 Capture The Flag Challenge에서 3위에 입상함
- 본 대회는 암호 알고리즘 AES에 다양한 부채널 분석 대응기법을 적용한 구현 방법들에 대한 전력 분석 공격을 수행하여 단시간 내에 비밀 키를 도출하는 능력을 발휘하며 서로의 역량을 발휘하는 최고의 국제대회임
- Information Security and Cryptology – ICISC 2017의 Organization Chair로 2017년 11월 29일부터 12월 1일까지 서울에서 진행된 정보보안 및 암호 분야의 국제 학술대회를 성공적으로 진행하였음
- 2019-2020 Applied Sciences 저널 Special Issue Side Channel Attacks and Countermeasures 특집호 에디터로 활동함

3.2 참여교수의 국제 공동연구 실적 및 계획

<표 3-5> 최근 5년간 국제 공동연구 실적

연번	공동연구 참여자		상대국 /소속기관	국제 공동연구 실적	DOI 번호/ISBN 등 관련 인터넷 link 주소
	교육연구단 참여교수	국외 공동연구자			
1	이옥연	Mark Teheranipoor	미국/ University of Florida	Technical Development of Security Validation for Firmware on IoT devices	-
2	김종성	Muhammad Yasin, Junaid Ahmad Qureshi; Firdous Kausar	사우디 아라비아/King Saud Univ; 사우디 아라비아/Mobily, Imam Univ.	A granular approach for user-centric network analysis to identify digital evidence. Peer-to-Peer Networking and Applications 8(5): 911-924 (2015)	https://doi.org/10.1007/s12083-014-0250-x
3	김종성	Hang Tu; Neeraj Kumar	중국/Wuhan Univ.; 인도/Thapar Univ.	A strongly secure pairing-free certificateless authenticated key agreement protocol suitable for smart media and mobile environments. Multimedia Tools Appl. 74(16): 6365-6377 (2015)	https://doi.org/10.1007/s11042-015-2470-3
4	박수현	Kwan Yi	미국/ Eastern Kentucky University	Khamdamboy Urunov, Soo-Young Shin, Soo-Hyun Park, and Kwan Yi (2017) U-SNMP for the Internet of Underwater Things, International Journal of Control and Automation, Vol. 10, pp. 199-216.	http//dx.doi.org/10.14257/ijca.2017.10.10.17
5	박수현	Mohan Krishna Varma N	인도/ Madanapalle Institute of Technology and Science	Mohan Krishna Varma N, Kalyani M, Soo-Young Shin & Soo-Hyun Park (2019) Underwater Spray and Wait Routing technique for Mobile Ad-hoc Networks, Indian Journal of Geo Marine Sciences, Vol. 48, pp. 1648-1655.	http://nopr.niscair.res.in/handle/123456789/51147
6	윤상민	김상국	미국/MIT	AI for Design: Virtual Design Assistant (CIRP Annals, Vol.68, pp.242-244, 2019.	https://doi.org/10.1016/j.cirp.2019.03.024
7	한동국	Máire O'Neill;Neil Hanley	영국/Queen's University	An Improved Second-Order Power Analysis Attack Based on a New Refined Expecter - Case Study on Protected AES -	https://doi.org/10.1007/978-3-319-31875-2_15

연번	공동연구 참여자		상대국 /소속기관	국제 공동연구 실적	DOI 번호/ISBN 등 관련 인터넷 link 주소
	교육연구단 참여교수	국외 공동연구자			
8	한동국	Máire O’Neill;Philip Hodgers	영국/Queen’s University	On the Security of Balanced Encoding Countermeasures	https://doi.org/10.1007/978-3-319-31271-2_15

3. 연구의 국제화 현황 및 계획

3.2 참여교수의 국제 공동연구 실적 및 계획

▣ 국가적 경계를 뛰어넘은 개방혁신(open innovation) 환경 기반 국제공동 연구 계획

▶김동찬 교수

- 국제 표준 기구 ISO/IEC의 SC27 (Information security, cybersecurity and privacy protection)은 정보보안 관련 표준 분야로, 5개의 WG (Working Group) 중 WG2는 암호 알고리즘 표준 그룹임
- 세계 각국의 암호 전문가들이 매년 2회의 정기 회의를 통해 우수 암호 알고리즘의 표준화를 추진함
- SC27 WG2 국내전문위원인 김동찬 교수는 2016년부터 WG2의 한국대표로 참여 중이며, 최근 주저자로 국내 경량 블록암호 LEA의 국제표준화(29192-2:2019)를 주도하였음
- 현재 WG2는 NIST 표준 양자내성암호 공모전 종료 시점에 맞춰 표준화 작업을 사전 준비 중에 있음
- 매 정기 회의에서 양자내성암호 튜토리얼 세션을 열 정도로 산업계의 큰 이슈인 양자내성암호에 대해 관심이 매우 높음
- 김동찬 교수는 향후 대학원생들과 지속적으로 국제표준화 활동을 통해 양자내성암호 국제표준 최신 동향 파악 및 국내 알고리즘의 국제표준화 작업을 수행할 계획임

▶김종성 교수

- 뉴질랜드 MASSEY 대학 컴퓨터과학 및 정보기술부의 Julian Jang-Jaccard 교수와 보안 관련 주제로 공동연구를 진행할 예정이며 공동 연구의 주제는 크게 IT 응용서비스 상의 사이버 안전성 연구와 사이버 범죄 수사 연구로 구성할 계획임

▶박수현 교수

- 국민대학교와 5G/6G 유무선 통신분야 전문가가 속한 대학/연구소는 인재교류와 공동연구 추진을 목표로 ‘대학/연구소 우수 인재의 국민대학교 교환학생’ 또는 ‘석박사 학위 교류, 실용학문 중심 기반의 연구’를 바탕으로 한 국제공동연구 등의 내용을 담은 양해각서(MoU)를 해외대학 혹은 연구소와 체결할 예정임
- 국제협력을 바탕으로 해외 유수 산, 학, 연에 종사하고 있는 전문가를 초빙하여 워크숍 및 세미나를 진행할 예정임
- Underwater IoT 또는 미래 산업/시장 적용을 위해 고려해야 할 보안 이슈에 대해 심도있는 연구를 수행하고 있는 전문가들로부터 빠르게 변화하고 있는 현 기술의 국제 동향을 습득하고, 연구 결과 공유 및 교류할 수 있는 기회의 장이 마련될 것임
- 이를 바탕으로 국제학회에서 구두 발표 혹은 국제 저널 투고 결과를 성취할 수 있도록 참여대학원생들을 독려할 예정임
- 현재 해양통신 또는 IoT 기반 해양 네트워크 기술에 대한 표준화가 공적 국제표준으로 ISO/IEC JTC 1/SC 41에서 각국의 Expert와의 직·간접적인 교류를 통하여 국제표준 기획 및 발간이 이뤄지고 있음
- 박수현 교수는 2014년 NWIP 제안을 시작으로 지속적으로 Project Leader 활동 및 Main Editor로 표준화를 진행하면서 각 표준의 Co-editor로서 인도, 미국, 핀란드 중국 등의 Expert와 함께 표준을 개발하고 있음
- 국제표준화 회의 참여를 바탕으로 이뤄지는 국제공동연구를 통하여 국제표준에 국내기술을 전략적으로 반영할 수 있는 발판 마련과 더불어 핵심기술에 대한 기술 주도권 선점으로 인

한 우리나라 기술 경쟁력 또한 높아질 것으로 예견됨

▶이옥연 교수

- 과학기술정보통신부 주관 국제공동연구사업의 ‘IoT 장비 펌웨어 보안성 검증 기술개발’ 연구를 통해 2018년 6월부터 2020년 12월까지 총 3년간 미국의 플로리다 주립대학교 내 FICS 연구소와 공동연구를 진행 중임
- 본 국제 공동연구를 통해 IoT 장비의 펌웨어 보안성 검증 기술 개발을 위해 펌웨어, 하드웨어, 통신채널, 서비스와 같은 서로 다른 4개의 계층에서 새로운 IoT 보안성 검증 프레임워크의 개발 및 보안성 검증을 수행하여 산업·사회 문제를 해결하기 위한 연구를 진행할 예정임
- 과학기술정보통신부 정보보안핵심원천기술개발 사업의 일환으로 2020년 04월 01일부터 2027년 12월 31일까지 총 93개월 동안 ‘5G+ 6G 이동통신 정보보안 기술 연구‘ 과제를 수행할 예정임
- 해당 과제를 통해 5G/6G 이동통신 정보보안에 대한 3GPP의 표준활동에 본 교육연구단의 대학원생이 참여할 예정임

▶한동국 교수

- 산업통상자원부 주관 국제공동기술개발사업의 ‘딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발’ 연구를 통해 2019년 12월부터 2021년 11월까지 총 3년간 프랑스의 Texplained와 공동연구를 진행 중임. 본 국제 공동연구를 통해 산업·사회 문제를 해결하기 위한 연구를 진행할 예정임

3. 연구의 국제화 현황 및 계획

3.3 외국 대학 및 연구기관과의 연구자 교류 실적 및 계획

▣ **본 교육연구단은,** 외국 주재 전문가를 초빙하여 강연회나 토론회를 열거나 외국의 유수한 대학, 연구소와 공동 연구를 진행하여, 학생들이 외국과의 기술을 익히고 경험할 수 있도록 프로그램을 꾸준히 개발해 운영하고 있으며, 계속해서 교류의 기회를 확대하고자 함

▶**Maire O'Neill의 주도로** Centre for Secure Information Technologies (CSIT), ECIT, Queen's university Belfast, Queens Road, Queens Island이 참여하는 공동 연구에 참여 (2015.03.02~2016.02.28)

- 한동국 교수와 더불어 2015년 4월 9일부터 동년 8월 10일까지 학생으로 안현진, 원유승이 참여했고 2015년 9월 1일부터 이듬해 2월 28일까지 박애선, 심보연 두 학생이 참여하였음
- 본 공동 연구를 통해 부채널을 사용한 금융 IC 카드, 하드웨어 보드, 소프트웨어 보드 등을 분석하는 기법과 부채널을 사용한 공격에 대응하는 기법, 부채널에 관련한 최신 동향과 Post-Cryptography의 최신 동향 등을 연구하였음

▶**인도 IIIT Delhi 소속 장동훈 교수 전문가 초빙(2016.06.21)**

- 인도 IIIT Delhi 장동훈 교수를 초빙하여 인증(Authentication) 메커니즘의 최근 동향과 연구결과를 소개하는 자리를 마련하였음

▶**미국 Eastern Kentucky University의 Kwan Yi 교수 전문가 초빙(2017.06.14)**

- 박수현 교수는 Eastern Kentucky University Kwan Yi 교수를 초빙하여 미국의 정보학에 관한 이해 및 최신동향을 파악하고 이를 바탕으로 다양한 정보를 분류하고 해석하여 활용하는 전략에 대해 토의하였음
- 새로운 통신 프로토콜 개발에 필요한 효과적인 통신 프로토콜 설계 지식 학습 방법에 대해 공동연구를 수행하고 "U-SNMP for the Internet of Underwater Things"을 2017년 10월 SCPOUS에 게재하였음

▶**IACR 주관으로** 대만의 타이페이에서 개최된 CHES 2017 컨퍼런스 참석(2017.09.25~28)

- 한동국 교수와 박애선, 원유승, 심보연, 이종혁 학생이 참석하여 하드웨어 임베디드 시스템에 적용되는 보안의 국제적 흐름을 파악할 수 있는 기회를 가졌음. 특히 부채널 분석과 관련된 최신 동향, 미래에 사용될 포스트 퀀텀 암호분야의 동향에 대해 알 수 있는 기회가 되었음

▶**IACR 주관으로** 홍콩 대학에서 개최된 Asiacrypt 2017 학회 참석(2017.12.03~07)

- 이재훈, 위한샘 학생은 현 보안연구의 국제적 흐름을 파악할 수 있는 기회를 가졌음. 특히 네트워크 프로토콜과 관련된 최신 연구 동향에 대해 알 수 있는 기회가 되었음.

▶**벨기에 루뱅** 가톨릭 대학교(KU Leuven) 소속 바트 프레닐(Bart Preneel) 전문가 초빙 (2017.12.08)

- 정보보안 분야 석학인 바르트 프레닐(Bart Preneel) 교수를 초빙하여 암호화폐(Cryptocurrency)의 최근 동향과 연구 결과를 소개하는 자리를 마련하였음

▶**네덜란드의** 부채널 분석 연구기관 Riscure에서 준침입 공격에 대한 교육을 2차례 수강 (1회: 2017.12.07~08) (2회: 2018.09.05~06)

- 이종혁 학생은 준침입 부채널 공격 방법인 오류 주입 공격 방법에 대한 교육을 수강함으로써 부채널 분석 기술을 주도하고있는 유럽의 선진 부채널 분석 기술을 습득할 기회를 가졌음

▶**미국 플로리다** 주립대학교의 Mark 교수팀과 국제공동연구 수행(2018~현재)

- 이옥연 교수는 ㈜이와이엘과 미국 플로리다 주립대학교의 Mark 교수팀과 함께 2018년부터 국제공동연구를 수행하고 있음

▶**말레이시아** UTAR 대학의 Ben Lee Wai Kong 교수 전문가 초빙(2018.10.12)

- GPU/FPGA 등이 적용된 고효율 데이터 프로세싱 방법에 대한 세미나를 진행하고, 수중통신의 제한된 리소스 상황에서 '지능화'를 목표로 적합한 시스템의 요구사항을 토의하였음

▶**인도 MITS** 대학(Madanapalle Institute of Technology and Science)과 MOU 체결 (2018. 11.19)

- 국민대학교와 MITS 대학은 양 대학간 인재교류와 공동연구 추진을 목표로 MOU를 체결하므로 MITS 우수 인재의 국민대학교 교환학생 또는 석박사 학위 교류 및 MITS 강점 분야인 실용학문 중심 기반의 연구를 바탕으로 한 국제공동연구를 수행하였음
- 수중통신 관련 주제로 공동연구를 진행한 결과 "Underwater Spray and Wait Routing technique for Mobile Ad-hoc Networks" 논문이 2019년 Indian Journal of GeoMarine Sciences에 게재되었음

▶**미국 Chapman** Univ.의 연구원으로 있는 조원희 박사를 전문가 초빙(2019.01.29)

- 대학원생들의 IT전문가로서 차별성을 위한 Deep Learning과 관련된 Python 및 TensorFlow에 관한 교육, 그리고 분야별 BigData 분석에 관한 교육을 실시하여 사회에서 필요로 하는 인력에 대한 전문지식을 습득하는 기회를 가졌음
- 대학원생들은 관련분야 연구를 진행하면서 가지고 있었던 생각들을 조원희 박사와 교환하는 토론시간을 가졌음
- 또한, 조원희 박사의 미국 University of Southern California의 연구 경험에 대하여도 발표하는 등 해외 취업에 관하여 이야기하는 시간을 가졌음

▶**사물인터넷 국제표준 전문가 초빙(2019.01.03) (2019.05.27)**

- 추진 중인 수중사물인터넷 국제표준그룹 설립을 목표로 미국의 전문가인 WSN Tech의 Howard Choe 박사(2019년 1월) 및 핀란드의 전문가인 Savonia 대학의 Arto Toppinen 교수(2019년 5월)를 초청하여 미국 및 유럽국가들의 지상망 네트워크 기반 지능화 사물인터넷과 산업/시장 적용 현황에 대한 세미나를 진행하고 수중사물인터넷 연구방향에 대한 토의를 진행하였음

▶**미국** University of Florida의 Mark M. Tehranipoor, PhD 교수 전문가 초빙(2018.08.25)

- 이옥연교수는 Mark M. Tehranipoor 교수를 초빙하여, 미국내의 암호장비에 관한 정책과

하드웨어 보안 및 암호 SoC 설계에 대한 최신동향을 공유하였음

▶**미국** University of Florida의 Swarup Bhunia, PhD 교수 전문가 초빙(2018.08.25)
- 이옥연교수는 Swarup Bhunia 교수를 초빙하여, 하드웨어 보안 및 암호 SoC 설계에 대한 최신동향을 공유하였음

▶**뉴질랜드** MASSEY 대학과의 교류
- 김종성 교수는 뉴질랜드 MASSEY 대학 컴퓨터과학 및 정보기술부의 Julian Jang-Jaccard 교수와 보안 관련 주제로 공동연구를 진행할 예정임

▶**인천국제해양포럼을 계기로 국제 교류 추진**
- 박수현 교수는 인천항만공사에서 2020년 9월 22-24일 개최예정인 제1회 인천국제해양포럼에서 '세션 4 스마트해양'을 총괄하며 IoT 분야의 저명한 해외전문가를 연사로 초청할 예정임
- 본 포럼을 통하여 4차산업혁명의 핵심을 기반으로 미래 통신시스템에 접목될 Underwater IoT 기술 경쟁력이 제고될 것이며, 더 나아가 대한민국 미래해양산업의 핵심이 될 수중통신 표준화 역량을 강화시킬 수 있을 것으로 기대됨

▶**싱가포르 난양 기술 대학과의 교류**
- 싱가포르 난양 기술 대학교(Nanyang Technology University)의 Physical Analysis & Cryptography Engineering (PACE) 소속 원유승 연구팀과 2020년 4월부터 격주 온라인 세미나를 통해 교류를 수행하며 연구를 진행하고 있음
- 2018년에 본 대학원 박사과정을 졸업한 원유승 박사와 2018년 6월부터 한동국 교수의 지도 학생 문재근 박사과정과 이종혁 석박사통합과정이 세미나를 진행하며 교류하고 있음
- 2020년 4월부터 격주 온라인 세미나를 통해 연구를 진행하고 있으며 연구 주제에 대한 논의와 더불어 외국 연구기관에서 관심을 갖는 주제들에 대한 동향 교류를 지속적으로 수행할 예정임
- PACE 팀과 2021년 1월~2월 겨울 방학 기간에 각 2주 이상 상호 기관 방문 통해 Cold-Boot Attack 연구주제와 Machine Learning 기반 상용 IC카드 분석 연구주제로 직접적인 교류를 추진할 계획임

Ⅳ. 사업비 집행 계획

1. 사업비 집행 계획(1-8차년도)

(단위: 천원)

항목	1차년도 (20.9-21.2)	2차년도 (21.3-22.2)	3차년도 (22.3-23.2)	4차년도 (23.3-24.2)	5차년도 (24.3-25.2)	6차년도 (25.3-26.2)	7차년도 (26.3-27.2)	8차년도 (27.3-27.8)	계
대학원생 연구장학금	129,360	258,720	258,720	258,720	258,720	258,720	258,720	129,360	1,811,040
신진연구인력 인건비	54,000	108,000	108,000	108,000	108,000	108,000	108,000	54,000	756,000
산학협력 전담인력 인건비	18,000	36,000	36,000	36,000	36,000	36,000	36,000	18,000	252,000
국제화 경비	10,000	22,848	22,848	22,848	22,848	22,848	22,848	10,000	157,088
교육연구단 운영비	15,000	30,000	30,000	30,000	30,000	30,000	30,000	15,000	210,000
교육과정 개발비	8,000	12,000	12,000	12,000	12,000	12,000	12,000	8,000	88,000
실험실습 및 산학협력 활동 지원비	11,424	24,000	24,000	24,000	24,000	24,000	24,000	11,424	166,848
간접비	12,936	25,872	25,872	25,872	25,872	25,872	25,872	12,936	181,104
합계	258,720	517,440	517,440	517,440	517,440	517,440	517,440	258,720	3,622,080

Ⅳ. 사업비 집행 계획

2. 사업비 집행 세부 내역(1~8차년도)

2. 사업비 집행 세부 내역(1-8차년도)

[1차년도]

1) 대학원생 연구장학금

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
석사과정생	15.4	700	6	64,680
박사과정생	5.6	1,300	6	43,680
박사수료생	3.5	1,000	6	21,000
합계	24.5	작성 불필요	작성 불필요	129,360

【작성방법】

1) 사업에 참여하는 교수 전체 지도학생 중 참여 요건을 충족하는 학생 70% 이내 범위에서 지원

※ '융합전공'으로 신청하는 경우 석사·박사 수료생은 연구장학금을 지원할 수 없음

2) 통합과정생의 경우 2년 이내는 석사과정생, 2년 초과는 박사과정생으로 포함

3) 석사과정생 월 70만원, 박사과정생 월 130만원, 박사 수료생 월 100만원

2) 신진연구인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
박사후 과정생	1	3,000	6	18,000
계약교수	2	3,000	6	36,000
합계	3	작성 불필요	작성 불필요	54,000

【작성방법】

1) 박사후 과정생 및 계약교수는 월 300만원 기준으로 작성

3) 산학협력 전담인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
산학협력 전담인력	1	3,000	6	18,000

【작성방법】

1) 산학협력 전담인력 인건비는 주관대학 지급기준에 따라 작성

※ 단, 전임교원 인건비로는 편성 불가

4) 국제화 경비

(단위: 천원)

구분	산출근거	금액
단기연수	▸Univ. of Florida FICS 단기 연수 세미나 - 항공료 및 체재비 ・항공료 : 2,000,000원 x 2회 = 4,000,000원 ・체재비(일비) : $30 x 2명 x 7일 x 1,200원(환율) = 504,000원 ・체재비(숙박) : $120 x 2명 x 7일 x 1,200원(환율) = 2,016,000원 ・체재비(일비) : $80 x 2명 x 7일 x 1,200원(환율) = 1,344,000원	7,864
장기연수	▸ - ・	
해외석학초빙	▸ - ・	
기타국제화활동	▸국제(TCC 학회 참석, 미국 2020.11.) -항공료 및 체재비 ・항공료 : 756,000원 x 1회 = 756,000원 ・체재비(일비) : $30 x 1명 x 5일 x 1,200원(환율) = 180,000원 ・체재비(숙박) : $120 x 1명 x 5일 x 1,200원(환율) = 720,000원 ・체재비(일비) : $80 x 1명 x 5일 x 1,200원(환율) = 480,000원	2,136
합계		10,000

【작성방법】

1) 대학원생의 장・단기 해외연수와 같이 대학원생이 주체가 되어 참여하는 국제협력 프로그램 및 기타 국제협력 활동에 대한 경비로 집행
2) 교수의 세미나 참석이 아닌, 대학원생이 국제학술대회 발표, 해외 연구자와의 공동세미나에 참석하는 경우에 대해 작성(참석 및 목적이 뚜렷하지 않은 단기 해외연수 지양)
3) 해외석학 초빙 경비의 경우 대학의 전문가 초청 기준에 따르며, 초빙 수당, 체재비 및 항공료 등 지원 항목별 세부적으로 기재

5) 교육연구단 운영비

(단위: 천원)

구분	산출근거	금액
교육연구단 전담직원 인건비	▸교육연구단 전임직원 - 행정직원 1인 · 3,500,000원 x 6개월 x 1인 x 25% = 10,500,000원	10,500
성과급	▸ - ·	
국내여비	▸ - ·	
학술활동지원비	▸ - ·	
산업재산권 출원등록비	▸특허 -국내특허 출원 1건 · 3,000,000원 x 1건 = 3,000,000원	3,000
일반수용비	▸ - ·	
회의 및 행사 개최비	▸ - ·	
각종 행사경비	▸교육단 전체 워크숍 -장소 사용 및 부대경비 · 1,500,000원 x 1회 = 1,500,000원	1,500
기타	▸ - ·	
합 계		15,000

【작성방법】

1) 인건비: 교육연구단 소속 업무전담 직원 인건비

2) 성과급: 참여교수, 신진연구인력, 참여 대학원생 중 우수한 연구 성과 및 사업에 공헌도가 있는 자에 대한 성과급

▸ 교육연구단별 운영 기준에 따라 기여도 평가를 실시하여 기여도에 따라 성과급 배분

3) 국내여비: 대학 자체 여비 기준 적용

4) 학술활동지원비

▸ 논문게재료, 국내 학회 및 세미나 참가비(일회성), 전문가 초청 자문료, 도서 등 문헌 구입비, 국내·외 정보 수집비

▸ 학회 연회비 등 참여교수 개인에 대한 경비 및 학회 후원금 성격 지출 불가

5) 산업재산권출원등록비: 국내외 특허 출원 및 등록비

6) 일반수용비: 사무용품비, 인쇄비, 각종 수수료 및 사용료, 전화료 등

▸ 연구기자재 구입비 및 시설비, 상품권 등 선물 구입비 편성 불가

6) 교육과정 개발비

(단위: 천원)

산출근거	금액
▸온라인 강의 교재 개발 -정보보안 최신 기술 교재 4건 ・2,000,000원 x 4건 = 8,000,000원	8,000
▸ - .	
▸ - .	

【작성방법】

1) 교재개발비, 사례조사비 및 실험비 등 교육과정 개발 관련 제반 경비를 편성

7) 실험실습 및 산학협력활동 지원비

(단위: 천원)

산출근거	금액
▸산학협력 워크숍 -전문가 강의료 ・300,000원 x 6인 = 1,800,000원 -강의장 대관료 ・5,000,000원 x 1회 = 6,200,000원	8,000
▸소모성 재료비 -암호장비용 PCB ・3,424,000원 x 1건 = 3,424,000원	3,424
▸ - .	

【작성방법】

1) 소모성 재료비 및 창업, 취업지도, 산업체와의 산학협력 공동활동 경비 편성(자문료, 강사료, 취・창업 관련 행사개최비 등)

※ 단, 기자재 및 장비 구매비 편성 불가

8) 간접비: 12,936 천원

【작성방법】

1) 연간 사업비의 5% 이내

2) 과학기술원 소속 교육연구단(팀) : 연간 사업비의 2% 이내

▸ 한국과학기술원, 울산과학기술원, 광주과학기술원, 대구경북과학기술원

[2차년도]

1) 대학원생 연구장학금

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
석사과정생	15.4	700	12	129,360
박사과정생	5.6	1,300	12	87,360
박사수료생	3.5	1,000	12	42,000
합계	24.5	작성 불필요	작성 불필요	258,720

【작성방법】

1) 사업에 참여하는 교수 전체 지도학생 중 참여 요건을 충족하는 학생 70% 이내 범위에서 지원

※ '융합전공'으로 신청하는 경우 석사박사 수료생은 연구장학금을 지원할 수 없음

2) 통합과정생의 경우 2년 이내는 석사과정생, 2년 초과는 박사과정생으로 포함

3) 석사과정생 월 70만원, 박사과정생 월 130만원, 박사 수료생 월 100만원

2) 신진연구인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
박사후 과정생	1	3,000	12	36,000
계약교수	2	3,000	12	72,000
합계	3	작성 불필요	작성 불필요	108,000

【작성방법】

1) 박사후 과정생 및 계약교수는 월 300만원 기준으로 작성

3) 산학협력 전담인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
산학협력 전담인력	1	3,000	12	36,000

【작성방법】

1) 산학협력 전담인력 인건비는 주관대학 지급기준에 따라 작성

※ 단, 전임교원 인건비로는 편성 불가

4) 국제화 경비

(단위: 천원)

구분	산출근거	금액
단기연수	▸Univ. of Kentucky 단기 연수 세미나 - 항공료 및 체재비 ・항공료 : 2,240,000원 x 2명 x 1회 = 4,480,000원 ・체재비(일비) : $30 x 2명 x 10일 x 1,200원(환율) = 720,000원 ・체재비(숙박) : $120 x 2명 x 10일 x 1,200원(환율) = 2,880,000원 ・체재비(일비) : $80 x 2명 x 10일 x 1,200원(환율) = 1,920,000원	10,000
장기연수	▸ - ・	
해외석학초빙	▸ - ・	
기타국제화활동	▸국제(CRYPTO2021 학회 참석, 미국 2021.08.) -항공료 및 체재비 ・항공료 : 2,350,667원 x 3명 x 1회 = 7,052,000원 ・체재비(일비) : $30 x 3명 x 7일 x 1,200원(환율) = 756,000원 ・체재비(숙박) : $120 x 3명 x 7일 x 1,200원(환율) = 3,024,000원 ・체재비(일비) : $80 x 3명 x 7일 x 1,200원(환율) = 2,016,000원	12,848
합계		22,848

【작성방법】

1) 대학원생의 장・단기 해외연수와 같이 대학원생이 주체가 되어 참여하는 국제협력 프로그램 및 기타 국제협력 활동에 대한 경비로 집행
2) 교수의 세미나 참석이 아닌, 대학원생이 국제학술대회 발표, 해외 연구자와의 공동세미나에 참석하는 경우에 대해 작성(참석 및 목적이 뚜렷하지 않은 단기 해외연수 지양)
3) 해외석학 초빙 경비의 경우 대학의 전문가 초청 기준에 따르며, 초빙 수당, 체재비 및 항공료 등 지원 항목별 세부적으로 기재

5) 교육연구단 운영비

(단위: 천원)

구분	산출근거	금액
교육연구단 전담직원 인건비	▸교육연구단 전임직원 - 행정직원 1인 · 3,500,000원 x 12개월 x 1인 x 50% = 21,000,000원	21,000
성과급	▸ - ·	
국내여비	▸ - ·	
학술활동지원비	▸ - ·	
산업재산권 출원등록비	▸특허 -국내특허 출원 1건 · 3,000,000원 x 1건 = 3,000,000원	3,000
일반수용비	▸사무용품비 -A4용지 · 30,000원 x 100박스 = 3,000,000원	3,000
회의 및 행사 개최비	▸ - ·	
각종 행사경비	▸교육단 전체 워크숍 2회 -장소 사용 및 부대경비 · 1,500,000원 x 2회 = 1,500,000원	3,000
기타	▸ - ·	
합 계		30,000

【작성방법】

1) 인건비: 교육연구단 소속 업무전담 직원 인건비

2) 성과급: 참여교수, 신진연구인력, 참여 대학원생 중 우수한 연구 성과 및 사업에 공헌도가 있는 자에 대한 성과급

▸ 교육연구단별 운영 기준에 따라 기여도 평가를 실시하여 기여도에 따라 성과급 배분

3) 국내여비: 대학 자체 여비 기준 적용

4) 학술활동지원비

▸ 논문게재료, 국내 학회 및 세미나 참가비(일회성), 전문가 초청 자문료, 도서 등 문헌 구입비, 국내·외 정보 수집비

▸ 학회 연회비 등 참여교수 개인에 대한 경비 및 학회 후원금 성격 지출 불가

5) 산업재산권출원등록비: 국내외 특허 출원 및 등록비

6) 일반수용비: 사무용품비, 인쇄비, 각종 수수료 및 사용료, 전화료 등

▸ 연구기자재 구입비 및 시설비, 상품권 등 선물 구입비 편성 불가

6) 교육과정 개발비

(단위: 천원)

산출근거	금액
▸온라인 강의 교재 개발 -정보보안 최신 기술 교재 4건 ・3,000,000원 x 4건 = 12,000,000원	12,000
▸ - .	
▸ - .	

【작성방법】

1) 교재개발비, 사례조사비 및 실험비 등 교육과정 개발 관련 제반 경비를 편성

7) 실험실습 및 산학협력활동 지원비

(단위: 천원)

산출근거	금액
▸산학협력 워크숍 3회 -전문가 강의료 ・300,000원 x 21인 = 5,400,000원 -강의장 대관료 ・5,000,000원 x 3회 = 15,000,000원	20,400
▸소모성 재료비 -암호 무선장비용 모듈 ・3,600,000원 x 1건 = 3,600,000원	3,600
▸ - .	

【작성방법】

1) 소모성 재료비 및 창업, 취업지도, 산업체와의 산학협력 공동활동 경비 편성(자문료, 강사료, 취・창업 관련 행사개최비 등)

※ 단, 기자재 및 장비 구매비 편성 불가

8) 간접비: 25,872천원

【작성방법】

1) 연간 사업비의 5% 이내

2) 과학기술원 소속 교육연구단(팀) : 연간 사업비의 2% 이내

▸ 한국과학기술원, 울산과학기술원, 광주과학기술원, 대구경북과학기술원

[3차년도]

1) 대학원생 연구장학금

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
석사과정생	15.4	700	12	129,360
박사과정생	5.6	1,300	12	87,360
박사수료생	3.5	1,000	12	42,000
합계	24.5	작성 불필요	작성 불필요	258,720

【작성방법】

1) 사업에 참여하는 교수 전체 지도학생 중 참여 요건을 충족하는 학생 70% 이내 범위에서 지원

※ '융합전공'으로 신청하는 경우 석사박사 수료생은 연구장학금을 지원할 수 없음

2) 통합과정생의 경우 2년 이내는 석사과정생, 2년 초과는 박사과정생으로 포함

3) 석사과정생 월 70만원, 박사과정생 월 130만원, 박사 수료생 월 100만원

2) 신진연구인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
박사후 과정생	1	3,000	12	36,000
계약교수	2	3,000	12	72,000
합계	3	작성 불필요	작성 불필요	108,000

【작성방법】

1) 박사후 과정생 및 계약교수는 월 300만원 기준으로 작성

3) 산학협력 전담인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
산학협력 전담인력	1	3,000	12	36,000

【작성방법】

1) 산학협력 전담인력 인건비는 주관대학 지급기준에 따라 작성

※ 단, 전임교원 인건비로는 편성 불가

4) 국제화 경비

(단위: 천원)

구분	산출근거	금액
단기연수	▸Univ. of Kentucky 단기 연수 세미나 - 항공료 및 체재비 ・항공료 : 2,240,000원 x 2명 x 1회 = 4,480,000원 ・체재비(일비) : $30 x 2명 x 10일 x 1,200원(환율) = 720,000원 ・체재비(숙박) : $120 x 2명 x 10일 x 1,200원(환율) = 2,880,000원 ・체재비(일비) : $80 x 2명 x 10일 x 1,200원(환율) = 1,920,000원	10,000
장기연수	▸ - ・	
해외석학초빙	▸ - ・	
기타국제화활동	▸국제(RSA2022 학회 참석, 미국.) -항공료 및 체재비 ・항공료 : 2,350,667원 x 3명 x 1회 = 7,052,000원 ・체재비(일비) : $30 x 3명 x 7일 x 1,200원(환율) = 756,000원 ・체재비(숙박) : $120 x 3명 x 7일 x 1,200원(환율) = 3,024,000원 ・체재비(일비) : $80 x 3명 x 7일 x 1,200원(환율) = 2,016,000원	12,848
합계		22,848

【작성방법】

1) 대학원생의 장・단기 해외연수와 같이 대학원생이 주체가 되어 참여하는 국제협력 프로그램 및 기타 국제협력 활동에 대한 경비로 집행
2) 교수의 세미나 참석이 아닌, 대학원생이 국제학술대회 발표, 해외 연구자와의 공동세미나에 참석하는 경우에 대해 작성(참석 및 목적이 뚜렷하지 않은 단기 해외연수 지양)
3) 해외석학 초빙 경비의 경우 대학의 전문가 초청 기준에 따르며, 초빙 수당, 체재비 및 항공료 등 지원 항목별 세부적으로 기재

5) 교육연구단 운영비

(단위: 천원)

구분	산출근거	금액
교육연구단 전담직원 인건비	▸교육연구단 전임직원 - 행정직원 1인 · 3,500,000원 x 12개월 x 1인 x 50% = 21,000,000원	21,000
성과급	▸ - ·	
국내여비	▸ - ·	
학술활동지원비	▸ - ·	
산업재산권 출원등록비	▸특허 -국내특허 출원 1건 · 3,000,000원 x 1건 = 3,000,000원	3,000
일반수용비	▸사무용품비 -A4용지 · 30,000원 x 100박스 = 3,000,000원	3,000
회의 및 행사 개최비	▸ - ·	
각종 행사경비	▸교육단 전체 워크숍 2회 -장소 사용 및 부대경비 · 1,500,000원 x 2회 = 1,500,000원	3,000
기타	▸ - ·	
합 계		30,000

【작성방법】

1) 인건비: 교육연구단 소속 업무전담 직원 인건비

2) 성과급: 참여교수, 신진연구인력, 참여 대학원생 중 우수한 연구 성과 및 사업에 공헌도가 있는 자에 대한 성과급

▸ 교육연구단별 운영 기준에 따라 기여도 평가를 실시하여 기여도에 따라 성과급 배분

3) 국내여비: 대학 자체 여비 기준 적용

4) 학술활동지원비

▸ 논문게재료, 국내 학회 및 세미나 참가비(일회성), 전문가 초청 자문료, 도서 등 문헌 구입비, 국내·외 정보 수집비

▸ 학회 연회비 등 참여교수 개인에 대한 경비 및 학회 후원금 성격 지출 불가

5) 산업재산권출원등록비: 국내외 특허 출원 및 등록비

6) 일반수용비: 사무용품비, 인쇄비, 각종 수수료 및 사용료, 전화료 등

▸ 연구기자재 구입비 및 시설비, 상품권 등 선물 구입비 편성 불가

6) 교육과정 개발비

(단위: 천원)

산출근거	금액
▸온라인 강의 교재 개발 -정보보안 최신 기술 교재 4건 ・3,000,000원 x 4건 = 12,000,000원	12,000
▸ - .	
▸ - .	

【작성방법】

1) 교재개발비, 사례조사비 및 실험비 등 교육과정 개발 관련 제반 경비를 편성

7) 실험실습 및 산학협력활동 지원비

(단위: 천원)

산출근거	금액
▸산학협력 워크숍 3회 -전문가 강의료 ・300,000원 x 21인 = 5,400,000원 -강의장 대관료 ・5,000,000원 x 3회 = 15,000,000원	20,400
▸소모성 재료비 -암호 평가용 모듈 ・3,600,000원 x 1건 = 3,600,000원	3,600
▸ - .	

【작성방법】

1) 소모성 재료비 및 창업, 취업지도, 산업체와의 산학협력 공동활동 경비 편성(자문료, 강사료, 취・창업 관련 행사개최비 등)

※ 단, 기자재 및 장비 구매비 편성 불가

8) 간접비: 25,872천원

【작성방법】

1) 연간 사업비의 5% 이내

2) 과학기술원 소속 교육연구단(팀) : 연간 사업비의 2% 이내

▸ 한국과학기술원, 울산과학기술원, 광주과학기술원, 대구경북과학기술원

[4차년도]

1) 대학원생 연구장학금

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
석사과정생	15.4	700	12	129,360
박사과정생	5.6	1,300	12	87,360
박사수료생	3.5	1,000	12	42,000
합계	24.5	작성 불필요	작성 불필요	258,720

【작성방법】

1) 사업에 참여하는 교수 전체 지도학생 중 참여 요건을 충족하는 학생 70% 이내 범위에서 지원

※ '융합전공'으로 신청하는 경우 석사박사 수료생은 연구장학금을 지원할 수 없음

2) 통합과정생의 경우 2년 이내는 석사과정생, 2년 초과는 박사과정생으로 포함

3) 석사과정생 월 70만원, 박사과정생 월 130만원, 박사 수료생 월 100만원

2) 신진연구인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
박사후 과정생	1	3,000	12	36,000
계약교수	2	3,000	12	72,000
합계	3	작성 불필요	작성 불필요	108,000

【작성방법】

1) 박사후 과정생 및 계약교수는 월 300만원 기준으로 작성

3) 산학협력 전담인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
산학협력 전담인력	1	3,000	12	36,000

【작성방법】

1) 산학협력 전담인력 인건비는 주관대학 지급기준에 따라 작성

※ 단, 전임교원 인건비로는 편성 불가

4) 국제화 경비

(단위: 천원)

구분	산출근거	금액
단기연수	▸Univ. of Florida FICS 단기 연수 세미나 - 항공료 및 체재비 ・항공료 : 2,240,000원 x 2명 x 1회 = 4,480,000원 ・체재비(일비) : $30 x 2명 x 10일 x 1,200원(환율) = 720,000원 ・체재비(숙박) : $120 x 2명 x 10일 x 1,200원(환율) = 2,880,000원 ・체재비(일비) : $80 x 2명 x 10일 x 1,200원(환율) = 1,920,000원	10,000
장기연수	▸ - ・	
해외석학초빙	▸ - ・	
기타국제화활동	▸국제(ASIACRYPTO2023 학회 참석) -항공료 및 체재비 ・항공료 : 2,350,667원 x 3명 x 1회 = 7,052,000원 ・체재비(일비) : $30 x 3명 x 7일 x 1,200원(환율) = 756,000원 ・체재비(숙박) : $120 x 3명 x 7일 x 1,200원(환율) = 3,024,000원 ・체재비(일비) : $80 x 3명 x 7일 x 1,200원(환율) = 2,016,000원	12,848
합계		22,848

【작성방법】

1) 대학원생의 장・단기 해외연수와 같이 대학원생이 주체가 되어 참여하는 국제협력 프로그램 및 기타 국제협력 활동에 대한 경비로 집행
2) 교수의 세미나 참석이 아닌, 대학원생이 국제학술대회 발표, 해외 연구자와의 공동세미나에 참석하는 경우에 대해 작성(참석 및 목적이 뚜렷하지 않은 단기 해외연수 지양)
3) 해외석학 초빙 경비의 경우 대학의 전문가 초청 기준에 따르며, 초빙 수당, 체재비 및 항공료 등 지원 항목별 세부적으로 기재

5) 교육연구단 운영비

(단위: 천원)

구분	산출근거	금액
교육연구단 전담직원 인건비	▸교육연구단 전임직원 - 행정직원 1인 · 3,500,000원 x 12개월 x 1인 x 50% = 21,000,000원	21,000
성과급	▸ - ·	
국내여비	▸ - ·	
학술활동지원비	▸ - ·	
산업재산권 출원등록비	▸특허 -국내특허 출원 1건 · 3,000,000원 x 1건 = 3,000,000원	3,000
일반수용비	▸사무용품비 -A4용지 · 30,000원 x 100박스 = 3,000,000원	3,000
회의 및 행사 개최비	▸ - ·	
각종 행사경비	▸교육단 전체 워크숍 2회 -장소 사용 및 부대경비 · 1,500,000원 x 2회 = 1,500,000원	3,000
기타	▸ - ·	
합 계		30,000

【작성방법】

1) 인건비: 교육연구단 소속 업무전담 직원 인건비

2) 성과급: 참여교수, 신진연구인력, 참여 대학원생 중 우수한 연구 성과 및 사업에 공헌도가 있는 자에 대한 성과급

▸ 교육연구단별 운영 기준에 따라 기여도 평가를 실시하여 기여도에 따라 성과급 배분

3) 국내여비: 대학 자체 여비 기준 적용

4) 학술활동지원비

▸ 논문게재료, 국내 학회 및 세미나 참가비(일회성), 전문가 초청 자문료, 도서 등 문헌 구입비, 국내·외 정보 수집비

▸ 학회 연회비 등 참여교수 개인에 대한 경비 및 학회 후원금 성격 지출 불가

5) 산업재산권출원등록비: 국내외 특허 출원 및 등록비

6) 일반수용비: 사무용품비, 인쇄비, 각종 수수료 및 사용료, 전화료 등

▸ 연구기자재 구입비 및 시설비, 상품권 등 선물 구입비 편성 불가

6) 교육과정 개발비

(단위: 천원)

산출근거	금액
▸온라인 강의 교재 개발 -정보보안 최신 기술 교재 4건 ・3,000,000원 x 4건 = 12,000,000원	12,000
▸ - .	
▸ - .	

【작성방법】

1) 교재개발비, 사례조사비 및 실험비 등 교육과정 개발 관련 제반 경비를 편성

7) 실험실습 및 산학협력활동 지원비

(단위: 천원)

산출근거	금액
▸산학협력 워크숍 3회 -전문가 강의료 ・300,000원 x 21인 = 5,400,000원 -강의장 대관료 ・5,000,000원 x 3회 = 15,000,000원	20,400
▸소모성 재료비 -양자내성 암호 개발 모듈 ・3,600,000원 x 1건 = 3,600,000원	3,600
▸ - .	

【작성방법】

1) 소모성 재료비 및 창업, 취업지도, 산업체와의 산학협력 공동활동 경비 편성(자문료, 강사료, 취・창업 관련 행사개최비 등)

※ 단, 기자재 및 장비 구매비 편성 불가

8) 간접비: 25,872천원

【작성방법】

1) 연간 사업비의 5% 이내

2) 과학기술원 소속 교육연구단(팀) : 연간 사업비의 2% 이내

▸ 한국과학기술원, 울산과학기술원, 광주과학기술원, 대구경북과학기술원

[5차년도]

1) 대학원생 연구장학금

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
석사과정생	15.4	700	12	129,360
박사과정생	5.6	1,300	12	87,360
박사수료생	3.5	1,000	12	42,000
합계	24.5	작성 불필요	작성 불필요	258,720

【작성방법】

1) 사업에 참여하는 교수 전체 지도학생 중 참여 요건을 충족하는 학생 70% 이내 범위에서 지원

※ '융합전공'으로 신청하는 경우 석사박사 수료생은 연구장학금을 지원할 수 없음

2) 통합과정생의 경우 2년 이내는 석사과정생, 2년 초과는 박사과정생으로 포함

3) 석사과정생 월 70만원, 박사과정생 월 130만원, 박사 수료생 월 100만원

2) 신진연구인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
박사후 과정생	1	3,000	12	36,000
계약교수	2	3,000	12	72,000
합계	3	작성 불필요	작성 불필요	108,000

【작성방법】

1) 박사후 과정생 및 계약교수는 월 300만원 기준으로 작성

3) 산학협력 전담인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
산학협력 전담인력	1	3,000	12	36,000

【작성방법】

1) 산학협력 전담인력 인건비는 주관대학 지급기준에 따라 작성

※ 단, 전임교원 인건비로는 편성 불가

4) 국제화 경비

(단위: 천원)

구분	산출근거	금액
단기연수	▸Univ. of Florida FICS 단기 연수 세미나 - 항공료 및 체재비 ・항공료 : 2,240,000원 x 2명 x 1회 = 4,480,000원 ・체재비(일비) : $30 x 2명 x 10일 x 1,200원(환율) = 720,000원 ・체재비(숙박) : $120 x 2명 x 10일 x 1,200원(환율) = 2,880,000원 ・체재비(일비) : $80 x 2명 x 10일 x 1,200원(환율) = 1,920,000원	10,000
장기연수	▸ - ・	
해외석학초빙	▸ - ・	
기타국제화활동	▸국제(CHES2024 학회 참석) -항공료 및 체재비 ・항공료 : 2,350,667원 x 3명 x 1회 = 7,052,000원 ・체재비(일비) : $30 x 3명 x 7일 x 1,200원(환율) = 756,000원 ・체재비(숙박) : $120 x 3명 x 7일 x 1,200원(환율) = 3,024,000원 ・체재비(일비) : $80 x 3명 x 7일 x 1,200원(환율) = 2,016,000원	12,848
합계		22,848

【작성방법】

1) 대학원생의 장・단기 해외연수와 같이 대학원생이 주체가 되어 참여하는 국제협력 프로그램 및 기타 국제협력 활동에 대한 경비로 집행
2) 교수의 세미나 참석이 아닌, 대학원생이 국제학술대회 발표, 해외 연구자와의 공동세미나에 참석하는 경우에 대해 작성(참석 및 목적이 뚜렷하지 않은 단기 해외연수 지양)
3) 해외석학 초빙 경비의 경우 대학의 전문가 초청 기준에 따르며, 초빙 수당, 체재비 및 항공료 등 지원 항목별 세부적으로 기재

5) 교육연구단 운영비

(단위: 천원)

구분	산출근거	금액
교육연구단 전담직원 인건비	▸교육연구단 전임직원 - 행정직원 1인 · 3,500,000원 x 12개월 x 1인 x 50% = 21,000,000원	21,000
성과급	▸ - ·	
국내여비	▸ - ·	
학술활동지원비	▸ - ·	
산업재산권 출원등록비	▸특허 -국내특허 출원 1건 · 3,000,000원 x 1건 = 3,000,000원	3,000
일반수용비	▸사무용품비 -A4용지 · 30,000원 x 100박스 = 3,000,000원	3,000
회의 및 행사 개최비	▸ - ·	
각종 행사경비	▸교육단 전체 워크숍 2회 -장소 사용 및 부대경비 · 1,500,000원 x 2회 = 1,500,000원	3,000
기타	▸ - ·	
합 계		30,000

【작성방법】

1) 인건비: 교육연구단 소속 업무전담 직원 인건비

2) 성과급: 참여교수, 신진연구인력, 참여 대학원생 중 우수한 연구 성과 및 사업에 공헌도가 있는 자에 대한 성과급

▸ 교육연구단별 운영 기준에 따라 기여도 평가를 실시하여 기여도에 따라 성과급 배분

3) 국내여비: 대학 자체 여비 기준 적용

4) 학술활동지원비

▸ 논문게재료, 국내 학회 및 세미나 참가비(일회성), 전문가 초청 자문료, 도서 등 문헌 구입비, 국내·외 정보 수집비

▸ 학회 연회비 등 참여교수 개인에 대한 경비 및 학회 후원금 성격 지출 불가

5) 산업재산권출원등록비: 국내외 특허 출원 및 등록비

6) 일반수용비: 사무용품비, 인쇄비, 각종 수수료 및 사용료, 전화료 등

▸ 연구기자재 구입비 및 시설비, 상품권 등 선물 구입비 편성 불가

6) 교육과정 개발비

(단위: 천원)

산출근거	금액
▸온라인 강의 교재 개발 -정보보안 최신 기술 교재 4건 ・3,000,000원 x 4건 = 12,000,000원	12,000
▸ - .	
▸ - .	

【작성방법】

1) 교재개발비, 사례조사비 및 실험비 등 교육과정 개발 관련 제반 경비를 편성

7) 실험실습 및 산학협력활동 지원비

(단위: 천원)

산출근거	금액
▸산학협력 워크숍 3회 -전문가 강의료 ・300,000원 x 21인 = 5,400,000원 -강의장 대관료 ・5,000,000원 x 3회 = 15,000,000원	20,400
▸소모성 재료비 -양자암호통신용 개발 모듈 ・3,600,000원 x 1건 = 3,600,000원	3,600
▸ - .	

【작성방법】

1) 소모성 재료비 및 창업, 취업지도, 산업체와의 산학협력 공동활동 경비 편성(자문료, 강사료, 취・창업 관련 행사개최비 등)

※ 단, 기자재 및 장비 구매비 편성 불가

8) 간접비: 25,872천원

【작성방법】

1) 연간 사업비의 5% 이내

2) 과학기술원 소속 교육연구단(팀) : 연간 사업비의 2% 이내

▸ 한국과학기술원, 울산과학기술원, 광주과학기술원, 대구경북과학기술원

[6차년도]

1) 대학원생 연구장학금

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
석사과정생	15.4	700	12	129,360
박사과정생	5.6	1,300	12	87,360
박사수료생	3.5	1,000	12	42,000
합계	24.5	작성 불필요	작성 불필요	258,720

【작성방법】

1) 사업에 참여하는 교수 전체 지도학생 중 참여 요건을 충족하는 학생 70% 이내 범위에서 지원

※ '융합전공'으로 신청하는 경우 석사박사 수료생은 연구장학금을 지원할 수 없음

2) 통합과정생의 경우 2년 이내는 석사과정생, 2년 초과는 박사과정생으로 포함

3) 석사과정생 월 70만원, 박사과정생 월 130만원, 박사 수료생 월 100만원

2) 신진연구인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
박사후 과정생	1	3,000	12	36,000
계약교수	2	3,000	12	72,000
합계	3	작성 불필요	작성 불필요	108,000

【작성방법】

1) 박사후 과정생 및 계약교수는 월 300만원 기준으로 작성

3) 산학협력 전담인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
산학협력 전담인력	1	3,000	12	36,000

【작성방법】

1) 산학협력 전담인력 인건비는 주관대학 지급기준에 따라 작성

※ 단, 전임교원 인건비로는 편성 불가

4) 국제화 경비

(단위: 천원)

구분	산출근거	금액
단기연수	▸Univ. of Florida FICS 단기 연수 세미나 - 항공료 및 체재비 ・항공료 : 2,240,000원 x 2명 x 1회 = 4,480,000원 ・체재비(일비) : $30 x 2명 x 10일 x 1,200원(환율) = 720,000원 ・체재비(숙박) : $120 x 2명 x 10일 x 1,200원(환율) = 2,880,000원 ・체재비(일비) : $80 x 2명 x 10일 x 1,200원(환율) = 1,920,000원	10,000
장기연수	▸ - ・	
해외석학초빙	▸ - ・	
기타국제화활동	▸국제(PKC2025 학회 참석) -항공료 및 체재비 ・항공료 : 2,350,667원 x 3명 x 1회 = 7,052,000원 ・체재비(일비) : $30 x 3명 x 7일 x 1,200원(환율) = 756,000원 ・체재비(숙박) : $120 x 3명 x 7일 x 1,200원(환율) = 3,024,000원 ・체재비(일비) : $80 x 3명 x 7일 x 1,200원(환율) = 2,016,000원	12,848
합계		22,848

【작성방법】

1) 대학원생의 장・단기 해외연수와 같이 대학원생이 주체가 되어 참여하는 국제협력 프로그램 및 기타 국제협력 활동에 대한 경비로 집행
2) 교수의 세미나 참석이 아닌, 대학원생이 국제학술대회 발표, 해외 연구자와의 공동세미나에 참석하는 경우에 대해 작성(참석 및 목적이 뚜렷하지 않은 단기 해외연수 지양)
3) 해외석학 초빙 경비의 경우 대학의 전문가 초청 기준에 따르며, 초빙 수당, 체재비 및 항공료 등 지원 항목별 세부적으로 기재

5) 교육연구단 운영비

(단위: 천원)

구분	산출근거	금액
교육연구단 전담직원 인건비	▸교육연구단 전임직원 - 행정직원 1인 · 3,500,000원 x 12개월 x 1인 x 50% = 21,000,000원	21,000
성과급	▸ - ·	
국내여비	▸ - ·	
학술활동지원비	▸ - ·	
산업재산권 출원등록비	▸특허 -국내특허 출원 1건 · 3,000,000원 x 1건 = 3,000,000원	3,000
일반수용비	▸사무용품비 -A4용지 · 30,000원 x 100박스 = 3,000,000원	3,000
회의 및 행사 개최비	▸ - ·	
각종 행사경비	▸교육단 전체 워크숍 2회 -장소 사용 및 부대경비 · 1,500,000원 x 2회 = 1,500,000원	3,000
기타	▸ - ·	
합 계		30,000

【작성방법】

1) 인건비: 교육연구단 소속 업무전담 직원 인건비

2) 성과급: 참여교수, 신진연구인력, 참여 대학원생 중 우수한 연구 성과 및 사업에 공헌도가 있는 자에 대한 성과급

▸ 교육연구단별 운영 기준에 따라 기여도 평가를 실시하여 기여도에 따라 성과급 배분

3) 국내여비: 대학 자체 여비 기준 적용

4) 학술활동지원비

▸ 논문게재료, 국내 학회 및 세미나 참가비(일회성), 전문가 초청 자문료, 도서 등 문헌 구입비, 국내·외 정보 수집비

▸ 학회 연회비 등 참여교수 개인에 대한 경비 및 학회 후원금 성격 지출 불가

5) 산업재산권출원등록비: 국내외 특허 출원 및 등록비

6) 일반수용비: 사무용품비, 인쇄비, 각종 수수료 및 사용료, 전화료 등

▸ 연구기자재 구입비 및 시설비, 상품권 등 선물 구입비 편성 불가

6) 교육과정 개발비

(단위: 천원)

산출근거	금액
▸온라인 강의 교재 개발 -정보보안 최신 기술 교재 4건 ・3,000,000원 x 4건 = 12,000,000원	12,000
▸ - .	
▸ - .	

【작성방법】

1) 교재개발비, 사례조사비 및 실험비 등 교육과정 개발 관련 제반 경비를 편성

7) 실험실습 및 산학협력활동 지원비

(단위: 천원)

산출근거	금액
▸산학협력 워크숍 3회 -전문가 강의료 ・300,000원 x 21인 = 5,400,000원 -강의장 대관료 ・5,000,000원 x 3회 = 15,000,000원	20,400
▸소모성 재료비 -5G 암호 개발 모듈 ・3,600,000원 x 1건 = 3,600,000원	3,600
▸ - .	

【작성방법】

1) 소모성 재료비 및 창업, 취업지도, 산업체와의 산학협력 공동활동 경비 편성(자문료, 강사료, 취・창업 관련 행사개최비 등)

※ 단, 기자재 및 장비 구매비 편성 불가

8) 간접비: 25,872천원

【작성방법】

1) 연간 사업비의 5% 이내

2) 과학기술원 소속 교육연구단(팀) : 연간 사업비의 2% 이내

▸ 한국과학기술원, 울산과학기술원, 광주과학기술원, 대구경북과학기술원

[7차년도]

1) 대학원생 연구장학금

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
석사과정생	15.4	700	12	129,360
박사과정생	5.6	1,300	12	87,360
박사수료생	3.5	1,000	12	42,000
합계	24.5	작성 불필요	작성 불필요	258,720

【작성방법】

1) 사업에 참여하는 교수 전체 지도학생 중 참여 요건을 충족하는 학생 70% 이내 범위에서 지원

※ '융합전공'으로 신청하는 경우 석사박사 수료생은 연구장학금을 지원할 수 없음

2) 통합과정생의 경우 2년 이내는 석사과정생, 2년 초과는 박사과정생으로 포함

3) 석사과정생 월 70만원, 박사과정생 월 130만원, 박사 수료생 월 100만원

2) 신진연구인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
박사후 과정생	1	3,000	12	36,000
계약교수	2	3,000	12	72,000
합계	3	작성 불필요	작성 불필요	108,000

【작성방법】

1) 박사후 과정생 및 계약교수는 월 300만원 기준으로 작성

3) 산학협력 전담인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
산학협력 전담인력	1	3,000	12	36,000

【작성방법】

1) 산학협력 전담인력 인건비는 주관대학 지급기준에 따라 작성

※ 단, 전임교원 인건비로는 편성 불가

4) 국제화 경비

(단위: 천원)

구분	산출근거	금액
단기연수	▸Univ. of Florida FICS 단기 연수 세미나 - 항공료 및 체재비 ・항공료 : 2,240,000원 x 2명 x 1회 = 4,480,000원 ・체재비(일비) : $30 x 2명 x 10일 x 1,200원(환율) = 720,000원 ・체재비(숙박) : $120 x 2명 x 10일 x 1,200원(환율) = 2,880,000원 ・체재비(일비) : $80 x 2명 x 10일 x 1,200원(환율) = 1,920,000원	10,000
장기연수	▸ - ・	
해외석학초빙	▸ - ・	
기타국제화활동	▸국제(RWC 학회 참석) -항공료 및 체재비 ・항공료 : 2,350,667원 x 3명 x 1회 = 7,052,000원 ・체재비(일비) : $30 x 3명 x 7일 x 1,200원(환율) = 756,000원 ・체재비(숙박) : $120 x 3명 x 7일 x 1,200원(환율) = 3,024,000원 ・체재비(일비) : $80 x 3명 x 7일 x 1,200원(환율) = 2,016,000원	12,848
합계		22,848

【작성방법】

1) 대학원생의 장・단기 해외연수와 같이 대학원생이 주체가 되어 참여하는 국제협력 프로그램 및 기타 국제협력 활동에 대한 경비로 집행
2) 교수의 세미나 참석이 아닌, 대학원생이 국제학술대회 발표, 해외 연구자와의 공동세미나에 참석하는 경우에 대해 작성(참석 및 목적이 뚜렷하지 않은 단기 해외연수 지양)
3) 해외석학 초빙 경비의 경우 대학의 전문가 초청 기준에 따르며, 초빙 수당, 체재비 및 항공료 등 지원 항목별 세부적으로 기재

5) 교육연구단 운영비

(단위: 천원)

구분	산출근거	금액
교육연구단 전담직원 인건비	▸교육연구단 전임직원 - 행정직원 1인 · 3,500,000원 x 12개월 x 1인 x 50% = 21,000,000원	21,000
성과급	▸ - ·	
국내여비	▸ - ·	
학술활동지원비	▸ - ·	
산업재산권 출원등록비	▸특허 -국내특허 출원 1건 · 3,000,000원 x 1건 = 3,000,000원	3,000
일반수용비	▸사무용품비 -A4용지 · 30,000원 x 100박스 = 3,000,000원	3,000
회의 및 행사 개최비	▸ - ·	
각종 행사경비	▸교육단 전체 워크숍 2회 -장소 사용 및 부대경비 · 1,500,000원 x 2회 = 1,500,000원	3,000
기타	▸ - ·	
합 계		30,000

【작성방법】

1) 인건비: 교육연구단 소속 업무전담 직원 인건비

2) 성과급: 참여교수, 신진연구인력, 참여 대학원생 중 우수한 연구 성과 및 사업에 공헌도가 있는 자에 대한 성과급

▸ 교육연구단별 운영 기준에 따라 기여도 평가를 실시하여 기여도에 따라 성과급 배분

3) 국내여비: 대학 자체 여비 기준 적용

4) 학술활동지원비

▸ 논문게재료, 국내 학회 및 세미나 참가비(일회성), 전문가 초청 자문료, 도서 등 문헌 구입비, 국내·외 정보 수집비

▸ 학회 연회비 등 참여교수 개인에 대한 경비 및 학회 후원금 성격 지출 불가

5) 산업재산권출원등록비: 국내외 특허 출원 및 등록비

6) 일반수용비: 사무용품비, 인쇄비, 각종 수수료 및 사용료, 전화료 등

▸ 연구기자재 구입비 및 시설비, 상품권 등 선물 구입비 편성 불가

6) 교육과정 개발비

(단위: 천원)

산출근거	금액
▸온라인 강의 교재 개발 -정보보안 최신 기술 교재 4건 ・3,000,000원 x 4건 = 12,000,000원	12,000
▸ - .	
▸ - .	

【작성방법】

1) 교재개발비, 사례조사비 및 실험비 등 교육과정 개발 관련 제반 경비를 편성

7) 실험실습 및 산학협력활동 지원비

(단위: 천원)

산출근거	금액
▸산학협력 워크숍 3회 -전문가 강의료 ・300,000원 x 21인 = 5,400,000원 -강의장 대관료 ・5,000,000원 x 3회 = 15,000,000원	20,400
▸소모성 재료비 -부채널 분석 개발 모듈 ・3,600,000원 x 1건 = 3,600,000원	3,600
▸ - .	

【작성방법】

1) 소모성 재료비 및 창업, 취업지도, 산업체와의 산학협력 공동활동 경비 편성(자문료, 강사료, 취・창업 관련 행사개최비 등)

※ 단, 기자재 및 장비 구매비 편성 불가

8) 간접비: 25,872천원

【작성방법】

1) 연간 사업비의 5% 이내

2) 과학기술원 소속 교육연구단(팀) : 연간 사업비의 2% 이내

▸ 한국과학기술원, 울산과학기술원, 광주과학기술원, 대구경북과학기술원

[8차년도]

1) 대학원생 연구장학금

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
석사과정생	15.4	700	12	129,360
박사과정생	5.6	1,300	12	87,360
박사수료생	3.5	1,000	12	42,000
합계	24.5	작성 불필요	작성 불필요	258,720

【작성방법】

1) 사업에 참여하는 교수 전체 지도학생 중 참여 요건을 충족하는 학생 70% 이내 범위에서 지원

※ '융합전공'으로 신청하는 경우 석사박사 수료생은 연구장학금을 지원할 수 없음

2) 통합과정생의 경우 2년 이내는 석사과정생, 2년 초과는 박사과정생으로 포함

3) 석사과정생 월 70만원, 박사과정생 월 130만원, 박사 수료생 월 100만원

2) 신진연구인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
박사후 과정생	1	3,000	12	36,000
계약교수	2	3,000	12	72,000
합계	3	작성 불필요	작성 불필요	108,000

【작성방법】

1) 박사후 과정생 및 계약교수는 월 300만원 기준으로 작성

3) 산학협력 전담인력 인건비

(단위: 천원)

구분	지원대상인원(A)	1인당 월지급액(B)	지급개월수(C)	산출액(A*B*C)
산학협력 전담인력	1	3,000	12	36,000

【작성방법】

1) 산학협력 전담인력 인건비는 주관대학 지급기준에 따라 작성

※ 단, 전임교원 인건비로는 편성 불가

4) 국제화 경비

(단위: 천원)

구분	산출근거	금액
단기연수	▸Univ. of Florida FICS 단기 연수 세미나 - 항공료 및 체재비 ・항공료 : 2,240,000원 x 2명 x 1회 = 4,480,000원 ・체재비(일비) : $30 x 2명 x 10일 x 1,200원(환율) = 720,000원 ・체재비(숙박) : $120 x 2명 x 10일 x 1,200원(환율) = 2,880,000원 ・체재비(일비) : $80 x 2명 x 10일 x 1,200원(환율) = 1,920,000원	10,000
장기연수	▸ - ・	
해외석학초빙	▸ - ・	
기타국제화활동	▸국제(FSE 학회 참석) -항공료 및 체재비 ・항공료 : 2,350,667원 x 3명 x 1회 = 7,052,000원 ・체재비(일비) : $30 x 3명 x 7일 x 1,200원(환율) = 756,000원 ・체재비(숙박) : $120 x 3명 x 7일 x 1,200원(환율) = 3,024,000원 ・체재비(일비) : $80 x 3명 x 7일 x 1,200원(환율) = 2,016,000원	12,848
합계		22,848

【작성방법】

1) 대학원생의 장・단기 해외연수와 같이 대학원생이 주체가 되어 참여하는 국제협력 프로그램 및 기타 국제협력 활동에 대한 경비로 집행
2) 교수의 세미나 참석이 아닌, 대학원생이 국제학술대회 발표, 해외 연구자와의 공동세미나에 참석하는 경우에 대해 작성(참석 및 목적이 뚜렷하지 않은 단기 해외연수 지양)
3) 해외석학 초빙 경비의 경우 대학의 전문가 초청 기준에 따르며, 초빙 수당, 체재비 및 항공료 등 지원 항목별 세부적으로 기재

5) 교육연구단 운영비

(단위: 천원)

구분	산출근거	금액
교육연구단 전담직원 인건비	▸교육연구단 전임직원 - 행정직원 1인 · 3,500,000원 x 12개월 x 1인 x 50% = 21,000,000원	21,000
성과급	▸ - ·	
국내여비	▸ - ·	
학술활동지원비	▸ - ·	
산업재산권 출원등록비	▸특허 -국내특허 출원 1건 · 3,000,000원 x 1건 = 3,000,000원	3,000
일반수용비	▸사무용품비 -A4용지 · 30,000원 x 100박스 = 3,000,000원	3,000
회의 및 행사 개최비	▸ - ·	
각종 행사경비	▸교육단 전체 워크숍 2회 -장소 사용 및 부대경비 · 1,500,000원 x 2회 = 1,500,000원	3,000
기타	▸ - ·	
합 계		30,000

【작성방법】

1) 인건비: 교육연구단 소속 업무전담 직원 인건비

2) 성과급: 참여교수, 신진연구인력, 참여 대학원생 중 우수한 연구 성과 및 사업에 공헌도가 있는 자에 대한 성과급

▸ 교육연구단별 운영 기준에 따라 기여도 평가를 실시하여 기여도에 따라 성과급 배분

3) 국내여비: 대학 자체 여비 기준 적용

4) 학술활동지원비

▸ 논문게재료, 국내 학회 및 세미나 참가비(일회성), 전문가 초청 자문료, 도서 등 문헌 구입비, 국내·외 정보 수집비

▸ 학회 연회비 등 참여교수 개인에 대한 경비 및 학회 후원금 성격 지출 불가

5) 산업재산권출원등록비: 국내외 특허 출원 및 등록비

6) 일반수용비: 사무용품비, 인쇄비, 각종 수수료 및 사용료, 전화료 등

▸ 연구기자재 구입비 및 시설비, 상품권 등 선물 구입비 편성 불가

6) 교육과정 개발비

(단위: 천원)

산출근거	금액
▸온라인 강의 교재 개발 -정보보안 최신 기술 교재 4건 ・3,000,000원 x 4건 = 12,000,000원	12,000
▸ - .	
▸ - .	

【작성방법】

1) 교재개발비, 사례조사비 및 실험비 등 교육과정 개발 관련 제반 경비를 편성

7) 실험실습 및 산학협력활동 지원비

(단위: 천원)

산출근거	금액
▸산학협력 워크숍 3회 -전문가 강의료 ・300,000원 x 21인 = 5,400,000원 -강의장 대관료 ・5,000,000원 x 3회 = 15,000,000원	20,400
▸소모성 재료비 -보안성 검증 평가용 개발 모듈 ・3,600,000원 x 1건 = 3,600,000원	3,600
▸ - .	

【작성방법】

1) 소모성 재료비 및 창업, 취업지도, 산업체와의 산학협력 공동활동 경비 편성(자문료, 강사료, 취・창업 관련 행사개최비 등)

※ 단, 기자재 및 장비 구매비 편성 불가

8) 간접비: 25,872천원

【작성방법】

1) 연간 사업비의 5% 이내

2) 과학기술원 소속 교육연구단(팀) : 연간 사업비의 2% 이내

▸ 한국과학기술원, 울산과학기술원, 광주과학기술원, 대구경북과학기술원

[첨부 1] 2020년도 신청학과 소속 전체 교수 현황

기준일	원소속		신청 학과명	성명		직급	연구자 등록번호	전공분야	세부전공분야	전임/ 겸임	참여요건 검증	신임/ 기존	이공계열/ 인문사회계열	임상/ 기초	외국인 /내국인	사업 참여 여부	비고
	대학명	학과명		한글	영문												
2020.05.15	국민대학교	정보보안암호수학과	금융정보보안학과	강주성	Ju-Sung Kang	교수	10127144	수학	확률과정론	겸임	X	기존	이공계열		내국인	참여	
2020.05.15	국민대학교	재무금융·회계학부	금융정보보안학과	권용재	YONGJAE KWON	부교수	10641553		사회과학	겸임	X	기존	인문사회계열		내국인	미참여	
2020.05.15	국민대학교	경영학부	금융정보보안학과	김도현	KIM, Dohyeon	교수	10076158	경영학	창업/벤처기업	겸임	X	기존	인문사회계열		내국인	미참여	
2020.05.15	국민대학교	정보보안암호수학과	금융정보보안학과	김동찬	Dong-Chan Kim	부교수	11579260	수학	암호론	겸임	X	기존	이공계열		내국인	참여	
2020.05.15	국민대학교	정보보안암호수학과	금융정보보안학과	김종성	Jongsung Kim	부교수	10182694	컴퓨터학	정보보호	겸임	X	기존	이공계열		내국인	참여	
2020.05.15	국민대학교	소프트웨어학부	금융정보보안학과	박수현	Soo Hyun Park	교수	10056675	컴퓨터학	컴퓨터학	겸임	X	기존	이공계열		내국인	참여	
2020.05.15	국민대학교	정보보안암호수학과	금융정보보안학과	서석충	SEO SEOGCHUNG	조교수	10875717	컴퓨터학	컴퓨터보안	겸임	X	신임	이공계열		내국인	참여	
2020.05.15	국민대학교	정보보안암호수학과	금융정보보안학과	염용진	Yeom Yongjin	교수	10090653	수학	해석학	겸임	X	기존	이공계열		내국인	참여	
2020.05.15	국민대학교	소프트웨어학부	금융정보보안학과	윤상민	Yoon Sang Min	부교수	10701285	컴퓨터학	인공지능	겸임	X	기존	이공계열		내국인	참여	
2020.05.15	국민대학교	정보보안암호수학과	금융정보보안학과	이옥연	Yi, Okyeon	교수	10056884	컴퓨터학	유무선통신보안	겸임	X	기존	이공계열		내국인	참여	
2020.05.15	국민대학교	소프트웨어학부	금융정보보안학과	최은미	Eunmi Choi	교수	10116354	컴퓨터학	컴퓨터학	겸임	X	기존	이공계열		내국인	참여	

기준일	원소속		신청 학과명	성명		직급	연구자 등록번호	전공분야	세부전공분야	전임/ 겸임	참여요건 검증	신임/ 기존	이공계열/ 인문사회계열	임상/ 기초	외국인 /내국인	사업 참여 여부	비고
	대학명	학과명		한글	영문												
2020.05.15	국민대학교	정보보안암호수학과	금융정보보안학과	한동국	Han, Dong-Guk	교수	10128486	수학	암호론	겸임	X	기존	이공계열		내국인	참여	

전체 교수 수	전체교수 수	12	기존 교수 수 (참여교수)	전체 교수 수	9	신임교수 수 (참여교수)	전체 교수 수	1
	전임 교수 수	0		전임 교수 수	0		전임 교수 수	0
	겸임 교수 수	12		겸임 교수 수	9		겸임 교수 수	1
전체 참여 교수 수	전체 교수 수	10	이공계열 교수 수 (참여교수)	전체 교수 수	10	인문사회계열 교수 수 (참여교수)	전체 교수 수	0
	전임 교수 수	0		신임 교수 수	1		신임 교수 수	0
	겸임 교수 수	10		기존 교수 수	9		기존 교수 수	0

신임교수 실적 포함 여부	기타 업적물(저서, 특허, 기술이전, 창업 실적) /연구비/ 교육역량 대표실적	신임교수 실적포함여부 : 예

[첨부 2] 2020년도 교육연구단 참여교수의 지도학생 현황

기준일	대학명	신청학과명	성 명		학번	생년 (YYYY)	외국인/ 내국인	자교/타교	지도교수 성명	임상/ 기초	학위과정		사업 참여 여부	비고
			한글	영문							과정	재학학기수		
2020.05.15	국민대학교	금융정보보안학과	권수진	Sujin Kwon	F2020002	1998	내국인	자교	염용진	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	강수진	Soojin Kang	F2020001	1994	내국인	자교	김종성	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	김기윤	Giyoon Kim	H2019351	1993	내국인	자교	김종성	해당없음	석박사통합	3학기	참여	
2020.05.15	국민대학교	금융정보보안학과	김소람	SO RAM KIM	X2018001	1991	내국인	자교	김종성	해당없음	박사	5학기	참여	
2020.05.15	국민대학교	금융정보보안학과	김예원	Yewon Kim	X2017501	1992	내국인	타교	염용진	해당없음	박사	6학기	참여	
2020.05.15	국민대학교	금융정보보안학과	김일주	IlJu Kim	F2019001	1993	내국인	자교	한동국	해당없음	석사	3학기	참여	
2020.05.15	국민대학교	금융정보보안학과	김한기	Hangi Kim	X2018002	1992	내국인	자교	김종성	해당없음	박사	5학기	참여	
2020.05.15	국민대학교	금융정보보안학과	김한준	Han-Jun Kim	F2017501	1987	내국인	타교	최은미	해당없음	석사	4학기	참여	
2020.05.15	국민대학교	금융정보보안학과	김현기	Hyunki Kim	X2018003	1992	내국인	자교	이옥연	해당없음	박사	4학기	참여	
2020.05.15	국민대학교	금융정보보안학과	델핀라즈	KESARI MARY DELPHIN RAJ	X2017015	1987	외국인	타교	박수현	해당없음	박사	5학기	참여	
2020.05.15	국민대학교	금융정보보안학과	문재근	JeaGeun Moon	X2018501	1990	내국인	타교	한동국	해당없음	박사	4학기	참여	
2020.05.15	국민대학교	금융정보보안학과	문환복	Hwan Bok	M2019067	1994	내국인	타교	윤상민	해당없음	석사	3학기	참여	

기준일	대학명	신청학과명	성 명		학번	생년 (YYYY)	외국인/ 내국인	자교/타 교	지도교수 성명	임상/ 기초	학위과정		사업 참여 여부	비고
			한글	영문							과정	재학학기수		
				Mun										
2020.05.15	국민대학교	금융정보보안학과	박명서	Myungseo Park	X2017007	1987	내국인	자교	김종성	해당없음	박사	7학기	참여	
2020.05.15	국민대학교	금융정보보안학과	박은후	Eunhu Park	F2018501	1993	내국인	자교	김종성	해당없음	석사	4학기	참여	
2020.05.15	국민대학교	금융정보보안학과	박한별	HanByeol Park	F2019002	1995	내국인	자교	한동국	해당없음	석사	3학기	참여	
2020.05.15	국민대학교	금융정보보안학과	박호중	Hojoong Park	X2017008	1989	내국인	자교	강주성	해당없음	박사	7학기	참여	
2020.05.15	국민대학교	금융정보보안학과	백상원	Sang Won Baek	M2020047	1991	내국인	자교	윤상민	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	백승준	Seungjun Baek	F2020003	1993	내국인	자교	김종성	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	성효은	Hyoeun Seong	F2019503	1993	내국인	자교	염용진	해당없음	석사	2학기	참여	
2020.05.15	국민대학교	금융정보보안학과	송진교	Jin-Kyo Song	F2020004	1993	내국인	자교	서석충	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	수간야	Suganya Selvaraj	X2016001	1988	외국인	타교	최은미	해당없음	박사	8학기	참여	
2020.05.15	국민대학교	금융정보보안학과	신수민	Sumin Shin	F2020005	1996	내국인	자교	김종성	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	안상우	Sang-Woo An	F2020019	1995	내국인	자교	서석충	해당없음	석사	1학기	참여	

기준일	대학명	신청학과명	성 명		학번	생년 (YYYY)	외국인/ 내국인	자교/타 교	지도교수 성명	임상/ 기초	학위과정		사업 참여 여부	비고
			한글	영문							과정	재학학기수		
2020.05.15	국민대학교	금융정보보안학과	염선호	Sun-Ho Yum	X2018502	1986	내국인	타교	박수현	해당없음	박사	4학기	참여	
2020.05.15	국민대학교	금융정보보안학과	오진혁	Jinhyeok Oh	F2019003	1995	내국인	자교	이옥연	해당없음	석사	3학기	참여	
2020.05.15	국민대학교	금융정보보안학과	위한샘	Hansaem Wi	X2018503	1991	내국인	자교	이옥연	해당없음	박사	4학기	참여	
2020.05.15	국민대학교	금융정보보안학과	윤병철	Byungchul Youn	F2019501	1993	내국인	자교	김종성	해당없음	석사	2학기	참여	
2020.05.15	국민대학교	금융정보보안학과	이세훈	Sehoon Lee	F2019004	1993	내국인	타교	김종성	해당없음	석사	3학기	참여	
2020.05.15	국민대학교	금융정보보안학과	이종혁	JongHyeok Lee	H2017351	1992	내국인	자교	한동국	해당없음	석박사통합	7학기	참여	
2020.05.15	국민대학교	금융정보보안학과	이태호	TaeHo Lee	F2020006	1995	내국인	자교	한동국	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	임성혁	SeongHyuck Lim	F2020007	1995	내국인	자교	한동국	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	임한섭	HanSeop Lim	F2019005	1994	내국인	자교	한동국	해당없음	석사	3학기	참여	
2020.05.15	국민대학교	금융정보보안학과	임형신	Hyoung Shin Yim	F2020008	1997	내국인	자교	염용진	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	장찬국	Chan-Guk Jang	X2018004	1991	내국인	자교	이옥연	해당없음	박사	5학기	참여	
2020.0	국민대학교	금융정보보안학과	전용진	Yongjin Jeon	F2018502	1995	내국인	자교	김종성	해당없음	석사	4학기	참여	

기준일	대학명	신청학과명	성 명		학번	생년 (YYYY)	외국인/ 내국인	자교/타 교	지도교수 성명	임상/ 기초	학위과정		사업 참여 여부	비고
			한글	영문							과정	재학학기수		
5.15														
2020.05.15	국민대학교	금융정보보안학과	정근호	Geun Ho Jung	M2020063	1992	내국인	타교	윤상민	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	조재형	Jaehyung Cho	X2017502	1987	내국인	자교	김종성	해당없음	박사	4학기	참여	
2020.05.15	국민대학교	금융정보보안학과	한재승	Jaeseung Han	F2020009	1995	내국인	자교	한동국	해당없음	석사	1학기	참여	
2020.05.15	국민대학교	금융정보보안학과	한주홍	Juhong Han	F2016006	1993	내국인	자교	이옥연	해당없음	석사	3학기	참여	
2020.05.15	국민대학교	금융정보보안학과	허욱	Uk Hur	F2019007	1993	내국인	타교	김종성	해당없음	석사	3학기	참여	

전체 대학원생 수 (명)	석사	25	참여 대학원생 수 (명)	석사	25	참여비율 (%)	석사	100.00
	박사	13		박사	13		박사	100.00
	석·박사통합	2		석·박사통합	2		석·박사통합	100.00
	계	40		계	40		전체	100.00
자교 학사 전체 대학원생 수 (명)	석사	20	자교 학사 참여 대학원생 수 (명)	석사	20	자교학사참여비율(%)	석사	100.00
	박사	8		박사	8		박사	100.00
	석·박사통합	2		석·박사통합	2		석·박사통합	100.00
	계	30		계	30		전체	100.00
외국인 전체 대학원생 수 (명)	석사	0	외국인 참여 대학원생 수 (명)	석사	0	외국인 참여비율 (%)	석사	-
	박사	2		박사	2		박사	100.00
	석·박사통합	0		석·박사통합	0		석·박사통합	-
	계	2		계	2		전체	100.00