보고서 표지

『4단계 BK21사업』 혁신인재양성사업(산업·사회 문제 해결분야)
- 교육연구단 성과평가 보고서

<table>
<tr><td>접수번호</td><td colspan="8">-</td></tr>
<tr><td>신청분야</td><td colspan="4">과학기술분야융복합</td><td>단위</td><td colspan="3">전국</td></tr>
<tr><td rowspan="4">학술연구분야
분류코드</td><td rowspan="2">구분</td><td colspan="2">관련분야</td><td colspan="2">관련분야</td><td colspan="3">관련분야</td></tr>
<tr><td>중분류</td><td>소분류</td><td>중분류</td><td>소분류</td><td>중분류</td><td colspan="2">소분류</td></tr>
<tr><td>분류명</td><td>컴퓨터학</td><td>정보보호</td><td>수학</td><td>응용수학</td><td>전자/정보통신공학</td><td colspan="2">정보통신</td></tr>
<tr><td>비중(%)</td><td colspan="2">50%</td><td colspan="2">30%</td><td colspan="3">20%</td></tr>
<tr><td rowspan="3">학과(부)/
협동과정/
융합전공/
학과(부)내
전공</td><td colspan="3" rowspan="3">금융정보보안학과
(협동과정)</td><td colspan="3">대학 간 연합 여부</td><td>x</td></tr>
<tr><td colspan="3">융합전공 여부</td><td>x</td></tr>
<tr><td colspan="3">협동과정 학과 여부</td><td>o</td></tr>
<tr><td>교육연구
단명</td><td colspan="8">국문) 안전한 초연결사회를 위한 문제해결형 정보보안 교육연구단</td></tr>
<tr><td></td><td colspan="8">영문) Institute of Information Security Education for Secure Hyperconnected Society</td></tr>
<tr><td rowspan="6">교육연구
단장</td><td colspan="2">소 속</td><td colspan="6">국민대학교 과학기술대학 정보보안암호수학과</td></tr>
<tr><td colspan="2">직 위</td><td colspan="6">교수</td></tr>
<tr><td rowspan="3">성명</td><td>국문</td><td colspan="2">이옥연</td><td>전화</td><td colspan="3" rowspan="3">XXXX</td></tr>
<tr><td></td><td colspan="2"></td><td>팩스</td></tr>
<tr><td>영문</td><td colspan="2">Yi, Okyeon</td><td>이동전화</td></tr>
<tr><td colspan="3"></td><td>E-mail</td><td colspan="3"></td></tr>
<tr><td rowspan="2">연차별
총 사업비
(백만원)</td><td colspan="2">구분</td><td>1차년도
('20.9~'21.2)</td><td>2차년도
('21.3~'22.2)</td><td>3차년도
('22.3~'23.2)</td><td colspan="3">4차년도
('23.3~'24.2)</td></tr>
<tr><td colspan="2">국고지원금</td><td>258.72</td><td>562.301</td><td>566.16</td><td colspan="3">700.783</td></tr>
<tr><td colspan="3">총 사업기간</td><td colspan="6">2020. 9. 1. ~ 2027. 8. 31. (84개월)</td></tr>
<tr><td colspan="3">평가 대상 기간</td><td colspan="6">2020. 9. 1. ~ 2024. 2. 29. (42개월)</td></tr>
</table>

본인은 『4단계 BK21』 사업 성과평가 보고서를 제출합니다. 아울러, 보고서에는 사실과 다른 내용이 포함되지 아니하였으며 만약 허위 사실이나 중대한 오류가 발견될 경우에는 그에 상응하는 불이익을 감수하겠음을 서약합니다.

2024년 05월 08일

작성자	교육연구단장	이 옥 연 (인)
확인자	국민대학교 산학협력단장	이 인 형 (인)
확인자	국민대학교 총장	정 승 렬 (인)

한국연구재단 이사장 귀하

<보고서 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
- AI 보안기술 기반 지능형 시스템과 사회 안전망 확보 기술 전문인력 양성

▶ 초연결사회의 정보보안을 선도하는 전문가 양성을 목표로 함
- 단계별 인력양성 프로그램 로드맵을 세워 추진중
- 정보보안 교육체계를 지속적으로 유지 및 개선하여 정보보안을 선도하는 전문가 양성에 힘쓰고 있음
- 교육연구단의 참여교수들은 교과과정 외에도 운영하는 랩을 통해 통신 보안, 디바이스 보안, 암호기술, AI 응용 분야에 다양한 기관 및 업체와의 협력 연구를 수행중
- 연구를 통해 얻은 연구성과는 국내외 학술대회와 논문지에 발표하였으며, 공모전 참여, 특허출원 등의 추가적인 성과를 내었음</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
- 교수진은 미래 초연결사회에 필수적으로 요구되는AI 보안, 무선통신 보안, 이동통신보안, 암호모듈 국가검증, 암호설계 및 분석, 디바이스 보안 등 5G/6G 초연결시대에 필수적인 다양한 정보보안 전공경험과 실무 경험을 모두 갖추고 있음
- 5G, 6G, IoT 기반의 지상망을 중심으로 위성, 수상통신, 수중통신에 이르는 공간통신의 모든 연결성 완성을 목표로 진행되는 초성능, 초대역, 초공간, 초정밀, 초지능, 초경험시대의 초신뢰 정보보안 전문인력 양성을 위한 교육역량을 갖춤
- 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
- 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 갖출 수 있도록 하는 교육프로그램을 보유함
- 연구소, 산업계의 전문가와 함께하는 교육과정 및 정보보안 실무과정을 운영하여 대외협력체계를 강화하고 우수 인재 양성에 힘쓰고 있음
- 실제 사회에 활용되는 데이터를 기반으로 스스로 학습하고 이해할 수 있는 다양한 인공지능 모델을 개발함과 동시에 시스템에 적용할 수 있는 역량을 갖추도록</td></tr>
</table>

	함 - 교육과정 편찬 추진 외에도 우수 인재 양성을 위해 보안강연 및 워크숍 등을 진행하고 있음 - 선정평가 당시 본 연구단에서 제안한 연구 역량 향상을 위한 대학원생 지원을 계획하였음
연구역량 영역	**▶ 다양한 정보보안 산업문제 해결 역량 보유한 연구진으로 구성** - 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 - 지속 가능한 발전을 선도하기 위해 본 연구단에서는 학부 및 대학원생에 대한 교육과 함께 다양한 연구를 진행하였음 **- 평가기간 내에 정부 160건, 산업체 22건 총 182건의 연구를 진행하였음** - 총 182건의 연구를 통해 243억에 해당하는 연구비를 수주해냈음 **- 이 외에도 국제 저널 120건, 국내 저널 65건, 국제 학회 57건, 국내 학회 220건, 특허(등록 38건, 출원 70건), 기술이전 32건 등 많은 연구 결과를 내었음**
향후 계획	- 교육연구단 단계기간(2025~2027)에서의 목표는 정보보안 대외협력체계 강화임 - 해당 목표를 위해 산업계의 전문가를 중심으로 한 정보보안 실무과정 운영, 재학생의 인턴 파견 추진을 계획중임 - 국내외 정보보안 IT 기업들과의 산학 네트워크를 구축하고 이를 토대로 한 유기적 산학협력 체계정착을 계획 중임 - 또한, 정보보안 기술개발과 커뮤니케이션의 활성화를 위한 보안기술 통합 테스트베드를 구축할 예정임 - 대외협력체계 강화를 위해 연구소, 산업계의 다양한 전문가와 함께 하는 교육과정 개설과 산업계의 정보보안 문제 해결을 위한 컨소시엄 구축을 계획하고 있음

목 차

4단계 BK21 사업

Ⅰ. 교육연구단의 구성, 비전 및 목표

I. 교육연구단 구성, 비전 및 목표

1. 교육연구단의 구성, 비전 및 목표

1.1 교육연구단의 필요성 및 기대효과

▶ 성과 평가기간(2020.09.01.~2024.02.29.)동안 다음과 같은 인력 배출 실적 달성

▣ 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 뒤쳐질경우, 글로벌 경쟁력 및 주도적 지위의 상실이 우려되어 기술 선점과 표준화 주도를 위한 전문인력 양성이 필요함.
- 본 연구단은 평가기간 내에 이동통신에서의 초연결에 필요한 경량 블록암호 PIPO를 제작하고, TTA 표준화에 성공하였음.
- 본 연구단은 평가기간 내에 유무선 통신 및 5G에서 6G에 이르는 보안 관련 기술의 표준화 분야 전문가들을 초청하여 워크숍 및 콜로키움 개최 등과 같이 특화된 교육 프로그램을 운영함.
- 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
- 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
- 본 연구단은 평가기간 내에 이동통신 및 IoT 보안 관련 연구결과를 국내외 학술지에 10건 이상 게재하여 국내 이동통신 연구 및 IoT 보안 연구 역량을 향상시킴
- 평가기간 내에 이동통신 보안 및 IoT 보안 분야의 전문인력 8명(현대오토에버, KT, 펜타시큐리티 등)을 배출함
- 미국 시장조사기관 가트너는 2023년도 IoT 장치는 97억 개 이상 설치돼있으며, 향후 2027년까지 선

진국 인구 50%가 AI 개인 비서를 갖게될 것을 예상함. 이에 따라 IoT 장치, 임베디드 장치부터 고성능 PC와 클라우드 서비스까지 모두 네트워크에 연결시켰을 때 생기는 다양한 사이버 공격에 대비하고자 하는 암호 기술 연구 및 체계적인 정보보안 시스템이 구성이 중요함

▶ 안전한 초연결사회를 위한 디바이스 보안 전문인력 양성

- 2011-2012년 영국의 보다폰이 이탈리아에서 백도어 발견 및 2020년 레딧에서 삼성 스마트폰에 치후360 설치, 타국 서버와 통신 논란이 생김에 따라, 백도어는 세계적 이슈가 되었음
- 국외에서는 부채널 정보 기반 디바이스 역공학 기술 연구가 활발히 진행되고 있지만, 국내에서의 관련 연구 및 인력 양성 프로그램은 충분하지 않기 때문에 해당 연구 및 전문인력 양성이 필요
- 본 연구단은 매년 부채널 분석 연구회를 개최하여 국내의 다양한 부채널 정보 분석 및 대응기술 관련 연구 결과 공유의 장을 만들어 국내에서의 부채널 정보 기반 기술의 발전에 기여함
- 평가기간 내에 부채널 정보 기반 디바이스 보안 분야의 전문인력 9명(국가보안기술연구소, LIG넥스원, 한국정보통신기술협회 등)을 배출함
- 최근 n번방 사건에서의 텔레그램 어플리케이션 분석 이슈 등 사회적으로 큰 파장을 일으킨 사건들의 수사를 위해서는 디지털 포렌식 전문가가 필수적임. 사회적 중요성을 뒷받침하듯, 2020년도 정부예산안에 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 분석 능력을 갖춘 전문가가 필요함
- 본 연구단은 평가기간 내에 디지털 포렌식 관련 연구 결과를 국제 학술지에 9건 이상 게재하여 국내 디지털 포렌식 연구 역량을 향상시킴
- 평가기간 내에 디지털 포렌식 기반 디바이스 보안 분야의 전문인력 4명(김앤장 법률사무소, 펜타시큐리티 등)을 배출함
- 2020년, 데이터 3법 개정안의 주요 내용에 따르면 개인정보보호, 보안의 중요성이 높아졌으며, 이에 따라, 동형암호를 포함한 차세대 암호 알고리즘들의 관심이 높아짐
- 동형암호를 포함한 차세대 암호 알고리즘은 낮은 성능 및 높은 메모리를 요구하는 단점이 있어서 암호 알고리즘에 대한 구현 최적화 연구가 필수적임. 그러나, 국외에 비해 국내의 소프트웨어 및 하드웨어 환경에서 암호 알고리즘을 고속 설계하는 전문가는 부족한 실정임
- 본 연구단은 평가기간 내에 구현 최적화 관련 연구 결과를 SCIE 급 국제 저널에 23건 이상 게재하여 국내 암호 구현 기술의 발전에 기여함
- 본 연구단은 평가기간내에 암호 알고리즘 구현 최적화 구현 분야의 전문인력 2명(LG U+, TTA)을 배출함

▶ 안전한 초연결사회를 위한 암호 전문인력 양성

- 오늘날 세계가 사용하는 DH 키공유 암호(1976년), RSA 공개키 암호(1977년), 타원곡선 암호(1985년)는 수학적 난제로 분류되는 인수분해 문제와 이산대수 문제를 기반으로 설계된 암호이며, 1994년 Peter Shor가 인수분해/이산대수 문제는 양자 컴퓨터를 통해 양자 알고리즘을 사용하면 다항식 시간 내에 풀 수 있음이 증명됨
- Global risk institute의 2023년도 보고서에 따르면 37명의 전문가 중 절반 이상은 향후 20년 이내에 현재의 공개키 암호를 무력화할 수준의 양자 컴퓨터 출현을 예상함
- 2016년부터 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)가 주관하여 국제 양자내성암호 표준 알고리즘 공모전이 진행 중이며 2022년도에 최종 PKE/KEM 1종과 전자서명 3종이 선정됐고 현재 알고리즘을 더 선정하기 위해 추가 라운드가 진행 중임

- 국내에서는 2022년부터 양자내성암호 국가공모전인 KpqC 공모전을 진행 중이며 2023년도에 2라운드 후보로 PKE/KEM 4종과 전자서명 4종이 선정되어 진행 중임
- 본 연구단은 코드 기반 양자내성암호 PALOMA를 개발하였고, 이는 한국 양자내성암호 연구단(이하 KpqC)이 주관하여 진행중인 KpqC 공모전 2라운드 암호로 선정됨
- 본 연구단은 그래프 기반 양자내성암호 IPCC7을 발표하고 이에 대한 안전성 분석을 진행하여 기존 양자내성암호와는 차별화된 암호화 방식을 제안함
- 현재 대부분의 양자내성암호 표준 후보 알고리즘은 구조가 복잡하여 구현 난이도가 매우 높고, 파라미터 설정 등 사용 방법이 다양하기 때문에 양자내성암호 알고리즘 관련 지식 습득이 필요함
- 본 연구단은 평가 대상 기간 내에 암호소프트웨어구현, 병렬암호구현 강의를 개설하여 암호 알고리즘의 고속 병렬 구현 방법 및 최신 동향, 기존 암호에의 적용 사례 등을 교육하였음
- 본 연구단은 평가 대상 기간 내에 화상회의 시스템의 키 교환 과정에서 양자내성암호를 적용한 키 캡슐화 매커니즘을 제안하여 양자내성암호의 응용 방향성을 제시함
- 따라서 기존 ICT 인프라의 보안체계를 양자컴퓨터에서도 안전한 양자내성암호 기반으로 교체하기 위한 장기간의 전문 인력양성 프로그램이 필요함
- 본 연구단은 평가 대상 기간 내에 정보보호프로토콜 강의를 개설하여 양자내성암호를 이해하기 위한 다양한 암호 알고리즘과 안전성 개념을 교육하여 학생들의 양자내성암호 관련 지식 및 연구 능력을 향상시킴
- 본 연구단은 양자내성암호 분야 인재 양성을 통해 KT, 현대자동차 등 양자내성암호로의 전환을 필요로 하는 기업으로 양질의 인적 자원을 배출하고 있음
- 본 연구단은 NIST에서 주관한 경량암호 공모전에서 선정된 Ascon에 대한 양자내성 평가를 진행하여 논문을 출판하고 있음. 현재, 대칭키 암호에 대한 양자내성 평가 경험을 바탕으로 새로운 대칭키 암호 제작을 착수하고 있음

▶ 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 요구됨더불어, 학습된 데이터를 활용할 수 있는 도메인이 제한적이기 때문에 다른 분야에의 적용 및 확산에 제한적임
- 미국, 중국 등 구글, 마이크로소프트, IBM, 샤오미, 바이두, 텐센트와 같은 글로벌 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
- 자율 성장 환경 취약점 발견 및 보안 기술을 통한 사회 지능형 시스템의 안정성 확보가 필요함. 또한,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
- 본 연구단은 평가기간 내에 디지털 포렌식 관련 연구 결과를 국제 학술지에 4건 이상 게재하여 국내 AI 보안 기술 연구 역량을 향상시킴
- 평가기간 내에 사회 지능형 시스템에 기여할 수 있는 전문인력 4명(중앙대학교 연구원, Bistos Co.Limited, 현대오토에버 등)을 배출함

1.2 교육연구단의 비전 및 목표 달성도

▶ 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

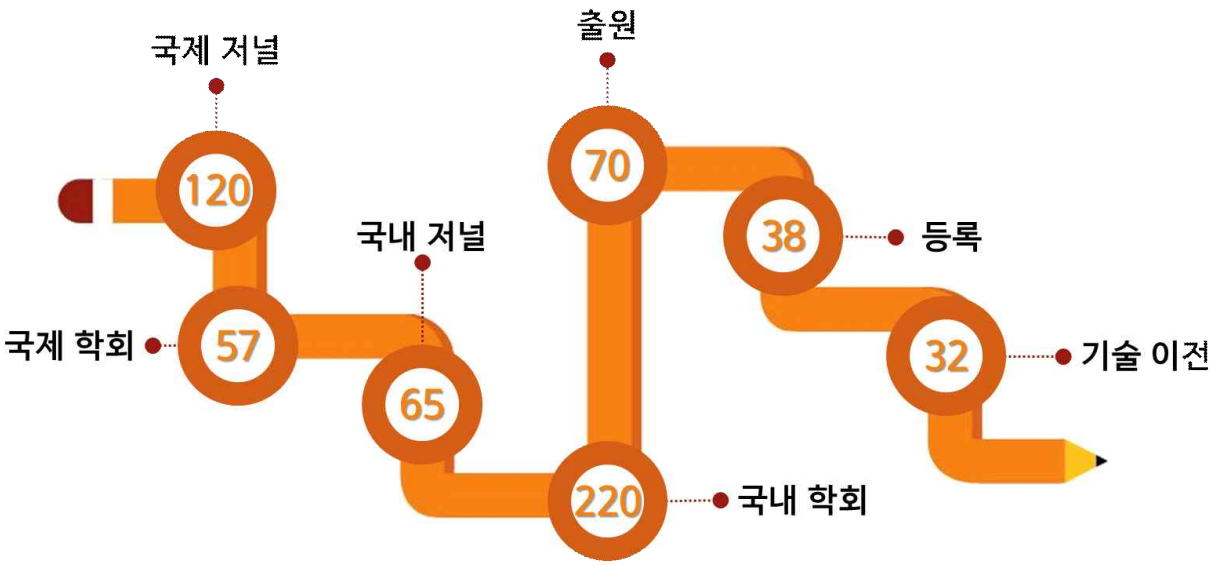
- 정보보안은 특성상 컴퓨터공학 및 암호 전공자의 융합 학문분야이며, 어느 한쪽의 전공지식만으로는 정보보안 위협을 이해하거나 대응할 수 없음
- 본 교육연구단은 정보보안전공 교수 8인과 컴퓨터공학 전공 교수 3인의 교수들로 구성되었으며, 중견교수 및 신진교수의 구성 비율이 적정하여, 경험과 도전정신을 모두 갖춘 구성임
- 또한, 단순 강의가 아닌 다양한 외부과제 및 정보보안 사례 기반 교육, 프로젝트 기반 교육 등 다양한 교육방법을 통해 교육하며, 강의평가가 매우 우수함
- 본 교육연구단을 구성하고 있는 교수진은 미래 초연결사회에 필수적으로 요구되는AI보안, 무선통신보안, 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 2월석사 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

▶ 성과 평가기간(2020.09.01.~2024.02.29.)동안 다음과 같은 연구 실적 달성



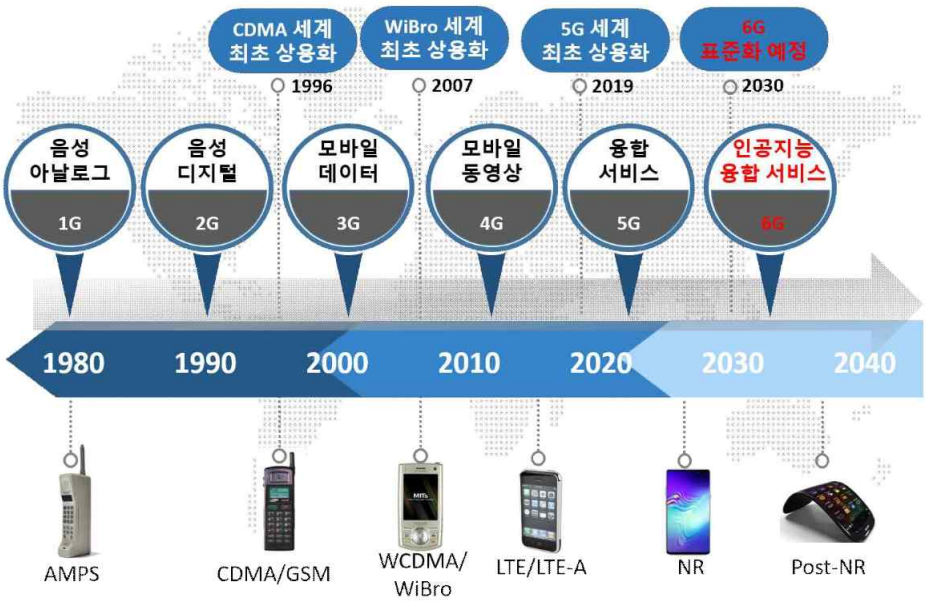
▣ 교육연구단의 교육목표

▶ 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
- 본 연구단은 평가기간 내에 국제 학술대회 MobiSec를 개최하여 이동통신환경에서의 다양한 정보보안 논문을 출판하여 5G 초연결사회의 문제에 대해 해결하는데 기여하였음
- 본 연구단은 평가기간 내에 5G 기술에 대한 안전성 측면에서의 연구를 통해 5건 이상의 국내외 학회에 논문을 투고하였음
- 본 연구단은 평가기간 내에 5G 기술과 IoT 기술을 위해 내 2개 대학(국민대학교, 순천향대학교), 해외 1개 대학(Georgia State University)의 2개 연구실로 총 3개 대학이 참여하는 국제 공동연구를 수행하였음
- ICT 환경의 지속적인 발전에 따라 미래의 IoT의 중심망이 될 이동통신망(5G/6G)과 위성통신 및 수중통신의 정보보안 문제를 해결 가능한 전문인력 양성을 목표로 함
- 본 연구단은 평가기간 내에 사물지능망특론 과목 개설을 통해 사물 인터넷 및 엣지 컴퓨팅 시스템을 설계 및 구현하는 아키텍처를 이해하고, 사물인터넷과 엣지 컴퓨팅 환경을 효과적으로 관리하는 방법에 대하여 지도하여 아키텍트가 IoT 및 엣지 컴퓨팅 프로젝트를 설계할 때 안전한 네트워크 아키텍처를 구축하고, 다양한 보안 위협으로부터 시스템을 보호하는 방법에 대하여 학습할 수 있도록 교육함
- 본 연구단은 평가기간 내에 수중 통신 및 극지 환경에서의 통신을 위한 연구 결과를 국내외 학술지에 5건 이상 게재하여 수중 통신 및 다양한 통신 환경 연구 역량을 향상시킴

- 본 연구단은 평가기간 내에 해안 어선 위험 수집 및 모니터링 플랫폼 설계와 관련한 연구를 통해 논문을 국제학회에 투고하고 Best Paper Award를 수상하였음
- 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 연구단은 평가기간 내에 사물지능망특론 과목 개설을 통해 사물 인터넷 및 엣지 컴퓨팅 시스템을 설계 및 구현하는 아키텍처를 이해하고, 사물인터넷과 엣지 컴퓨팅 환경을 효과적으로 관리하는 방법에 대하여 지도하여 아키텍트가 IoT 및 엣지 컴퓨팅 프로젝트를 설계할 때 안전한 네트워크 아키텍처를 구축하고, 다양한 보안 위협으로부터 시스템을 보호하는 방법에 대하여 학습할 수 있도록 교육함
- 본 연구단은 평가기간 내에 수중 통신 및 극지 환경에서의 통신을 위한 연구 결과를 국내외 학술지에 5건 이상 게재하여 수중 통신 및 다양한 통신 환경 연구 역량을 향상시킴
- 본 연구단은 평가기간 내에 해안 어선 위험 수집 및 모니터링 플랫폼 설계와 관련한 연구를 통해 논문을 국제학회에 투고하고 Best Paper Award를 수상하였음
- 본 교육연구단에서는 5G / 6G와 IoT를 수상통신, 위성통신, 수중통신 3차원 공간의 통신 환경을 모두 통합 분석능력을 갖춘 정보보안 전문가 양성을 목표로 함
- 본 연구단은 평가기간 내에 사물지능망특론 과목 개설을 통해 사물 인터넷 및 엣지 컴퓨팅 시스템을 설계 및 구현하는 아키텍처를 이해하고, 사물인터넷과 엣지 컴퓨팅 환경을 효과적으로 관리하는 방법에 대하여 지도하여 아키텍트가 IoT 및 엣지 컴퓨팅 프로젝트를 설계할 때 안전한 네트워크 아키텍처를 구축하고, 다양한 보안 위협으로부터 시스템을 보호하는 방법에 대하여 학습할 수 있도록 교육함
- 본 연구단은 평가기간 내에 수중 통신 및 극지 환경에서의 통신을 위한 연구 결과를 국내외 학술지에 5건 이상 게재하여 수중 통신 및 다양한 통신 환경 연구 역량을 향상시킴
- 본 연구단은 평가기간 내에 해안 어선 위험 수집 및 모니터링 플랫폼 설계와 관련한 연구를 통해 논문을 국제학회에 투고하고 Best Paper Award를 수상하였음

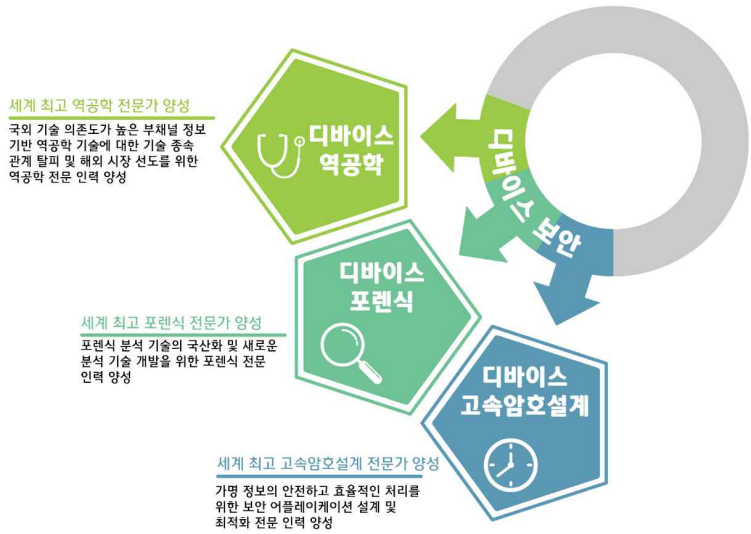


▶ 안전한 초연결사회를 위한 디바이스 보안 전문인력 양성

- 본 교육연구단은 안전한 초연결사회 구축에 필수적인 디바이스 보안 관련 부채널 분석, 디지털 포렌식, 고속구현 전문가 양성을 목표로 함
- 평가기간 내에 부채널공격론, 부채널공격대응론, 금융디바이스공격론 과목을 개설하여 초연결사회의 부채널 보안을 위해 실 기기에 대한 부채널 공격 및 대응을 교육하고 디바이스 부채널 보안 전문가를 양성함
- 평가기간 내에 디지털포렌식개론, 디지털포렌식특수연구 과목을 개설하여 디지털 포렌식 분석 기술 및 최신 기술을 통한 데이터 획득 방법을 교육하고 디지털 포렌식 전문가를 양성함
- 평가기간 내에 암호소프트웨어구현, 보안구현개발방법론, 금융키관리시스템 과목을 개설하여 디바이스 보안에 사용되는 암호 및 프로토콜의 안전성을 보장하면서도 효율적인 개발 방법을 교육하고 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 활성화 기여를 목표로 함
- 본 교육연구단은 매년 부채널 분석 워크숍을 개최하여 부채널 정보 분석 및 대응기술의 중요성을 알리고 학교, 연구소, 기업 간의 지식 공유의 장을 만들어 국내 산업 활성화에 기여함
- 부채널 정보 수집 기술, 분석 성능 향상을 위한 부채널 신호 처리 기술, 부채널 신호에 내재되어 있는 유의미한 정보 추출 기술 교육과 부채널 안전성 검증 시스템을 개선하는 전문인력 양성을 목표로 함
- 부채널공격론, 부채널공격대응론 등 관련 과목 개설 및 연구 지원을 통해 참여대학원생이 국제 하드웨어 보안 취약점 경진대회 HACK@SEC2020 3위, HACK@SEC2022 2위에 입상했으며, 관련 전문인력 9명을 관련 기관(국가보안기술연구소, LIG넥스원, 한국정보통신기술협회 등)에 배출함
- 날이 갈수록 다양해지는 디지털 기기의 방대한 데이터로부터 정확한 증거를 수집하여 객관적으로 증명 가능한 법정 제출용 디지털 증거를 수집 및 분석하는 방법과 정확한 원칙 및 절차를 교육하여 전문역량을 갖춘 디지털 포렌식 전문인력 양성을 목표로 함
- 디지털포렌식개론 과목 개설을 통해 참여대학원생이 디지털 포렌식, 안티 포렌식 기술에 대한 이해와 적절한 디지털 증거 수집 및 분석 방법을 교육함
- 다양한 디바이스가 가지는 각각의 특징 및 데이터에 대한 기본적인 이해를 돕기 위해 OS, 메모리, 저장공간 등의 전반적인 컴퓨터 이론 교육과 이스라엘 Cellebrite사의 UFED, 미국 Opentext의 EnCase, 국내 한컴위드의 MD-NEXT, MD-RED 등의 실사례 교육을 통해 분석이 불가능한 신규 기기나 새로운 프로그램에서 얻을 수 있는 데이터 분석 방법 연구 교육을 목표로 함
- 디지털포렌식특수연구 과목 개설을 통해 최신 디지털포렌식 기술 동향을 교육하고 Protonmail, 카카오톡 등의 실사례에 대한 분석 방법론을 교육함
- 평가기간 내에 참여대학원생의 디지털포렌식 연구 역량 발전을 통해 디지털포렌식 관련 연구결과를 국제 학술지에 9건 이상 게재함
- 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
- 동형암호 및 양자내성암호와 같은 차세대 암호 알고리즘은 낮은 성능 및 높은 메모리를 요구하므로 디바이스 고속 설계 기술 교육을 통하여 정보를 안전하고 효율적으로 처리할 수 있는 다양한 보안 어플리케이션을 설계하고 최적화할 수 있는 전문인력을 양성하는 것이 필요함
- 본 연구단은 평가기간 내에 구현 최적화 관련 연구 결과를 SCIE 급 국제 저널에 23건 이상 게재하여 국내 암호 구현 기술의 발전에 기여함
- 본 연구단은 평가기간 내에 암호 알고리즘 구현 최적화 분야의 전문인력을 양성하여 2명을 관련 기

관(LG U+, TTA)으로 배출함

- 동형 암호를 교육하기 위해서는 많은 교과목의 이해가 필수적이므로, 현대대수학 등 동형암호의 수학적인 원리에 대한 선수 과목과 양자내성암호에서도 다루어지는 Lattice 기반 동형 암호 등의 보안 방식에 대한 원리 또한 학습되어야 함
- 본 연구단은 평가기간 내에 암호소프트웨어구현, 보안구현개발방법론 과목을 개설하여 NIST 표준화 대상 양자내성암호에 대한 원리 및 최신 구현 연구결과들을 교육함
- 암호 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
- 본 연구단은 평가기간 내에 암호소프트웨어구현, 보안구현개발방법론, 병렬암호구현 과목을 개설하여 성능 및 메모리가 제한된 임베디드 환경, 고성능 병렬 환경에서의 암호 및 보안 구현 개발 방법을 교육함



▶ 양자내성암호 정보보안 전문인력 양성

- 본 교육연구단은 미래 정보통신 환경의 가장 큰 변화가 될 것으로 예상되는 양자내성암호 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 $h=\underbrace{g*g*\cdots*g}_{n}$ 주어졌을 때, n을 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 기술이므로 실용적 수준의 양자컴퓨터가 개발되면 현재 사용하는 모든 암호 체계의 안전성을 보장하지 못함
- Peter Shor의 논문이 발표되었을 때 학계에서는 양자 컴퓨팅의 실현성에 의구심을 가졌으나, 2010년 이후부터 양자 컴퓨팅의 괄목할만한 결과들이 소개되면서 학계의 지대한 관심을 받고 있으며, 2023년 Global risk institute의 보고서에 따르면 전문가의 50% 이상이 20년 이내에 현재의 암호 체계를 공격할 수 있는 양자 컴퓨터가 등장할 것이라고 주장함
- 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
- 2019년 구글의 53-qubit 양자 컴퓨터 Sycamore를 시작으로, 2020년 IBM의 65-qubit 양자 컴퓨터 Hummingbird, 2022년 IBM의 433-qubit 양자 컴퓨터 Osprey, 그리고 가장 최근에는 2023년 12월 IBM의 1121-qubit 양자컴퓨터 Condor가 제안되었음
- 미국 저명 컨설팅 회사인 맥킨지&컴퍼니는 2022년 68억 달러 수준 규모이던 세계 양자기술 시장이 2040년에는 최대 1060억 달러로 급성장할 것으로 예상하였음
- 암호 학계는 실용적 양자컴퓨터 시대를 대비하기 위해 양자내성암호(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 양자내성암호 표준 알고리즘 공모전이 진행 중이며, 2022년 4개의 후보 알고리즘이 선정된 이후 추가 선정을 위해 현재까지 추가 라운드를 진행 중
- 양자내성암호 기반 암호 체계의 조기 확보는 단기적으로는 보안방법 전환 비용을 감소시키며, 장기적으로는 국내 ICT 인프라 보안체계의 국외 의존도를 낮출 수 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
- 본 연구단은 평가 대상 기간 내에 보안기술표준분석및구현 강의를 개설하여 표준 암호 알고리즘 규격 및 구현 방법과 더불어 안전성 관점에서의 설계 사상 등을 주제로 교육하였음
- 본 연구단은 양자내성암호 기술의 내재화를 필요로 하는 기업들에게 Kyber, PALOMA 등 양자내성암호 알고리즘 구현 기술 이전을 진행함
- 본 연구단은 평가 대상 기간 내에 양자내성 부호 기반 암호에 대하여 정보 이론적 안전성 분석 및 정보 집합 공격 복잡도 확인과 같은 계산적 관점의 안전성 분석 연구를 통한 보안 파라미터를 제시함으로써 양자내성암호 분야의 전문인력을 배출하였음
- 기존 ICT 인프라의 보안체계를 양자컴퓨터에서도 안전한 양자내성암호 기반으로 교체를 하기 위해서는 장기간의 전문인력 양성 프로그램이 필요함
- 본 연구단은 평가 대상 기간 내에 공개키 암호 분석 이론 강의를 개설하여 Shor의 알고리즘 원리에 대해 교육하고, 공개키 암호의 안전성 개념을 지도함
- 본 연구단은 부호 기반 양자내성암호인 PALOMA를 개발하고 이는 한국 양자내성암호 연구단에서 주관하는 KpqC 공모전 2 라운드에 진출함
- 본 연구단은 기업체를 대상으로 양자내성암호 내재화를 위한 격자/부호 기반 암호의 필수 기반 지식 대해 강연을 진행하고 이에 대하여 주기적인 세미나를 진행함으로써 양자내성암호 분야의 전문인력을 양성함
- 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 기존 교육과정을 유력한 표준 양자내성암호(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
- 2022년 10월, 한국 양자내성암호 연구단이 양자내성암호 개발을 위한 공모전을 개최함. 이후 2023년 12월부터 8개의 후보 암호가 2라운드에 진입하였으며, 2024년 말에는 최종적으로 한국형 양자내성암호를 선정할 계획임.
- 2023년 7월, 국가정보원과 과학기술정보통신부가 행정안전부 등 관련 부처와 협력하여, KpqC 양자내성암호 공모전을 통해 선정된 암호체계로 국내 암호 시스템을 2035년까지 전환하기 위한 마스터플랜을 발표함.
- 본 교육연구단은 부호 기반의 양자내성암호 PALOMA을 개발하였으며, 이는 KpqC 양자내성내성암호 공모전의 2라운드 암호로 선정됨
- 따라서 본 교육연구단은 양자내성암호 중 부호 기반 알고리즘을 소개하는 교육을 실시하였으며, 전문인력 양성을 위해 PALOMA에 관한 연구를 진행하였음
- 이후 교육과 연구를 유지해 공개키 암호의 안전성 분석 교육을 바탕으로 PALOMA의 안전성 분석을 진행할 계획이며, 이는 안전성 요구 보안 수준에 맞춰 매개변수를 설정할 수 있는 전문인력 양성을 목표로 함

▶ 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 양성하여, 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 기술과 관련된 통신 시스템, 대용량 데이터 기반 AI 기술, 적대적 공격 및 방어와 관련된 교육체계를 수립을 위한 국제적 경쟁력을 갖춘 연구 수행 및 교육 기관들과의 협력 연구를 목표로 함
- 본 연구단은 평가기간 내에 사물지능망특론 과목 개설을 통해 사물 인터넷 및 엣지 컴퓨팅 시스템을 설계 및 구현하는 아키텍처를 이해하고, 사물인터넷과 엣지 컴퓨팅 환경을 효과적으로 관리하는 방법에 대하여 지도하여 아키텍트가 IoT 및 엣지 컴퓨팅 프로젝트를 설계할 때 안전한 네트워크 아키텍처를 구축하고, 다양한 보안 위협으로부터 시스템을 보호하는 방법에 대하여 학습할 수 있도록 교육함
- 본 연구단은 평가기간 내에 (해양수산부, 해양수산과학기술진흥원, 극지연구소 등) 다양한 사회 안전망에서의 국내 AI 보안 기술 연구 역량을 향상시키는 프로젝트들을 진행하였으며, 국제/국내 수중통신 표준화 관련 활동을 지속함으로써 AI 보안 전문가 양성에 힘씀
- 본 연구단은 평가기간 내에 savonia 대학과 협력하여 공동 연구를 진행하고 관련 연구 결과를 국제 학술지에 논문을 발표하였음

1.3 교육연구단의 구성

① 교육연구단장의 교육・연구・행정 역량

성 명	한 글	이옥연	영 문	Yi, Okyeon
소 속 기 관	국민대학교 과학기술대학 정보보안암호수학과			

<표 1-1> 평가 대상 기간(2020. 9. 1. ~ 2024. 2. 29.) 내 교육연구단장 변경 현황

연번	성명	교육연구단장 수행 기간 (YYYYMMDD-YYYYMMDD)	변경 사유
1	이옥연	20200901-20240229	변경없음

▶ 교육연구단장 최근 5년간 연구실적

연번	저자/수상자/발명자/창업자	논문제목/저서제목	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	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	발명자	대기환경 분석 가능형 교통신호 처리 장치	특허청	2021년 08월 06일	특허 등록	제 10-2289406호
5	저자	Privacy Preservation in Edge Consumer Electronics 3 by Combining Anomaly Detection with Dynamic 4 Attribute-Based Re-Encryption	Mathematics 2020	Mathematics 2020, 8, 1871	게재	doi:10.3390/math8111871
6	저자	Secure and Optimal Secret Sharing Scheme for Color Images	Mathematics 2021	Mathematics 2020, 9, 2360	게재	doi:10.3390/math9192360
7	저자	Convolution Neural Network-Based Sensitive Security Parameter Identification and Analysis	Hindawi WCMC	2022:1-13	게재	doi:10.1155/2022/9584894

8	저자	A Study on Scalar Multiplication Parallel Processing for X25519 Decryption of 5G Core Network SIDF Function for mMTC IoT Environment	Hindawi WCMC	2022:1-17	게재	doi:10.1155/2022/4087816
9	발명자	양자 엔트로피 기반 일회용 양자 비밀번호 생성 장치	특허청	2022년 04월 08일	특허 출원	제 10-2022-0043951호

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

▶ 국내 정보보안 및 암호산업 발전에 기여

- 2007년부터 2021년 08월 현재까지 대검찰청의 디지털수사 자문위원으로 디지털 포렌식 분야의 기술력 연구 및 관련 기술확보에 기여함
- 2013년부터 한국암호포럼의 안전성평가분과위원장과 정책분과위원장을 역임하였고, 2019년 11월부터 한국암호포럼 의장으로 정보보안의 핵심 원천기술인 암호모듈 시험기술 개발 및 표준화에 기여함
- 2016년부터 한국정보화진흥원(NIA)와 교통신호제어시스템용 무선모뎀용 정보보안 표준규격서를 개발을 성공하여, 2017년 4월 경찰청의 교통신호제어기용 표준규격서 (NPA-TSC-STANDARD-2018-04-30 (2010R16) 제정을 주도하였고, 현재에는 디지털교통신호제어기 보안 표준연구를 진행하고 있음
- 과학기술정보통신부의 5G 보안협의회 위원으로 5G 보안기술 및 상용화 방안 수립에 기여하고 있음
- 국내 정보보안 및 암호관련 사회문제 해결에 기여
- 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 스마트 그리드용 검증필암호모듈(CM-112-2021.03, CM-132-2022.11) 개발에 성공하여, 2016년 2,500억 규모의 200만 가구 및 2017년 3,000억원 규모의 300만 가구용 지능형전력망의 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, 국가정보원이 후원하는 ‘2020년, 2021년 국가암호공모전’을 한국암호포럼 의장으로써 총괄 작업을 주도하여 국내 암호기술 발전과 관련 인력양성에 기여함

② 교육연구단 참여교수

<표 1-2> 교육연구단 참여교수 현황

연번	소속대학 및 소속학과	성명 (한글/영문)	연구자 등록번호	세부전공분야	대표연구 업적물 분야	신임교수	외국인
1	국민대학교 정보보안암호수학과	강주성 /Ju-Sung Kang	10127144	확률과정론	정보보안 정보보안 	기존	내국인
2	국민대학교 정보보안암호수학과	김동찬 /Dong-Chan Kim	11579260	암호론	암호론/부호론/정보이론/알고리즘 암호론/부호론/정보이론/알고리즘 	기존	내국인
3	국민대학교 정보보안암호수학과	김종성 /Jongsung Kim	10182694	정보보호	정보보안 정보보안 정보보안	기존	내국인
4	국민대학교 소프트웨어전공	박수현 /Soo Hyun Park	10056675	컴퓨터학	통신(원천) 통신(원천) 통신(원천)	기존	내국인
5	국민대학교 정보보안암호수학과	서석충 /SEO SEOGCHUNG	10875717	컴퓨터보안	정보보안 정보보안 정보보안	기존	내국인
6	국민대학교 정보보안암호수학과	염용진 /Yeom Yongjin	10090653	해석학	정보보안 정보보안 	기존	내국인
7	국민대학교 정보보안암호수학과	유일선 /Ilsun You	10146537	정보보호	정보보안 정보보안 	기존	내국인
8	국민대학교 인공지능학부	윤상민 /Yoon Sang Min	10701285	인공지능	소프트웨어 소프트웨어 소프트웨어	기존	내국인
9	국민대학교 정보보안암호수학과	이옥연 /Yi, Okyeon	10056884	유무선통신보안	정보보안 정보보안 정보보안	기존	내국인
10	국민대학교 소프트웨어전공	최은미 /Eunmi Choi	10116354	컴퓨터학	인공지능/빅데이터 통계분석(응용통계) 인공지능/빅데이터 통계분석(응용통계) 인공지능/빅데이터 통계분석(응용통계)	기존	내국인
11	국민대학교 정보보안암호수학과	한동국 /Han, Dong-Guk	10128486	암호론	정보보안 정보보안 	기존	내국인

〈표 1-3〉 교육연구단 참여교수 현황

평가 대상 기간	구분	총 환산 참여교수 수 (단위: 명)		
		기존교수 수	신임교수 수	합계
2020. 9. 1. ~ 2024. 2. 29.	전체	10.57	0	10.57
	이공계열	10.57	0	10.57
	인문사회계열	0	0	0

③ 교육연구단 구성의 적절성

〈표 1-4〉 참여교수진의 해당 산업·사회 문제 해결분야 교육 실적 및 연구 분야

연번	성명 (한글/영문)	직급	연구자등록번호	소속대학 및 소속학과	세부전공분야	산업·사회 문제 해결분야 관련 대학원 교과목 개설 실적
	산업·사회 문제 해결분야 관련 연구분야와의 연계성					
1	이옥연	교수	10056884	국민대학교 금융정보보안학과	유무선통신보안	이동통신보안(통신) (2020년 2학기)
	이동통신 기술의 이론 교육을 통해 이동통신 세대에 따른 특징 및 보안 요소에 대한 이해를 높이고 특히 5G 이동통신의 보안 프로토콜을 교육함. 이를 통해 이동통신 기술 이해와 이동통신 기술의 보안 수준을 향상시킴					
2	이옥연	교수	10056884	국민대학교 금융정보보안학과	유무선통신보안	암호모듈평가및검증(암호) (2022년 1학기)
	국가/공공기관 정보통신망 내 자료 중 비밀로 분류되지 않은 중요 정보보호에 사용되는 암호모듈의 안전성과 적합성을 검증하는 암호모듈 평가 및 검증 방법에 대한 이론과 실습 교육을 수행하고, 보안평가 기술 이해와 현장시험 능력을 향상시킴					
3	강주성	교수	10127144	국민대학교 금융정보보안학과	확률과정론	정보보안프로토콜(암호) (2021년 1학기)
	다양한 암호 알고리즘의 기능과 안전성 연구를 기반으로 정보보호프로토콜의 안전성과 효율성 분석 기법 및 보안 프로토콜을 선택 기준을 교육함. 이를 통해 전반적인 암호 시스템의 프로토콜 안전성을 확보하고 국내 산업의 보안 수준을 향상시킴					
4	강주성	교수	10127144	국민대학교 금융정보보안학과	확률과정론	난수성분석론(암호) (2022년 1학기)
	난수발생기의 안전성 평가와 분석을 위한 확률론과 통계학적 이론을 기반으로 통계적 난수성 평가와 엔트로피 추정 방법 연구함으로써 안전한 난수발생기 설계 및 평가 방법을 교육함. 이를 통해 국내 산업의 암호 시스템 건전성 수준을 향상시킴					
5	김동찬	부교수	11579260	국민대학교 금융정보보안학과	암호론	보안기술표준분석및구현 (2021년 1학기)
	양자내성암호는 기반문제를 기준으로 크게 격자/부호기반으로 나뉘며, 각 기반 문제는 깊은 수학 지식이 필요함. 격자/부호 기초 이론과 각 기반 문제로 암호를 구성하는 방법을 파악하여, 국내 산업의 양자내성암호 이해 수준을 향상시킴					

6	김동찬	부교수	11579260	국민대학교 금융정보보안학과	암호론	공개키암호분석이론(암호) (2021년 2학기)
	암호의 증명가능 안전성에 대한 이해를 높이고, 현재 사용되고 있는 공개키암호 규격을 교육함. 이를 통해 현재 사용되는 알고리즘의 구조가 어떤 안전성을 근거로 설계되었는지 파악하여, 국내 산업의 보안 수준을 향상시킴					
7	김종성	부교수	10182694	국민대학교 금융정보보안학과	정보보호	디지털포렌식개론(디바이스) (2021년 2학기)
	디지털 포렌식의 이론을 교육하고 디지털 포렌식 수사 과정에 필요한 법령과 여러 도구에 대한 교육을 진행함. 실제 디지털 포렌식 수사에 대한 이해를 높임으로써 문제해결형 정보보안 전문인력을 양성하는 데 기여함.					
8	김종성	부교수	10182694	국민대학교 금융정보보안학과	정보보호	디지털포렌식특수연구(디바이스) (2022년 1학기)
	스마트폰, PC 같은 기기에 존재하는 디지털 데이터가 디지털 포렌식 수사에 활용될 수 있도록 관련 지식을 이론과 실습을 병행하여 교육함. 실전적인 디지털 포렌식 수사를 경험함으로써 문제해결형 정보보안 전문인력을 양성하는 데 기여함					
9	박수현	교수	10056675	국민대학교 금융정보보안학과	컴퓨터학	사물지능망특론 (2023년 1학기)
	사물지능망특론 과목을 통해 IoT 및 엣지 컴퓨팅 시스템의 설계를 교육함. 또한 극한 환경에서의 사물지능망 설계의 정보보안에 관한 최신 논문 동향을 살펴봄으로써 국내 산업의 문제를 해결하는데 필요한 기술을 연구함					
10	박수현	교수	10056675	국민대학교 금융정보보안학과	컴퓨터학	무선이동통신네트워크 (2021년 2학기)
	무선이동통신네트워크 과목을 통해 IEEE 802.11 기술 표준 문서를 통해 기본적인 무선 이동통신 기술과 최근 산업에서 활용안에 대해 교육함. 이를 통해 실제 산업 환경에서의 무선 이동통신 네트워크의 보안 취약점을 진단하고 해결하는 실질적인 기술을 연구하여 산업 발전에 기여함					
11	서석충	조교수	10875717	국민대학교 금융정보보안학과	컴퓨터보안	암호소프트웨어구현(암호) (2021년 1학기)
	공개키 암호 (ECC, 이산대수 기반) 체계를 산업환경에서 사용되는 디바이스 관점에서의 구현 방법론을 교육함. 공개키 암호 연산의 성능 부하를 줄이고 안전성 관점의 구현을 배움으로써 국내 산업의 보안 수준을 향상시킴					
12	서석충	조교수	10875717	국민대학교 금융정보보안학과	컴퓨터보안	보안구현개발방법론(디바이스) (2021년 2학기)
	검증대상 암호모듈에 대한 설계사상과 CAVP, 정적분석 등 검증대상 암호알고리즘과 유한상태모델의 구현 안전성과 관련된 교육을 진행함. 국내 산업에서 사용하는 암호모듈을 상세히 분석하고 보안 수준을 향상시킴					
13	염용진	교수	10090653	국민대학교 금융정보보안학과	해석학	융합보안특강 (2020년 2학기)
	암호학을 기반으로 IT 융합 및 보안에 대한 종합적인 이론을 습득하고, 암호학의 악의적 사용과 대책에 대하여 교육함. 이를 통해 실제 수행될 수 있는 공격 기법에 안전한 암호 시스템을 설계 기술을 확보하고 국내 산업의 보안 수준을 향상시킴					

<table>
<tr><td rowspan="2">14</td><td>염용진</td><td>교수</td><td>10090653</td><td>국민대학교
금융정보보안학과</td><td>해석학</td><td>대칭키암호분석(암호)
(2021년 1학기)</td></tr>
<tr><td colspan="6">블록암호 및 스트림암호 해시함수 등에 대한 안전성 분석 기술을 연구하고, 이를 바탕으로 암호 알고리즘의 설계 기준과 사용환경에 따른 안전한 알고리즘의 선택 및 활용 기법을 교육함. 이를 통해 국내 산업의 안전성 기반 마련에 기여함</td></tr>
<tr><td rowspan="2">15</td><td>유일선</td><td>교수</td><td>10146537</td><td>국민대학교
금융정보보안학과</td><td>정보보호</td><td>인공지능과보안이론(AI)
(2023년 1학기)</td></tr>
<tr><td colspan="6">인공지능 및 보안이론 교육을 통해 인공지능 기술에 대한 이해를 높이고 보안 이론과 융합하여 더욱 강한 보안성 검증을 진행할 수 있는 방안을 교육함. 이를 통해 4차 산업혁명 시대에 대응할 수 있는 보안 이론의 수준을 향상시킴</td></tr>
<tr><td rowspan="2">16</td><td>유일선</td><td>교수</td><td>10146537</td><td>국민대학교
금융정보보안학과</td><td>정보보호</td><td>금융네트워크보안
(2023년 2학기)</td></tr>
<tr><td colspan="6">금융네트워크보안 교육을 통해 금융 환경에서의 네트워크에서 발생할 수 있는 공격에 대해 소개하고 취약점을 도출할 수 있는 방안을 교육함. 이를 통해, 금융 환경에서의 보안성 수준을 검증하고 국내 산업 보안 수준을 향상시킴</td></tr>
<tr><td rowspan="2">17</td><td>한동국</td><td>교수</td><td>10128486</td><td>국민대학교
금융정보보안학과</td><td>암호론</td><td>부채널공격대응론(디바이스)
(2021년 1학기)</td></tr>
<tr><td colspan="6">부채널 공격 이론 및 실습 교육을 통해 부채널 공격에 대한 이해를 높이고 부채널 공격의 대응기술에 대한 이론 및 적용 방안을 교육함. 이를 통해 암호 디바이스의 부채널 안전성을 확보하고 국내 산업의 보안 수준을 향상시킴</td></tr>
<tr><td rowspan="2">18</td><td>한동국</td><td>교수</td><td>10128486</td><td>국민대학교
금융정보보안학과</td><td>암호론</td><td>금융디바이스공격론
(2022년 1학기)</td></tr>
<tr><td colspan="6">스마트카드, 스마트폰 등 금융 디바이스에 대한 부채널 공격 교육 및 실제 디바이스에 대한 부채널 취약성 검증 과정을 교육함. 이를 통해 금융 디바이스의 부채널 안전성을 검증하고 국내 산업의 보안 수준을 향상시킴</td></tr>
</table>

▣ **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 11인의 교수는 안전한 초연결사회에 필수적으로 요구되는 5G/6G 통신 분야, 디바이스 보안 분야, 암호 분야, 인공지능 분야 등에 전문성을 보유함
- 소속된 11인의 교수는 전문지식을 바탕으로 단순 전달식 강의가 아닌 다양한 외부과제 및 정보보안 사례기반 교육, 실습 위주의 실사구시 교육을 통하여 다양한 산업·사회 문제해결이 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

[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 인공지능 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

④ 전임교수(신임교수) 충원 실적

▶ 우수 신임교원 충원을 위한 계획

- 대학원의 우수한 인재들이 실질적인 연구활동을 수행할 수 있는 학·연·산 협동과정 확대
- ‘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
- 우리대학은 대학원 운영을 위해 행정지원 인력을 배치하여 각 학과·전공의 제반 학사관리를 수행하고 있으며, 이러한 인력 중 신임교원에 대한 전담지원 담당자 제도를 계획하고 있음

▶ 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, 대학원제도혁신, 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 참여대학원생 현황

<표 1-5> 교육연구단 평균 참여대학원생 현황

(단위: 명)

구분	참여대학원생 수			
	석사	박사	석·박사통합	계
7개 학기의 평균	23.29	10	2.71	36

<표 1-6> 교육연구단 외국인 참여대학원생 현황

연번	성명	국적	학사출신대학	공인어학성적		비고
				국어	영어	
1	K E S A R I M A R Y DELPHIN RAJ	인도	Malankara Catholic College, M.S.University	-	-	
2	S H R U T I K A SINHA	인도	Shaheed Bhagat Singh Technical University, Ferozepur, Punjab	-	TEPS(total score: 386, level: 2; percentile rank 72.87) / TOEIC(870)	
3	SHURENGEREL SERGELEN	몽골	서울과학기술대학교	TOPIK(6급)	-	

4단계 BK21사업

Ⅱ. 교육역량 영역

Ⅱ. 교육역량 영역

1. 교육과정 구성 및 운영 실적

▣ 교육연구단 교육 목표

- 초연결사회의 정보보안을 선도하는 전문가 양성을 위한 미래 정보보안 교육과정 운영

▣ 문제해결형 전문가 양성을 위한 교육 과정 세부 목표

▶ 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
- 산업계, 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

▶ **교육과정표 대비 개설현황**

순번	구분	개설시기	교과목명(신청서 기준)	담당교수	비고(개설교과명)
1	공통기초		연구윤리와논문연구		
2	공통기초	20-2학기	암호알고리즘	김동찬	
3	공통기초	20-2학기	정보보안론	이수미	금융정보보안론
4	공통기초		PKI개론		(공개키기반구조)
5	기반이론	23-2학기	고급정보통신론(통신)	박수현	
6	기반이론		해시함수와데이터인증(암호)		
7	기반이론		임베디드시스템(통신)		
8	기반이론	22-2학기	병렬암호구현(암호)	염용진	
9	기반이론		실시간시스템(통신)		
10	기반이론	21-1학기	정보보안프로토콜(암호)	강주성	정보보호프로토콜
11	기반이론	23-1학기	부채널공격론(디바이스)	한동국	
12	기반이론		데이터마이닝(AI)		
13	기반이론	21-2학기	보안구현개발방법론(디바이스)	서석충	
14	기반이론	23-1학기	인공지능과보안이론(AI)	유일선	
15	기반이론	21-2학기	디지털포렌식개론(디바이스)	김종성	
16	핵심역량	21-2학기	공개키암호분석이론(암호)	김동찬	
17	핵심역량	21-2학기	무선보안특강(통신)	이옥연	
18	핵심역량	21-1학기	암호소프트웨어구현(암호)	서석충	
19	핵심역량		클라우드컴퓨팅(통신)		
20	핵심역량	21-1학기	대칭키암호분석(암호)	염용진	
21	핵심역량	21-1학기	부채널공격대응론(디바이스)	한동국	
22	핵심역량		모델기반시스템설계(AI)		
23	핵심역량	22-1학기	디지털포렌식특수연구(디바이스)	김종성	
24	핵심역량		자율성장인공지능특론(AI)		
25	심화응용	20-2학기	이동통신보안(통신)	이옥연	
26	심화응용	22-1학기	난수성분석론(암호)	강주성	
27	심화응용		정보시스템개발방법론(통신)		
28	심화응용	20-2학기	증명가능안전성론(암호)	강주성	
29	심화응용		IoT네트워크(통신)		
30	심화응용	22-1학기	암호모듈평가및검증(암호)	이옥연	
31	심화응용	22-1학기	디바이스공격대응론(디바이스)	한동국	금융디바이스공격론
32	심화응용		인공지능융합기술특강(AI)		

33	산업융합		정보보안시스템평가방법론		
34	산업융합	20-2학기	융합보안특강	염용진	
35	산업융합		정보보안컨설팅		
36	산업융합	23-1학기	사물지능망특론	박수현	
37	산업융합	21-1학기	보안기술표준분석및구현	김동찬	
38	심화응용	23-2학기	금융네트워크보안	유일선	

▣ 단계별 인력양성 프로그램 로드맵

▶ 1단계(2020~2021) : 정보보안 교육체계 수립

- 교육목표 및 비전 수립
- 정보보안 협동과정의 교과목 및AI 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 체계정착
- 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

▣ 통신보안 분야 교육과정 운영

▶ 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: 무선이동통신네트워크, 사물지능망특론

▶전임교원 추진 실적 및 강의 계획
- 참여교수인 이옥연 교수는 이동통신 분야인 5G / 6G의 정보보안 구현 및 정보보안 서비스 신뢰성 확보를 위한 기술에 관하여 교과과정을 구성하여 운영함.
- 이동통신 보안을 위해서는 이동 통신환경에서의 구성요소 및 프로토콜에 대한 충분한 이해가 필요하며, 이동통신 보안에서 사용하는 타원곡선암호에 대한 이해를 위해 이동통신보안, 암호알고리즘 등의 교과과정을 구성함
- 정보보호프로토콜, 이동통신보안, 암호모듈평가 및 검증 등의 과목을 주요 과목으로 선정하고 연차별로 과목 개설을 하고 있음
- 2020년, 이옥연 교수는 이동통신보안(Mobile Security)과목 개설을 통해 2G, 3G, LTE, 5G 등의 이동통신망의 보안구조를 학습하고, 이후 LoRa, NB-IoT, LTE Cat.M1 등의 다양한 소물인터넷 등의 환경

에서의 정보보안구조 및 그 응용 기술에 대해 교육함
- 2021년, 이옥연 교수는 융합보안특강 과목 개설을 통해 암호이론에 기반한 정보보호 개념을 바탕으로 3G, 4G, 5G 등의 이동통신망, WiFi, TVWS 등의 무선망 등 다양한 유무선 통신망에 기반한 보안의 활용 기술에 대해 교육함
- 2021년, 이옥연 교수는 무선보안특강 과목 개설을 통해 4G, 5G, 6G, TVWS, WiFi, 위성통신 등의 무선통신 기술 및 관련 정보보안과 다양한 무선통신에 사용되는 정보보안 구조를 학습하고, 필요한 암호 알고리즘에 대해 교육함
- 2022년, 이옥연 교수는 암호모듈평가및 검증 과목 개설을 통해 공개키, 대칭키, 해쉬함수 등의 검증필 암호모듈 제도에 대하여 학습하고 검증필 암호모듈 제도에 따른 절차 및 구현방법에 대한 내용을 교육함. 국내외 검증필 암호모듈 제도의 변화 및 방향에 대해서도 교육함
- 2022년, 이옥연 교수는 암호알고리즘 과목 개설을 통해 공개키 암호알고리즘인 타원곡선 암호의 수학적 구조, 최적화 구현 등을 교육하고 타원곡선 암호의 응용 분야와 활용 목적 등에 대한 내용에 대해서도 교육함
- 유무선 통신 및 5G에서 6G에 이르는 보안 관련 기술의 표준화 분야 전문가들을 초청하여 워크숍 및 콜로키움 개최 등과 같이 특화된 교육 프로그램을 운영함.

- 참여교수인 박수현 교수는 수중, 해상, 극한지 등 특수한 환경에서의 통신 네트워크의 정보 보안 구현 및 서비스 신뢰성 확보를 위한 기술에 관하여 교육 과정을 운영했음
- 2021년, 박수현 교수는 무선이동통신네트워크 과목 개설을 통해 사물인터넷과 디지털 트윈의 개념을 학습하고, IoT를 서비스, 플랫폼, 연결 및 디바이스의 관점에서 이해할 수 있고, 디지털 트윈의 응용, 프레임 워크, 아키텍처 및 AI 기반 모델링 및 시뮬레이션 등에 대하여 수행할 수 있는 방법을 교육함
- 2024년, 박수현 교수는 사물지능망특론 과목 개설을 통해 사물 인터넷 및 엣지 컴퓨팅 시스템을 설계 및 구현하는 아키텍처를 이해하고, 사물인터넷과 엣지 컴퓨팅 환경을 효과적으로 관리하는 방법에 대하여 지도하여 아키텍트가 IoT 및 엣지 컴퓨팅 프로젝트를 설계할 때 안전한 네트워크 아키텍처를 구축하고, 다양한 보안 위협으로부터 시스템을 보호하는 방법에 대하여 학습할 수 있도록 교육함

- 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 전문인력양성을 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

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

▶전임교원 추진 실적 및 강의 계획
- 참여교수인 한동국 교수는 부채널 공격 및 대응기술에 대한 교과 과정을 구성하여 운영함
- 부채널 분석 기술 이론과 암호 디바이스의 동작 과정 이해 및 제어를 통한 부채널 정보 수집 및 분석 과정에 대해 교육함
- 2021년, '부채널공격대응론' 과목을 개설하여 부채널 공격 이론 및 실습 교육을 통해 부채널 공격에 대한 이해를 높이고 부채널 공격의 대응기술에 대한 이론 및 실제 적용 방식을 교육함
- 2022년, '금융디바이스공격론' 과목을 개설하여 금융 디바이스의 동작 과정과 그 구조에 적용될 수 있는 부채널 공격을 교육하고 실험을 통해 금융 디바이스의 부채널 취약점과 그에 대한 대응기술을 교육함
- 2023년, '부채널공격론' 과목을 개설하여 다양한 대칭키, 공개키 암호에 대한 부채널 공격 적용 논리를 교육하고, 이를 통해 다른 암호에 대해서도 부채널 공격 논리를 찾는 방식을 교육함
- 2023년, '부채널공격대응론' 과목을 개설하여 부채널 공격 이론 및 실습 교육을 통해 부채널 공격에 대한 이해를 높이고 부채널 공격의 대응기술에 대한 이론 및 실제 적용 방식을 교육함

- 참여교수인 김종성 교수는 디지털 포렌식 기술을 이용한 증거획득 기술 및 산업보안 기술에 관하여 교과 과정을 구성하여 운영함
- 포렌식 분석도구 사용 및 해석, 실제 디바이스에서의 데이터 추출 및 분석을 진행하는 등 디바이스 포렌식 기술에 대해 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

- 2021년, 김종성 교수는 해시함수와데이터인증(Hash Function and Message Authentication)과목 개설을 통해 전자서명에 활용되는 충돌 회피 해시 함수 및 이를 응용하여 데이터 위변조를 검출할 수 있는 MAC 생성 방법의 설계 원리를 교육함
- 2022년, 김종성 교수는 디지털포렌식개론과목 개설을 통해 안티포렌식 기술에 대한 이해와 안티포렌식 기술을 우회하기 위한 안티안티포렌식 기술을 교육하고 실사례를 분석함으로써 원리를 교육함
- 2022년. 김종성 교수는 디지털포렌식특수연구과목 개설을 통해 최신 디지털포렌식 기술 동향을 학습하고, 크리덴셜 정보 활용 등 다양한 기법을 활용한 데이터 획득 방법을 교육함
- 2023년, 김종성 교수는 COVID-19 언택트 환경에서의 보안 및 암호의 중요성을 알 수 있도록 보안프로토콜 과목을 개설하였고, 이를 인공지능 전문가의 시각에서 바라볼 수 있도록 인공지능 분야 전문가를 초빙하여 세미나를 개최함
- 2023년, 김종성 교수는 ‘디지털 포렌식 개론’ 과목을 개설하여 디지털 포렌식 수사과정과 실제 현장에서 사용되는 포렌식 분석 기술들을 강의함으로써 본교 대학원생들의 연구역량 강화에 기여함
- 2023년, 김종성 교수는 ‘해시함수와데이터인증’ 과목을 개설하여 암호 분야의 핵심 프리미티브인 해시함수의 개념과 안전성 개념을 강의하였고, 대학원생들이 해시함수를 기반으로 블록암호와 같은 다른 종류의 암호 프리미티브를 생성하는 방식을 습득할 수 있도록 하였음

- 참여교수인 서석충 교수는 양자내성암호 분석 및 구현, 암호모듈 평가 및 검증과 관련된 산업보안 기술과 관련하여 교과과정을 개설하였음
- 양자내성암호 분석 및 구현 관점에서 NIST 양자내성암호 공모전에 제안되고 표준화 대상으로 선정된 알고리즘에 대한 구현적 관점의 분석을 교육함. 또한, 성능 및 메모리가 제한된 임베디드 환경에서의 구현 방법론 교육과 고성능 병렬 환경에서의 구현 방법론에 대한 교육을 진행하였음
- 현재 국내의 KCMVP 검증제도의 이해를 돕기 위해 검증대상 알고리즘에 대한 구현 방법론 및 암호모듈의 유한상태모델에 대한 구현 방법론을 교육함
- 2021년, 서석충 교수는 “암호소프트웨어구현” 과목 개설을 통해 현존하는 공개키 암호 (ECC, 이산대수 기반) 체계에 대해 산업환경에서의 사용되는 디바이스에서의 구현 방법론을 교육함.
- 2021년 서석충 교수는 “보안구현개발방법론” 과목 개설을 통해 검증대상 암호모듈에 대한 설계사상과 CAVP, 정적분석 등 검증대상 암호알고리즘과 유한상태모델의 구현 안전성과 관련된 교육을 진행함
- 2022년 서석충 교수는 “금융키관리시스템” 과목 개설을 통해 금융 보안관점으로 산업에서 사용하고 있는 키 관리 모듈에 대한 보안 요구사항을 교육함
- 2022년 서석충 교수는 “암호소프트웨어구현” 과목 개설을 통해 NIST 표준화 대상 양자내성암호에 대한 최신 구현 연구결과들을 교육하고, 임베디드 환경에서의 다항식 곱셈 구현 방법론에 대한 교육을 진행함
- 2023년 서석충 교수는 “보안구현개발방법론” 과목 개설을 통해 검증대상 암호모듈의 설계 사상을 비롯한, 검증대상 공개키암호 시스템에 대한 구현 방법론에 대한 교육을 진행함
- 2024년 서석충 교수는 “암호모듈평가 및 검증” 과목 개설을 통해 암호모듈 검증 시험관 관점에서의 CAVP 및 유한상태모델 평가 방법론에 대한 교육을 진행함

- 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 정보수집과 노이

즈 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 신호처리기법에 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 기존의비밀 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 분석해보면서 포렌식 분석 기술 향상을 도모함
- 디바이스별 데이터 추출 및 분석에 대한 교육을 마치면 EnCase, MD-RED 등의 상용 포렌식 분석도구 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 하

드웨어-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

▶전임교원 추진 실적 및 강의 계획
- 참여교수인 강주성 교수는 안전한 암호 시스템을 구축하기 위한 원천 기술인 난수발생기 및 안전선 증명에 관하여 교과 과정을 구성하여 운영함
- 암호 시스템의 안전성을 보장하는 암호키 및 IV(initial vector)에 사용되는 솔트(salt)와 논스(nonce)는 난수발생기를 이용하여 생성하므로, 난수발생기가 암호학적 난수를 생성할 수 있는가 평가하기 위한 확률론적 이론을 교육함
- 보안 인프라의 각 요소들은 단순히 프로그램적 연동만으로는 목적하는 안전성을 달성할 수 없으므로 안전성 평가 기법에 대한 이해 하에 연동해야만 함. 이를 위해 다양한 암호학적 스킴(scheme)을 설계할 때 고려해야 하는 전반적인(general) 공격에 대한 암호 시스템의 안전성 증명을 위한 일반론적 모델 구축 기법에 대해 교육함
- 2020년, 강주성 교수는 증명가능안전성론(Provable Security)과목 개설을 통해 암호 시스템 안전성의 본질적 개념을 구성하는 perfect secrecy와 실질적 암호 알고리즘 구축을 위한 확장 및 응용 과정에서 안전성 저해를 막기 위하여 고려할 확률론적 개념을 교육함
- 2021년, 강주성 교수는 정보보호프로토콜과목 개설을 통해 키교환의 안전성 보장을 위한 프로토콜 설계 기법에 관하여 교육하고, 적용 어플리케이션의 요구 조건에 따른 보안 요소 구성 기법 및 안전성과 효율성 분석 능력을 교육함
- 2021년, 강주성 교수는 증명가능안전성론과목 개설을 통해 Pseudo-randomness, 정보이론 관점의 안전성, 계산복잡도 측면의 안전성 등 암호 알고리즘 및 프로토콜에 대한 증명가능 안전성 이론에 관해 교육함
- 2022년, 강주성 교수는 난수성분석론과목 개설을 통해 정보보안 프로토콜 및 암호 알고리즘에 필수적으로 사용되는 난수발생기의 설계와 안전성 평가, 분석 방법을 교육함
- 2022년, 강주성 교수는 증명가능안전성론과목 개설을 통해 Shannon’s Perfect Secrecy, 엔트로피, 블록암호의 의사난수성, 블록암호 운영모드의 안전성 분석, 해쉬함수의 안전성 분석, MAC의 안전성 등을 교육함
- 2023년, 강주성 교수는 정보보호프로토콜과목 개설을 통해 키교환 프로토콜, 위탁 프로토콜, 식별 프로토콜 등의 보안 목적에 부합하는 정보보호프로토콜의 안전성과 효율성을 올바르게 분석할 수 있는 능력을 배양함
- 2023년, 강주성 교수는 난수성분석론과목 개설을 통해 난수발생기의 안전성 평가 능력을 배양하기 위해 통계적 난수성 검정, 엔트로피 추정 방법 등을 교육함

- 참여교수인 염용진 교수는 안전 암호 시스템을 구축하기 위한 암호 스킴 설계 및 분석 기법 중 화이트박스 암호 및 암호 시스템 전반에 대한 공격 기법 분석에 대한 응용 교과 과정을 구성하여 운영함
- 암호의 개발과 안전성 평가 및 분석을 위해 필요한 암호 시스템 중 대칭키 암호 시스템에 대한 분석 기법과 이를 활용하는 화이트박스 암호시스템에 대하여 교육하고, 확률론적 안전성 분석을 위한 정보이론에 대한 능력을 배양함
- 2020년, 염용진 교수는 융합보안특강과목 개설을 통해 안전할 것으로 보이는 암호 알고리즘들의 공격 가능성을 파악하는 관점을 기르고 공격에 대응하기 위하여 수행 가능한 일반적인 대응 기법들에 관하여 교육함
- 2021년, 염용진 교수는 대칭키암호분석(Tophics in Symmetric Key Cryptanalysis)과목 개설을 통해 블록암호 및 스트림암호 해시함수 등에 대한 안전성 분석을 위한 기본기술과 사용 환경에 따라 안전한 알고리즘의 선택, 활용 능력을 교육함
- 2022년, 염용진 교수는 보안기술표준분석및구현과목 개설을 통해 국제표준화기구(ISO/IEC), 미국 국가표준기술연구원(NIST), IETF등에서 발간하는 보안기술 관련 표준을 학습함으로써 안전한 구현 기법과 ISO/IEC, IETF등의 국제표준기술에 대한 이해를 바탕으로 표준기술을 활용한 보안시스템을 안전하게 설계할 수 있는 능력을 배양함
- 2022년, 염용진 교수는 병렬암호구현과목 개설을 통해 현장에서 대칭키 암호 알고리즘을 구현할 때 성능 향상을 위하여 고려할 수 있는 기법을 교육하고 컴퓨터 구조에 대한 이해를 암호 시스템 설계 및 구현에 활용하는 능력을 배양함
- 2023년, 염용진 교수는 고급정보통신론과목 개설을 통해 정보통신과 정보보안에 필수적인 정보이론을 중심으로 엔트로피 개념, 오류정정부호 원리 등을 학습함으로써 암호학적 안전성 분석 능력을 교육함

- 참여교수인 김동찬 교수는 안전한 초연결사회를 위한 암호 전문인력 양성을 위해 다음과 같은 교육과정을 운영했음
- 학부 강의인 ‘고급 응용 프로그래밍’을 통해 공개키 암호인 RSA나 타원곡선암호 등을 구현하기 위한, 큰정수 연산을 다루는 알고리즘과 C언어의 메모리 할당 방법등을 지도하였음. 이를 응용하여 표준 규격에 맞춰 암호 알고리즘을 구현하는 ‘보안기술 표준 분석 및 구현’(대학원) 강의를 개설하였음.
- 증명가능 안전성을 보장하는 암호를 설계하는 전문인력 양성을 위해 다음과 같은 강의를 개설하였음.
- 학부 강의인 ‘공개키 암호’에서 공개키 암호의 기반 문제와 규격을 지도하였고, 이를 바탕으로 대학원 강의인 ‘공개키 암호 분석 이론’을 개설하였음. 해당 강의에서는 안전성의 개념을 이해하도록 지도하고, 현재 사용되고 있는 공개키 암호의 증명가능 안전성 분석을 수행하였음.
- 대학원 강의인 ‘해시함수와 데이터 인증‘에서는 안전성을 보장하며 암호를 설계하는 방식을 지도하였음.

- 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, 유일선
- 최은미 교수: 데이터마이닝, 분산지능화 시스템
- 윤상민 교수: 인공지능 기술, 빅데이터 분석 및 적대적 공격 / 방어 시스템
- 유일선 교수: 정보보안/AI, 미래 초연결 환경

▶전임교원 추진 실적 및 강의 계획
- 참여교수인 최은미는 데이터마이닝, 분산지능화 시스템, 인공지능 기술 확보를 위해 다음과 같은 교육 과정을 추진하고 있음. 데이터마이닝, 인공지능과 보안 이론, 모델기반시스템설계, 자율성장 인공지능 특론, 인공지능 융합기술 특강 과목을 주요 과목으로 선정하고 연차별로 과목 개설을 하고 있음. 실제 사회에 활용되는 데이터를 기반으로 한 실습 및 분석을 통하여 학생들 스스로 사회 문제에 이해할 수 있도록 교육함
- 2020년 최은미 교수는 모델기반시스템설계 (Model-based system design)과목 개설을 통해 소프트웨어 시스템을 도메인 모델에 기반하여 설계 방법론과 다양한 환경의 문제들을 소프트웨어 시스템으로 구조적 설계와 응용에 관련 교육함.
- 2020년, 최은미 교수는 소프트웨어아키텍처 (Software Architecture) 과목을 개설하여 소프트웨어 시스템을 최적으로 설계하는 방법론, 다양한 시스템의 특성, 품질 속성을 소프트웨어 시스템 아키텍처 설계에 적용하며, 시스템 설계의 주요 구조에 대해서 교육하였음.
- 2021년, 최은미 교수는 과학과소프트웨어적사고, 객체지향프로그래밍 개설한 수업들은 소프트웨어 언어를 처음으로 접하는 학생들에게 프로그래밍 언어를 습득하도록 하며, 과학과 소프트웨어적으로 소프트웨어를 구현하도록 기초적 교육하였음.
- 2022년, 최은미 교수는 과학과소프트웨어적사고, 객체지향프로그래밍 개설한 수업들은 소프트웨어 언어를 처음으로 공부하는 학생들에게 프로그래밍 언어를 습득하도록 하며, 과학과 소프트웨어적으로 소프트웨어를 구현하도록 기초적 자질을 습득하게 함.
- 2023년, 최은미 교수는 객체지향프로그래밍 수업 개설하여 자바 언어의 기본적인 문법 체계와 활용법을 습득하도록 하며, 체계적인 소프트웨어 설계하기 위한 객체지향적인 접근법을 공부하며, 클래스 구성, 객체의 역할, 객체지향 인터페이스 설정, 추상화 설계, 다형성, 예외 상황 등을 교육함.

- 참여교수인 유일선 교수는 정보보안/AI 분야의 융합교육 실현, 미래 초연결 환경의 지속 가능한 발전을 선도하는 정보보안 전문인력 양성을 위해 다음과 같은 교육 과정을 운영했음
- 공개키암호 : 공개키암호의 배경 지식 및 기본 원리와 함께 RSA 등 주요 알고리즘을 학습 한 후, 공개키 기반구조와 공개키 응용 사례를 다루었음
- 캡스톤디자인 : 수강자로 하여금 직접 주제를 선택하고 프로젝트를 진행하도록 지도함으로써 관심분야에 대한 깊이있는 지식과 실무역량, 더 나아가서 문제 해결 능력을 함양하도록 하였음
- 사제동행세미나 : 사물인터넷 보안을 위한 핵심주제를 선택하고, 깊이 있는 학습과 연구를 수행하도록 지도하는데 목적을 두고 학생들이 사물인터넷 보안의 핵심 개념을 습득하고 세미나 기반의 심화학습을 수행하면서 수요지향적인 최신 기술을 학습할 수 있도록 하였음
- 연구참여과정 : 5G보안과 체내삽입형 의료기기보안 (의료 사물인터넷보안), 정형화 보안 검증을 기반으로 담당교수와 연구과제 참여 대학원생들의 도움을 받아 연구주제 선정 및 개인과제 계획을 수립한 후, 연구에 몰입하여 과제 결과를 도출하였음
- 이동통신보안 : 2G부터 5G까지 이동통신 보안구조와 보안 프로토콜, 최신 이동통신 보안위협 및 공격 탐지·대응기술 등을 다뤘으며 관련 내용으로 보안 프로토콜과 EAP(Extensible Authentication Protocol) 프레임워크를 학습했음
- 금융보안개론 : 금융보안의 차세대 핵심기술인 사용자 인증 기술 및 블록체인에 초점을 맞춰 사용자 인증기술, 블록체인의 개요, 블록체인의 구조와 동작원리, 블록체인의 응용사례 등을 학습했음
- 산업체세미나 : 산업 현장에서 활용되는 최신 정보보안 기술을 산업체 강사에 의하여 진행함으로써 정보보안 전공 학생들의 지식을 고취함과 동시에 학생들에게 진로에 대한 동기 부여하고 다양한 분야의 산업체 전문가를 통해 실제적으로 산업체에 사용될 수 있는 기술 및 관련 분야의 동향을 분석할 수 있도록 했음
- 정보보호프로토콜(대학원) : 정보보호 프로토콜에 대한 핵심 이론과 정형화 검증, 사례 연구를 학습하도록 지도함으로써 정보보호 프로토콜 설계 및 분석 능력을 갖출 수 있게 하였음
- 인공지능과보안이론(대학원) : 인공지능을 활용한 보안 기술 및 인공지능의 허점을 분석하기 위한 개념 및 이론을 연구하고 이를 위해 먼저 기계학습과 딥러닝에 대한 핵심 기술을 학습 한후, 최신 관련 논문을 중심으로 인공지능 보안 사례분석을 수행하였음
- 금융네트워크보안(대학원) : 금융네트워크보안의 핵심인 보안프로토콜 개요를 학습하고, 보안 프토토콜의 유효성을 정형적으로 검증하는 기법을 다뤘음. 금융 보안 프로토콜 정형화 검증을 위한 기본적인 도구인 BAN 논리를 학습한 후, 최신 정형화 검증 도구인 Proverif을 통한 보안프로토콜 검증 기법을 학습하고, 실제 Target protocol의 정형화 검증을 수행하였음

- 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 공

격에 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 및 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 현황 및 지원 실적

2.1 교육연구단의 우수 참여대학원생 확보 및 지원 실적

▶ 우수 대학원생 확보 노력

- 본 교육단은 3차년도 기간 동안 대학본부의 국고 예산 대비 20% 현금매칭 등의 지원을 계획하고 시행함
- 본 교육단은 대학원 과목을 학부생이 사전이수 하는 것으로 해당 학생이 대학원에 입학하였을 때 이수 학기를 단축할 수 있는 수업 연한 단축 제도를 계획하고 시행함
- 본 교육단은 국제학술지 논문 투고를 통해 이수 학기를 단축할 수 있는 수업 연한 단축 제도를 시행하고 있으며 이를 통해 연구 의욕 증진을 계획하고 시행함
- 교육연구단의 홈페이지 구축을 통해 랩별 성과 및 연구내용을 소개하였으며, 랩 별로 자체적으로 진학관련 고민 및 궁금증 해소를 위한 상담을 진행함
- 우수 대학원생 확보를 위해 정보보안암호수학과 내에 부채널 분석 동아리, 난수성 분석 동아리, 디지털 포렌식 동아리, 암호 동아리를 지속적으로 운영하는 것으로 계획하고 시행함
- 본교 정보보안암호수학과 학생들을 대상으로 한 공모전을 개최하여 대학원에 관한 관심을 높였으며, 이는 향후 대학원에 입학할 경우 수행할 연구에 대한 밑거름 역할을 할 것으로 기대함
- 본 교육연구단은 학부 교육과정의 일환으로 유레카 프로젝트 과목을 신설하여 각 연구실별 대학원생 멘토를 선정하여 학부 1학년 학생을 대상으로 대학원 연구와 관련된 체험 및 실습 기회를 제공하고 있음
- 유레카 프로젝트를 통해 학부 교육과정에서 습득한 내용의 실제 응용을 통해 관련 분야에대한 연구 식견을 넓히고, 각 팀별 결과물을 '국민암호 페스티벌'에서 공유할 수 있는 기회를 마련하여 학부생의 연구 참여를 독려하고 대학원 연구에 대한 체험 기회를 제공할 계획임
- 본 교육연구단의 각 연구실은 정보보안암호수학과 내에 다양한 동아리 및 소모임을 운영하고 있으며, 대학원 연구와 연계된 다양한 연구 참여 기회를 지속적으로 제공할 계획임
- 동아리 활동의 일환으로 학생들에게 학습과 연구에 필요한 지식과 기자재 지원 등을 통해 학부생의 연구를 지원하고 있으며, 이를 통해 우수 대학원생을 확보하고 있음
- 방학기간 UROP과 학부생 인턴십 프로그램을 통해 학부 과정 학생들에게 연구실에서 진행하고 있는 과제를 경험할 수 있는 기회를 제공하며, 연구실 과제에 대해 소개하고 흥미를 가질 수 있도록 도우며 우수 대학원생을 확보하고 있음
- '학부연구생' 제도 시행을 통해, 학부생들이 BK 교육연구단의 연구 프로젝트에 참여하여 정보보안 분야의 관심을 유도하고, 책임감과 전문성을 갖춘 학생으로 육성하고 있음.
- 본 교육단의 각 실험실 앞에 모니터 설치를 통해 연구실 별로 성과 및 연구 내용 홍보 진행 영상이 출력되도록 함으로써, 대학원에 대한 궁금증을 해소하여 대학원 진학에 흥미를 갖도록 하고 있음

▶ 우수 대학원생 지원 계획

- 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' (연구조교 A: 수업료의 100 %, 연구조교 B: 수업료의 70 %) 등 다양한 장학금 지원을 통해, 인재 확보, 연구 기회, 교육환경 제공에 기여함
- 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 지급하고 있음
- 국내·외 전문가 초청 강연을 진행하여 전공 분야 최신 연구주제 집중특강 및 교수/국내외전문가/대학원생 간 3자 간담회 등을 통해 연구 활동과 학문에 대한 다양한 경험과 열정을 공유함으로써 대학원생에게 미래가 요

구하는 과학 인재로 성장할 기회를 제공함

▶우수 대학원생 확보를 위한 국민대학교 연구 공간 지원

- 교육연구단의 원활한 연구수행을 위하여 2014년 10월 신축한 산학협력관에 교육연구단장 또는 사업참여교수의 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, 학사운영 상의 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 국제 +우수학술지(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

2.2 참여대학원생 학술활동 지원 실적

- 오프라인으로 진행되는 교류 행사에 필요한 항공 운임비 및 체류비를 지원하여 원활한 연구가 진행될 수 있도록 지원하고 있음
- 정보보안 기술을 활용한 다양한 사례를 기반으로 한 국제 학술대회에서 관련 결과물에 대한 발표 및 참석에 대해 지원하고 있음
- 참여대학원생들이 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 지원하고 있음
- 과제 교육비를 통해 미래 암호 워크숍, 위험관리 워크숍, 랜섬웨어대응연구회 워크숍, 5G 보안 워크숍, CPS 보안 워크숍, 공급망 보안 워크숍, 국제 표준화 워크숍, 양자보안 워크숍, IoT 보안 워크숍, 차세대 인프라 보안 워크숍 등에 참석을 지원하여 참여대학원생의 연구 능력을 향상시켰음
- 국내·외 전문가 초청 강연을 진행하여 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 제공함
- 본 교육연구단은 전담 행정인력을 1명 채용할 수 있도록 지원하고 있으며, 산학협력단 내에 배정된 협약 담당자, 정산 담당자와의 협력을 통해 대학원생들이 연구에 매진할 수 있게 지원하고 있음
- 산학협력단에서 별도로 채용한 변리사를 통해 지식재산 권리화, 교육 및 기술사업 활성화를 시키고 있으며, 특허와 기술이전 그리고 사업화의 관리를 지원함으로써 대학원생들이 연구에 매진할 수 있게 지원하고 있음

▣ 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 부여
- 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 국제공동 연구가 진행될 수 있도록 지원할 계획임
- 항공 운임비 및 체류비는 본교 국외출장 기준을 적용하여 지급함
- 해외 교류를 통해 연구 결과물 혹은 해외 산업체의 업무 프로세스 경험을 얻을 수 있도록 진행함
- 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 동기부여

▶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 환

경을 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 통하여사회에서 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 위한각국의 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
- 성과평가 대상 기간(2020.09.01.~2024.02.29)동안 국제 저널 120건, 국제 학회 57건, 국내 저널 65편, 국내 학회 220건, 특허 출원 70건, 특허 등록 38건, 기술이전 32건의 실적을 달성함

▶ 국제저널

- 참여학생 김현기는 “Convolution Neural Network-Based Sensitive Security Parameter Identification and Analysis” 논문을 통해 잡음원들이 수집될 때 발생되는 정보들을 통해 그들을 식별할 수 있음을 나타냄. 난수 생성 중 암호모듈에 예측 불가능성을 제공하는 소스들을 수집하는 단계(stage)에서 잡음원들이 식별 가능하다면 그 데이터의 특성에 따라 미래의 값들을 예측이 가능해질 수 있기 때문에 임의의 암호모듈을 물리적으로 획득하였을 때, 학습된 모델로 암호모듈에서 사용하는 엔트로피 소스를 식별하여 난수를 분석할 수 있다는 공격 시나리오를 세움.
- 참여학생 박명서는 “A methodology for the decryption of encrypted smartphone backup data on android platform: A case study on the latest samsung smartphone backup system” 논문을 통해 안드로이드 플랫폼 상의 암호화된 스마트폰 백업 데이터의 해독 방법론을 소개하며, 특히 최신 삼성 스마트폰 백업 시스템을 case study로 방법론을 적용하고 증명함.

▶ 국내 저널

- 참여학생 김태완은 “양자 엔트로피 기반 난수 발생기를 이용한 드론 제어 데이터 보안 연구” 논문을 통해 현재 드론이 사용하고 있는 통신 프로토콜인 MAVLink 프로토콜의 취약점을 분석함. 결과 기밀성 및 인증에 대한 취약점이 밝혀내었으며, 이를 보완하기 위하여 양자 엔트로피 기반 난수발생기를 가상 드론환경에 적용시켜 기밀성과 인증을 제공하는 방법을 제시함.
- 참여학생 장찬국은 “5G+ 초연결 환경을 위한 암호기술 연구”논문을 통해 5G 이동통신 환경에서의 암호기술을 소개하고, 안전한 5G 이동통신과 이에 기반한 5G+ 응용환경에서의 초고속, 초저지연, 초연결 서비스를 위해 고려해야 하는 항목들을 제시함.

▶ 국제 학회

- 참여학생 정서우는 “Analysis of 5G AKA vulnerabilities through 5G Simulator” 논문을 통해 무선 구간에서의 5G 이동통신 보안을 제공하기 위한 5G AKA 취약점에 대해 분석하고, 모의 공격에 따른 결과와 해결 방안을 제시함.
- 참여학생 김태완은 “Analysis of Radioactive Decay Based Entropy Generator in the IoT Environments“ 논문을 통해 제한된 리소스로 인해 충분한 엔트로피를 수집하기 어려운 IoT 환경에서 α 기반 및 β 기반의 잡음원을 통한 엔트로피 발생기를 분석함.

▶ 국내 학회

- 참여학생 김태완은 “5G-AKA 및 SMC의 RAN 취약점 분석” 논문을 통해 5G 인증 프로토콜인 5G-AKA를 분석하고, 기존에 알려진 공격방법 중 허위 기지국을 통한 MitM 공격을 가상 시뮬레이션을 진행하였음. 결과, 암호화 알고리즘에 따라 기밀성에 대한 취약점이 존재한다는 것을 밝혔으며, 이동통신 세대별로 여전히 존재하는 취약점에 대해 안전성 확보가 필요함을 밝힘.
- 참여학생 이세윤은 “6G 보안을 위한 5G 코어 오픈소스 프로젝트 분석” 논문을 통해 5G 관련 오픈소스 프로젝트들이 5G 보안 표준을 준수하지 못함을 밝힘. 하지만, 이를 기반으로 5G 보안 취약점 해결방안 연구에 쓰일 수 있을 것이라는 점을 제안하였음. 마지막으로, 표준화될 6G 이동통신에서 안전한 보안 표준을 설계하기 위해 PQC를 이용한 이동통신 보안을 제시하였음.

2.3 참여대학원생의 취(창)업 현황

① 취(창)업률

<표 2-1> 평가 대상 기간(2020. 9. 1. ~ 2024. 2. 29.) 내 졸업한 참여대학원생 취(창)업률 실적

구 분		졸업 및 취(창)업 현황 (단위: 명)						취(창)업률(%) (D/C)×100
		졸업자 (A)	비취업자(B)			취(창)업대상자 (C=A-B)	취(창)업자 (D)	
			진학자		입대자			
			국내	국외				
2023년 2월 졸업자	석사	15	1	0	0	14	13	94
	박사	4			0	4	4	
2023년 8월 졸업자	석사	0	0	0	0	0	0	0
	박사	0			0	0	0	

② 취(창)업의 질적 우수성 (평가 대상 기간)

<표 2-2> 평가 대상 기간(2020. 9. 1. ~ 2024. 2. 29.) 내 졸업한 참여대학원생 중 취(창)업의 질적 우수성

연번	성명	졸업연월	수여 학위 (석사/박사)	학위취득 시 학과(부)명	현 직장(직위)
	대표 취(창)업 사례의 우수성				
1	박명서	2021.8	박사	금융정보보안학과	한성대학교 (교수)
	박사학위 취득 후 산학협력전담연구인력으로 강의 및 인력 양성에 기여함. 이후 강남대학교에 교수로 취임 후 2024년 한성대학교 교수로 취임함				
2	이세훈	2021.8	석사	금융정보보안학과	한국원자력연구원 (연구원)
	다양한 기기 및 OS의 데이터 및 통신 프로토콜을 분석한 성과를 바탕으로 한국 원자력 연구원에 취업함. 이후, 과거 연구 성과를 바탕으로 새롭게 떠오른 원자력 발전소의 드론 위협에 대한 대응을 위한 연구를 수행하고 있음.				
3	윤병철	2021.8	석사	금융정보보안학과	법무법인(유) 세종 (연구원)
	다양한 모바일 애플리케이션의 복호화 및 분석방안에 관하여 연구하였으며, 국내 5대 법률 사무소인 법무법인 세종에 취업함. 이후, 과거 연구 경험을 바탕으로 다양한 법률 분쟁에서 데이터 분석에 힘쓰고 있음.				
4	신수민	2022.2	석사	금융정보보안학과	국가보안기술연구소 (연구원)
	다양한 모바일 애플리케이션의 복호화 및 분석방안에 관하여 연구하였으며, 국가보안기술연구소에 취업함.				
5	박종현	2023.2	석사	금융정보보안학과	한국시스템보증 (연구원)
	암호 인증과 관련된 다양한 업무를 수행하였으며, 이를 기반으로 한국시스템보증에 취업함. 이후, 과거 연구 경험을 바탕으로 국내 다양한 기업 및 기관의 CC평가, 암호모듈 검증 등의 업무를 수행하고 있음.				
6	최용철	2023.2	석사	금융정보보안학과	INCA Internet (연구원)
	다양한 안티포렌식 애플리케이션의 데이터 은닉 기법에 대하여 연구를 수행하였으며, 국내 보안업체 INCA Internet에 취업함.				
7	김소람	2023.2	박사	금융정보보안학과	국가보안기술연구소 (연구원)
	다수의 랜섬웨어의 암호기능 분석을 연구하였으며, 국가보안기술 연구소에 취업함.				
8	김한기	2023.2	박사	금융정보보안학과	금융보안원 (연구원)
	국내 경량 암호 표준인 PIPO 암호 설계에 주도적으로 참여하였으며, 현재 금융보안원에 취업하여 다양한 금융 보안에 대한 연구를 수행 중임.				
9	박귀은	2024.2	석사	금융정보보안학과	김앤장 법률사무소 (연구원)
	다양한 모바일 애플리케이션의 복호화 및 분석방안에 관하여 연구하였으며, 국내 최대 법률 사무소인 김앤장 법률 사무소에 취업함. 이후, 과거 연구 경험을 바탕으로 다양한 법률 분쟁에서 데이터 분석에 힘쓰고 있음.				
10	이민정	2024.2	석사	금융정보보안학과	펜타시큐리티 (연구원)
	다양한 모바일 애플리케이션의 아티팩트 분석 연구를 수행하였으며, 교내에서 진행된 국내 보안업체 펜타시큐리티의 인턴쉽 참여 후 관련 성과를 인정받아 취업으로 연계함.				

11	전창열	2023.2	석사	금융정보보안학과	국민은행(대리)
	부호기반 양자내성 암호 분야에서의 깊이 있는 연구를 바탕으로 국민은행에 취업해 금융 서비스의 보안 솔루션 개발을 담당하고 있음. 이러한 전문성은 그가 금융 보안 산업에서 요구하는 높은 기술적 요구사항을 충족시키며, 취업 기관에 이상적인 인재상으로 자리매김하게 한 주요 요인임.				
12	오진혁	2021.2	석사	금융정보보안학과	펜타시큐리티(선임연구원)
	다양한 IoT 환경에서의 암호학적 보안 설계 및 기술 개발 연구를 기반으로 펜타시큐리티시스템에 취업하여 정보보안 국책 사업을 수행 중임.				
13	한주홍	2021.2	석사	금융정보보안학과	NAVER LINE(연구원)
	글로벌 메신저 플랫폼 기업인 LINE Plus에 취업하여 LINE의 암호 기술 고도화와 함께 보안 시스템 설계, 개발, 컨설팅 업무를 수행 중임.				
14	김현기	2023.2	박사	금융정보보안학과	현대오토에버(선임연구원)
	현대자동차그룹 계열 소프트웨어 전문 업체로 펌웨어 내의 암호모듈 수행 연구를 기반으로 In-Car와 Out-Car 영역 전반의 소프트웨어와 인프라를 안정적, 효율적, 혁신적으로 지원 컨설팅 서비스를 제공함.				
15	장찬국	2023.2	박사	금융정보보안학과	국민대학교(전임연구교수)
	이동 통신 보안 연구를 기반으로 국민대학교에 연구교수로 취업하여 이동통신 암호 기술 고도화와 함께 보안 시스템 설계, 개발을 수행 중임.				
16	김태완	2023.2	석사	금융정보보안학과	국방과학기술연구소(연구원)
	무이동 통신 보안과 방사선 동위 원소 기반의 양자 난수에 대한 연구 기반으로 국방력 강화와 자주국방 완수에 기여하는 국방과학연구소에 취업하여 국방에 필요한 무기 및 국방과학기술에 대한 기술적 조사, 연구, 개발 및 시험 등을 수행 중임.				
17	이세윤	2023.2	석사	금융정보보안학과	KT(대리)
	이동 통신 보안 및 양자 내성 암호에 관한 연구를 기반으로 KT에 취업하여 암호 기술 고도화와 함께 보안 시스템 설계, 개발 등의 연구를 수행 중임.				
18	정서우	2023.2	석사	금융정보보안학과	국군방첩사령부(주무관)
	군 보안 기술 개발 관련 업무 및 기타 군사 보안에 관한 지원 업무, 방첩 업무 등 군과 관련한 안보 업무를 수행 중임.				
19	위한샘	2024.2	박사	금융정보보안학과	국민대학교(전임연구교수)
	무인이동체 보안 연구를 기반으로 국민대학교에 연구교수로 취업하여 무인 이동체 내의 암호 기술 고도화와 함께 보안 시스템 설계, 개발 중임.				
20	박호중	2021.2	박사	금융정보보안학과	KT 연구개발센터(선임 연구원)
	양자난수발생기와 암호학적 난수발생기의 안전성에 관한 연구를 기반으로 KT 연구개발센터에 취업하여 양자통신 기술 및 양자네트워크 인프라 구축 개발 연구를 수행 중임.				
21	유현도	2024.2	석사	금융정보보안학과	현대자동차(연구원)
	암호학적 난수발생기의 설계 및 구현에 관한 연구를 기반으로 현대자동차에 취업하여 차량 보안기술 개발, 차량 제어기 보안 요구사양 개발, 제어기 보안 취약점 분석 및 대응 방안 수립 연구를 수행 중임.				
22	송진교	2022.2	석사	금융정보보안학과	LG U+ (연구원)
	다양한 양자내성암호 분석 및 임베디드 환경에서 최적화연구를 진행하였으며, 다양한 프로토콜로의 마이그레이션 연구를 진행하였고, LG U+에 취업함.				

23	안상우	2022.2	석사	금융정보보안학과	한국정보통신기술협회 (사원)
	다양한 양자내성암호 분석 및 그래픽장치에서 최적화연구를 진행하였고, 한국정보통신기술협회에 취업함.				
24	박한별	2021.2	석사	금융정보보안학과	한국정보통신(주임연구원)
	스마트 디바이스 취약성 분석 및 대응기법 개발 연구를 기반으로 한국정보통신에 취업하여 보안 강화된 신용카드 단말기 제품 개발 업무를 진행하고 있음.				
25	임한섭	2021.2	석사	금융정보보안학과	한국정보통신기술협회(선임연구원)
	인증 시스템 및 블록암호에 대한 전자파 오류주입 안전성 분석 연구를 기반으로 한국정보통신기술협회(TTA)에 취업하여 정보통신망 연결기기에 대한 정보보호 인증 시험 업무를 진행하고 있음.				
26	이태호	2022.2	석사	금융정보보안학과	한국정보통신기술협회(선임연구원)
	블록암호, 양자내성암호에 대한 부채널 안전성 분석 연구를 기반으로 한국정보통신기술협회(TTA)에 취업하여 정보통신망 연결기기에 대한 정보보호 인증 시험 업무를 진행하고 있음.				
27	임성혁	2022.2	석사	금융정보보안학과	국방부(7급군무원)
	블록암호의 전자파 오류주입 공격 및 대응 연구를 기반으로 국방부에 취업하여 군사보안, 국방 내의 암호 기술 고도화를 위한 보안 시스템 설계, 개발 등의 연구를 진행하고 있음.				
28	김수진	2023.2	석사	금융정보보안학과	국가보안기술연구소(연구원)
	소프트웨어, 하드웨어 구현된 양자 내성 암호 부채널 분석 안전성 연구를 기반으로 국가보안기술연구소에 취업하여 소프트웨어 보안 기술 연구 업무를 수행하고 있음.				
29	김연재	2023.2	석사	금융정보보안학과	LIG넥스원(연구원)
	소프트웨어, 하드웨어 구현된 블록 암호 부채널 분석 안전성 연구를 기반으로 LIG 넥스원에 취업하여 암호 장비의 전자파 취약점 분석 업무를 진행하고 있음.				
30	문혜원	2023.2	석사	금융정보보안학과	쿤텍(주)(매니저)
	소프트웨어 구현 암호가 탑재된 암호 장비의 안전성 분석 연구를 기반으로 쿤텍(주)에 취업하여 화이트박스 암호 구현 및 안전성 분석 업무를 진행하고 있음.				
31	안성현	2023.2	석사	금융정보보안학과	LIG넥스원(연구원)
	전자파 신호 처리 및 분석 연구를 기반으로 LIG 넥스원에 취업하여 드론에 대한 안전성 분석 업무를 진행하고 있음.				
32	우지은	2023.2	석사	금융정보보안학과	코나아이(사원)
	소프트웨어 구현 암호 부채널 분석 안전성 연구를 기반으로 코나아이에 취업하여 스마트 카드 암호 구현 업무를 진행하고 있음.				
33	델핀라즈	2022.2	박사	금융정보보안학과	중앙대학교(연구원)
	이동통신 정보 보안을 기반으로 중앙대학교 일반대학원 연구실 박사후 연구원으로 취업하여 자동차 통신 관련 정보 보안과 관련된 연구를 수행 중임.				

평가 대상 기간(2020. 9. 1. ~ 2024. 2. 29.) 내 졸업한 참여대학원생 수	**석사**	45	**제출 요구량**	1~6
	박사	9		

2.4 우수 신진연구인력 확보 및 지원 실적

<표 2-3> 교육연구단 신진연구인력 현황

구분	신진연구인력 수 (단위: 명, 개월)		
	평가 대상 기간 내 총 인원 수	총 참여 개월 수	1인당 평균 참여 개월 수
박사후 과정생	1	6	6
계약교수	3	88	29
계	4	94	24

① 우수 신진연구인력 확보 및 지원 실적

▣ 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+α>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
- 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
- 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

▣ 우수 신진연구인력 확보 및 지원을 위한 조직 체계 재설정

- 산학연구부총장: 대학원, 산학협력단, LINC+사업단, 그리고 창업지원단을 산학연구 부총장에게 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: 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

- 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

▣ 연구중심형 연구지원 체계 및 연구지원제도 개선 운영

▶산학협력단 운영

- 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 4개 부서로 조직을 운영함

▶연구지원제도 개선

- 연구역량강화 및 활성화를 위한 연구지원제도 개선 및 신규 제도 시행을 위해 아래와 같은 연구지원 제도를 마련하여 운영함
- 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 운영중
- 학술회의 지원금 기준을 신설함으로써 부설연구소의 학술회의 개최를 활성화 함
- 연구개발능률성과급 지급 지침, 교원의 연구 활동 독려 및 우수 연구성과 창출을 위한 성과급 지급 지침을 기준으로 매년 산학협력단 간접비에서 평가에 의해 차등 지급함
- 연구책임자 연구활동 지원금 제도, 연구자의 연구활동을 지원하기 위한 제도 운영중
- 교내 융복합 연구팀 구성을 위한 기획비 지원제도 운영중, 교내 구성원간의 융복합 연구 활성화를 위한 기획비 지원

▣ 연구몰입 환경 인프라 구축 및 제도 운영

▶연구지원 제도 운영

- 신진연구자의 연구몰입 환경 조성을 위한 인프라 구축 및 제도를 마련하여 시행하고 있음
- 연구실 및 부설연구소 행정인력 운영방안을 마련하여 국가연구개발사업 수행 연구책임자의 행정업무 부담을 최소화하기 위하여 행정인력 지원중
- 산학협력단 외부연구비 관리 매뉴얼 제공: 내·외부 각종 규정 및 서식을 한권으로 통합하여 연구자에게 연구비 신청의 편의성을 제공하고 있음
- 산학협력단 차세대 연구행정시스템 운영: 대학 차세대 시스템 개발과 연계하여 데이터간·업무간·시스템간 정보의 연결성 강화 및 연구자가 연구에만 전념할 수 있는 친 연구시스템 운영중

▶미래 지향적 지원체계 운영

- 대학의 혁신비전 및 중장기 발전계획 <KMU Vision 2030+α>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·연구·산학협력의 3대 영역별 혁신전략을 구체적으로 수립함
- 우수한 산업문제 해결을 위한 기술사업화를 위해 교원창업 및 기술사업 통합지원 플랫폼 구축하고 진로 및 취·창업 총괄기구인 "대학일자리본부" 운영중, 진로지도 및 취·창업 지원의 One-stop 서비스와 기능적 연계 등을 위해 경력개발지원단과 총장직속 기구인 창업지원단을 총괄하는 대학일자리본부를 운영하여 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 격려함
- 국민대학교는 매년 본 교육연구단의 업무를 전담하는 행정직원을 지원하며, 이를 통해 본 교육연구단의 교원과 재학생들이 행정업무에 얽매이지 않고, 자유롭게 연구에 집중할 수 있도록 운영함
- 국민대학교는 신진연구인력이 우수한 신입생을 적극 유치할 수 있도록 성곡장학금(수업료전액), 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

② 우수 신진연구인력의 대표 연구 실적

<표 2-4> 평가 대상 기간(2020. 9. 1. ~ 2024. 2. 29.) 내 신진연구인력 대표 연구 실적

<table>
<tr><th rowspan="2">연번</th><th>구분</th><th>성명</th><th>참여
시작일</th><th>실적 종류</th><th>대표 연구 실적 상세내용</th></tr>
<tr><th colspan="5">대표 연구 실적의 우수성</th></tr>
<tr><td rowspan="9">1</td><td rowspan="8">연구교수</td><td rowspan="8">박명서</td><td rowspan="8">2021.9.1.</td><td rowspan="8">학술지 논문</td><td>① Soojin Kang, Giyoon Kim, Myungseo Park, Jongsung Kim</td></tr>
<tr><td>② Methods for decrypting the data encrypted by the latest Samsung smartphone backup programs in Windows and macOS</td></tr>
<tr><td>③ Forensic Science International: Digital Investigation</td></tr>
<tr><td>④ 39, 301310</td></tr>
<tr><td>⑤ 2666-2825</td></tr>
<tr><td>⑥ 2021</td></tr>
<tr><td>⑦ https://doi.org/10.1016/j.fsidi.2021.301310</td></tr>
<tr><td colspan="5">본 연구는 삼성 스마트폰의 최신 백업 프로그램이 사용하는 암호화 기술에 대한 해석과 그 데이터를 Windows 및 macOS 환경에서 복호화하는 방법을 제시함. 각 운영체제에서 삼성 스마트폰의 백업 프로그램의 암호화 프로세스를 상세히 설명하고 해당 프로그램이 사용하는 암호화 키 생성 과정과 암호화 과정을 분석함. 이를 통해 생성된 암호화된 데이터를 복호화하기 위해 필요한 데이터와 절차를 상세적으로 기술함. 삼성 스마트폰의 백업 프로그램은 많은 사용자들이 이용하고 있으며, 이러한 사용자들의 디지털 활동 내역은 디지털 포렌식 수사에서 중요한 역할을 할 수 있음. 따라서 이 연구는 디지털 범죄 수사 및 포렌식 분야에서의 실질적인 가치를 지님. 더불어 암호화 기술과 디지털 보안 분야에서의 기술적인 이해를 높이고, 암호 해독 및 보안 취약점 해결에 대한 방법론을 개발하는 데 기여함.</td></tr>
<tr><td colspan="2" rowspan="3">총 신진연구인력 수</td><td>박사후과정생</td><td>1</td><td rowspan="3">제출 요구량</td><td rowspan="3">1~2</td></tr>
<tr><td>계약교수</td><td>3</td></tr>
<tr><td>계</td><td>4</td></tr>
</table>

3. 참여대학원생 연구역량

3.1 참여대학원생 연구 실적의 우수성

① 참여대학원생 대표연구업적물의 우수성

<표 2-5> 평가 대상 기간(2020. 9. 1. ~ 2024. 2. 29.) 내 참여대학원생 대표연구업적물

<table>
<tr><th rowspan="2">연번</th><th>학위과정
(석사/박사/
석박사통합)</th><th>참여대학원생
성명</th><th>지도교수
세부전공분
야</th><th>업적물
종류</th><th>대표연구업적물 상세내용</th></tr>
<tr><td colspan="5">대표연구업적물의 우수성</td></tr>
<tr><td rowspan="9">1</td><td rowspan="8">박사</td><td rowspan="8">김한기</td><td rowspan="8">암호학,
디지털포렌
식</td><td rowspan="8">학술지
논문</td><td>① 김한기, 전용진, 김기윤, 김종성, 심보연, 한동국, 서화정, 김성겸, 홍석희, 성재철, 홍득조</td></tr>
<tr><td>② A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application</td></tr>
<tr><td>③ IEEE ACCESS</td></tr>
<tr><td>④ Volume 9, pp. 150592--150607</td></tr>
<tr><td>⑤ 2169-3536</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2021</td></tr>
<tr><td>⑧ 10.1109/ACCESS.2021.3126008</td></tr>
<tr><td colspan="5">해당 논문은 메모리나 전력이 부족한 경량 환경에서 구현하기 적합한 새로운 경량블록암호 PIPO를 제안함. PIPO는 같은 파라미터를 갖는 경량블록암호 중에서 가장 효율적이며, 부채널 대응 기법에도 효율적으로 개발됨. 일반적인 부채널 대응 기법은 경량블록암호의 성능을 크게 저하해 경량의 의미를 퇴색시킴. 그러나, PIPO는 주요 프리미티브로 적은 양의 비선형 연산자를 갖는 8-bit S-box를 사용하여 효율적인 부채널 대응 기법을 적용할 수 있게 함. 또한, 8-bit S-box를 확장구조로 생성하여 DLBN 3이라는 특정한 성질을 갖게 만들어, 단순 로테이션 연산의 추가만으로 적은 라운드에도 안전한 구조가 되었음. PIPO는 현재 TTA 표준에 등록되어있으며, 기밀성 제공이 필요한 다양한 정보보호 환경에서 활용할 수 있음. 국제적인 성능의 경량블록암호의 제안을 통해 우리나라 대칭키 암호에 대한 과학기술력을 향상시키는 것에 큰 기여를 하였음.</td></tr>
</table>

<table>
<tr><td rowspan="2">2</td><td>박사</td><td>강수진</td><td>암호학,
디지털포렌식</td><td>학술지
논문</td><td>① 김기윤, 김소람, 강수진, 김종성</td></tr>
<tr><td colspan="5">② A method for decrypting data infected with Hive ransomware
③ Journal of Information Security and Applications
④ vol. 71, 103387
⑤ 2214-2126
⑥
⑦ 2022
⑧ 10.1016/j.jisa.2022.103387</td></tr>
<tr><td colspan="6">본 논문에서는 전 세계적으로 큰 위협이된 HIVE 랜섬웨어의 취약점을 분석하고 전세계 최초로 복호화 방안을 제시함. 랜섬웨어는 가장 큰 사이버 보안 위협 중 하나로, 피해자의 파일을 암호화하고 복호화를 대가로 금전을 요구하는 악성 소프트웨어임. 이 과정에서 기업과 개인은 막대한 금전적 손실과 중요 데이터의 상실이 일어나기도 함. 일반적으로 랜섬웨어는 대칭키 암호와 공개키 암호를 사용하는 하이브리드 암호화 시스템을 활용함. 대칭키 암호로 데이터를 빠르게 암호화하고 공개키 암호를 이용해 대칭키 암호의 암호키를 암호화하는 경우 공격자의 개인키 없이는 데이터의 복호화가 어려움. HIVE 랜섬웨어는 잘 알려진 암호알고리즘이 아닌 자체 개발한 암호알고리즘을 사용하였음. 본 논문에서는 자체 개발된 암호알고리즘의 취약점을 분석하여 암호화된 파일중 95% 이상이 복호화가 가능함을 보임. 이를 통해 전 세계적으로 큰 피해를 일으킨 HIVE 랜섬웨어에 피해자들이 몸값을 지불하지 않고도 자신의 파일을 복구할 수 있는 길을 제시하였으며, 랜섬웨어 공격자들에게 흐르는 자금을 차단하고, 사이버 보안 커뮤니티에 랜섬웨어 대응 방안을 제공하였다는 점에서 큰 기여를 하였음.</td></tr>
<tr><td rowspan="2">3</td><td>박사</td><td>백승준</td><td>암호학,
디지털포렌식</td><td>학술지
논문</td><td>① 백승준, 조세희, 김종성</td></tr>
<tr><td colspan="5">② Quantum cryptanalysis of the full AES-256-based Davies-Meyer, Hirose and MJH hash functions
③ Quantum Information Processing
④ vol. 21, 163
⑤ 1573-1332
⑥
⑦ 2022
⑧ 10.1007/s11128-022-03499-5</td></tr>
<tr><td colspan="6">양자 컴퓨터는 매우 빠르게 발전하고 있으며, 이는 현존하는 암호 체계의 안전성이 새로운 관점에서 다시 검증되어야 한다는 점을 보여줌. 대칭키 기반의 암호에서는 AES 알고리즘이 세계적으로 가장 많이 쓰이는데, 사물 인터넷(IoT) 환경에서의 작은 기기들에서는 AES를 기반으로 한 해시함수를 사용하는 것이 효율성 관점에서 의미가 있음. 본 논문에서는 미래에 도래하게 될 양자 환경들에서 전체 라운드 AES-256 기반 Davies-Meyer, Hirose, MJH 해시함수에 대한 충돌쌍 공격을 수행함. 기존 축소 라운드 AES-256에 대한 해당 해시함수들은 분석된 바가 있으나, 높은 공격 복잡도 때문에 전체 라운드에 대한 공격이 이루어진 적은 없었음. 논문에서는 자유 변수 기술을 기반으로 한 새로운 선택키 차분 경로를 제시하였고, 이를 통해 전체 라운드 AES-256 기반 해시 함수들을 공격하는 데 성공함. 이 공격들은 양자 컴퓨터에서 구동 가능한 Grover’s algorithm을 차분 경로에 적용함으로써 성공할 수 있으며, 논문에서는 이에 대한 상세한 복잡도 분석을 제시함. 이를 통해 본 논문은 대칭키 암호 분야의 양자 보안 향상에 이바지함.</td></tr>
</table>

<table>
<tr><td rowspan="9">4</td><td rowspan="8">박사</td><td rowspan="8">박명서</td><td rowspan="8">암호학,
디지털포렌식</td><td rowspan="8">학술지
논문</td><td>① Uk Hur, Myungseo Park, Jongsung Kim</td></tr>
<tr><td>② A reused key attack on an encrypted mobile app database: Case study on KakaoTalk and ProtonMail</td></tr>
<tr><td>③ Journal of Information Security and Applications</td></tr>
<tr><td>④ Volume 67, 103181</td></tr>
<tr><td>⑤ 2214-2126</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2022</td></tr>
<tr><td>⑧ 10.1016/j.jisa.2022.103181</td></tr>
<tr><td colspan="5">스트림 암호와 CTR 및 OFB 모드를 사용하는 블록암호는 동일한 Key와 IV가 재사용된 경우 동일한 키스트림의 XOR로 데이터를 암호화함. 따라서, Key와 IV가 재사용된 암호문 데이터와 평문 데이터를 동시에 획득할 수 있다면 키스트림을 복구할 수 있음. 이후 복구된 키스트림과 나머지 암호문을 XOR 연산하면 데이터를 복호화할 수 있음. 본 논문에서는 보안 이메일 서비스인 ProtonMail의 iOS 앱 데이터와 KakaoTalk 메신저의 백업데이터를 키 재사용 공격을 통해 복호화하고 분석하는 방법에 대하여 제시함. 제안된 방법은 기기에서 제공하는 보안 기능과 사용자가 입력한 패스워드 획득 없이 데이터 복호화가 가능하였으며, 데이터 구조 분석을 함께 수행하여 평문을 획득할 수 없는 경우의 키스트림 복구 방법을 함께 제시함.</td></tr>
<tr><td rowspan="9">5</td><td rowspan="8">박사</td><td rowspan="8">전용진</td><td rowspan="8">암호학,
디지털포렌식</td><td rowspan="8">학술지
논문</td><td>① Yongjin Jeon, Seungjun Baek, Hangi Kim, Giyoon Kim, and Jongsung Kim</td></tr>
<tr><td>② Differential Uniformity and Linearity of S-Boxes by Multiplicative Complexity</td></tr>
<tr><td>③ Cryptography and Communications</td></tr>
<tr><td>④ Volume 14, pp. 849--874</td></tr>
<tr><td>⑤ 1936-2447 / 1936-2455</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2022</td></tr>
<tr><td>⑧ 10.1007/s12095-021-00547-2</td></tr>
<tr><td colspan="5">해당 논문은 전자회로의 효율성과 암호 주요 프리미티브 S-box의 대표적인 안전성 간의 관계를 분석한 논문임. 암호는 효율성과 안전성 간의 trade-off가 있으며, 효율적인 통신을 위해 이에 대한 분석이 요구됨. 해당 논문에서 분석한 multiplicative complexity (MC)는 그 중에서도 밝히기 어려운 성질이며, 특수한 S-box라고 볼 수 있는 Boolean function에 대해서도 다항 시간안에 계산할 수 없음이 증명되어있음. S-box는 다수의 Boolean function이 통합된 구조를 가지며, 대표적인 안전성 지표로 differential uniformity와 linearity를 가짐. 해당 논문에서는 MC와 S-box의 안전성 관계를 이론적으로 규명하고 실존하는 S-box를 통해 확인하여 표로 제시하였음. 그러므로 해당 논문은 암호 설계자에게 이론적 토대를 만들어 주고, 무의미한 계산을 줄이는 것으로 암호 설계 연구에 기여함.</td></tr>
</table>

<table>
<tr><td rowspan="9">6</td><td rowspan="8">석박사통합
과정</td><td rowspan="8">김기윤</td><td rowspan="8">암호학,
디지털포렌
식</td><td rowspan="8">학술지
논문</td><td>① 김기윤, 강수진, 허욱, 김종성</td></tr>
<tr><td>② A Study on Vulnerability of the Wickr Login System in Windows from a Live Forensics Perspective</td></tr>
<tr><td>③ Computers & Security</td></tr>
<tr><td>④ vol. 139, 103672</td></tr>
<tr><td>⑤ 1872-6208</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2023</td></tr>
<tr><td>⑧ https://doi.org/10.1016/j.cose.2023.103672</td></tr>
<tr><td colspan="6">보안 메신저 Wickr는 고강도의 안전성을 자랑함. 디지털포렌식 수사관점에서 메신저는 다양한 사용자 정보를 보관하는 애플리케이션으로 주요 분석 대상 중 하나임. 그러나 높은 안전성을 갖는 보안 메신저는 디지털포렌식 수사 관점에서 안티포렌식으로 작용하기도 함. 이로인해 보안 메신저가 범죄에 악용된 경우 수사관은 주요 증거 확보가 어려워짐. 본 논문에서는 Wickr의 동작과정을 상세하게 분석하고 다양한 시나리오를 제시하여 디지털포렌식 수사관이 데이터를 수집할 수 있는 방안을 제시함. 그리고 분석된 결과를 토대로 사용자 인증 없이 패스워드를 변경하는 취약점을 밝혀내 다양한 증거자료를 수집할 수 있게 함. Wickr는 실제로 범죄에도 많이 악용되는 보안메신저이기에 해당 메신저의 데이터를 수집할 수 있게 한 본 논문은 디지털포렌식 수사 관점에서 큰 기여를 하였음.</td></tr>
<tr><td rowspan="9">7</td><td rowspan="8">석사</td><td rowspan="8">이세훈</td><td rowspan="8">암호학,
디지털포렌
식</td><td rowspan="8">학술지
논문</td><td>① Sehoon Lee, Myungseo Park, and Jongsung Kim</td></tr>
<tr><td>② Magniber v2 Ransomware Decryption: Exploiting the Vulnerability of a Self-Developed Pseudo Random Number Generator</td></tr>
<tr><td>③ Electronics</td></tr>
<tr><td>④ Vol. 10</td></tr>
<tr><td>⑤ 2079-9292</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2021</td></tr>
<tr><td>⑧ https://doi.org/10.3390/electronics10010016</td></tr>
<tr><td colspan="6">해당 논문은 아시아 지역에 큰 영향을 미친 Magniber v2를 분석하여 상세한 동작과정을 밝히고, 암호화키 생성에 사용되는 의사난수생성기의 취약점을 밝힘. 발견한 의사난수생성기의 취약점을 이용하여 실제로 암호화키 복구에 성공하였으며, 이를 패딩 검증과 통계적 검증을 수행하여 성공적으로 암호키를 복구하였음을 증명함. 특히, 이 결과는 최초로 Magniver v2의 감염된 파일의 복구 성공 결과이며, 이를 통해 랜섬웨어에 감염된 피해자들의 피해 감소에 기여하였음. 또한, 동일한 취약점이 포함된 의사난수생성기를 이용한 랜섬웨어에 감염된 파일은 본 논문에서 제안한 방법을 이용하여 복호화가 가능할 수 있음을 제시함으로써 향후 랜섬웨어 피해를 줄이는데 기여함.</td></tr>
</table>

<table>
<tr><td rowspan="9">8</td><td rowspan="8">박사</td><td rowspan="8">김소람</td><td rowspan="8">암호학,
디지털포렌식</td><td rowspan="8">학술지
논문</td><td>① Soram Kim, Giyoon Kim, Sumin Shin, Byungchul Youn, Jian Song, Insoo Lee, JongsungKim</td></tr>
<tr><td>② Methods for recovering deleted data from the Realm database: Case study on Minitalk and Xabber</td></tr>
<tr><td>③ Forensic Science International: Digital Investigation</td></tr>
<tr><td>④ Vol. 40, 301353</td></tr>
<tr><td>⑤ 2666-2817</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2022</td></tr>
<tr><td>⑧ https://doi.org/10.1016/j.fsidi.2022.301353</td></tr>
<tr><td colspan="6">해당 논문은 모바일 기기에 최적화된 데이터베이스인 Realm 데이터베이스의 구조와 다양한 삭제 기능을 분석하였음. Realm DB의 데이터 구조를 분석하고 4가지 삭제 기능의 동작 및 특징을 분석한 결과를 제시함. 이를 통해 테이블 단위, 컬럼 단위, 필드 단위의 세 가지 관점에서 할당되지 않은 영역에서 삭제된 데이터를 복구하는 방법을 제안하였음. 복구 테스트를 수행하기 위한 PoC 코드를 개발하고 시나리오를 구성하여 샘플 앱과 실제 앱인 MiniTalk 및 Xabber에 적용하였음. 이를 통해 삭제된 데이터를 복구하여 추가 데이터를 획득할 수 있음을 보임. 이는 디지털 포렌식 수사에 활용될 수 있음.</td></tr>
<tr><td rowspan="9">9</td><td rowspan="8">박사</td><td rowspan="8">허욱</td><td rowspan="8">암호학,
디지털포렌식</td><td rowspan="8">논문</td><td>① Uk Hur, Giyoon Kim, Soojin Kang, Jongsung Kim</td></tr>
<tr><td>② Forensic analysis for multi-platform Cisco Webex</td></tr>
<tr><td>③ Forensic Science International: Digital Investigation</td></tr>
<tr><td>④ Vol. 47</td></tr>
<tr><td>⑤ 2666-2817</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2023</td></tr>
<tr><td>⑧ https://doi.org/10.1016/j.fsidi.2023.301659</td></tr>
<tr><td colspan="6">해당 논문은 Windows, macOS, iOS, Android 환경 에서 널리 사용되는 화상회의 및 협업 애플리케이션인 Cisco Webex의 데이터 분석하고 데이터 보호 API로 보호되는 데이터를 해제하는 방법과 암호화된 Webex 사용자 데이터를 해독하는 방법을 제안함. 연구를 통해 복호화된 데이터에는 사용자 데이터의 대부분이 포함되어 있음을 밝히고 이를 분석하여 삭제된 메시지를 복구할 수 있는 방법을 제안함. 복호화된 데이터를 활용하여 디바이스에 저장된 자격 증명 데이터를 마이그레이션함으로써 클라우드 데이터를 획득하는 방법을 제안함. 논문에서 제안된 마이그레이션 방법은 유사한 방식으로 자격 증명을 활용하는 다른 애플리케이션에서 사용될 수 있도록 제안하였으며, 이 결과는 디지털 포렌식 수사에 유용하게 사용될 수 있을 것으로 기대함.</td></tr>
</table>

<table>
<tr><td rowspan="9">10</td><td rowspan="8">석사</td><td rowspan="8">전창열</td><td rowspan="8">암호학</td><td rowspan="8">학술지
논문</td><td>① Dong-Chan Kim, Chang-Yeol Jeon, Yeonghyo Kim, and Minji Kim</td></tr>
<tr><td>② PALOMA: Binary Separable Goppa-Based KEM</td></tr>
<tr><td>③ CBCrypto2023</td></tr>
<tr><td>④ 1, pp. 144--173</td></tr>
<tr><td>⑤ 0302-9743/978-3-031-46495-9/1611-3349</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2023</td></tr>
<tr><td>⑧ 10.1007/978-3-031-46495-9_8</td></tr>
<tr><td colspan="6">현재 암호학의 시급한 과제 중 하나는 양자 컴퓨터에 대응할 수 있는 양자내성암호(PQC)의 개발임. 이에 대응하여, 본 학생은 부호 기반 PQC인 PALOMA 알고리즘을 개발하였으며, 이의 우수성은 국제 부호 기반 학회 CBCrypto에 채택되어 인정받았음. 더불어, 한국양자내성암호연구단 주관 양자내성암호 공모전의 2라운드에도 진출함으로써, 양자 컴퓨팅 시대를 대비하는 한국의 기술력과 국가 경쟁력 강화에 기여할 것으로 기대됨. 본 연구의 성과는 양자 컴퓨터에 대응하는 암호기술의 필수성을 강조하며, 양자 시대를 선도할 핵심 기술로서의 잠재력을 확인시켜 줌.</td></tr>
<tr><td rowspan="9">11</td><td rowspan="8">박사</td><td rowspan="8">고용호</td><td rowspan="8">정보보호</td><td rowspan="8">학술지
논문</td><td>① H Park, PVB Astillo, Y Ko, Y Park, T Kim, I You</td></tr>
<tr><td>② SMDFbs: Specification-Based Misbehavior Detection for False base Stations</td></tr>
<tr><td>③ Sensors</td></tr>
<tr><td>④ 23(23), 9504</td></tr>
<tr><td>⑤ 1424-8220</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2023</td></tr>
<tr><td>⑧ 10.3390/s23239504</td></tr>
<tr><td colspan="6">셀룰러 통신 기술의 발전은 인간의 삶을 깊이 있게 변화시켰음. 사람들은 이제 언제 어디서나 고화질 동영상을 시청하고 고급 자율 주행을 활용할 수 있게 되었음. 그러나 이러한 환경의 지속 가능성은 가짜 기지국에 의해 위협을 받고 있음. 가짜 기지국은 셀룰러 시스템의 무선 접속 네트워크 (RAN)에서 공격을 실행하여 네트워크나 사용자에게 해를 끼침. 이러한 도전 과제를 해결하기 위해 우리는 행동 규칙 명세를 기반으로 한 가짜 기지국 탐지 시스템인 SMDFbs를 제안하였음. 우리는 기지국의 정상 작동에서 행동 규칙을 유도하고 이러한 규칙을 상태 기계로 변환함. 이 상태 기계를 기반으로 네트워크 이상을 감지하고 위협을 대응하였음. 우리는 5G RAN 시뮬레이터에서 가짜 기지국을 탐지하는 실험을 실시하여 우리의 시스템을 일곱 가지 기계 학습 기반 탐지 기술과 비교하였음. 실험 결과는 우리가 제안한 시스템이 98%의 탐지 정확도를 달성하고 다른 알고리즘과 비교하여 더 낮은 오버헤드를 보였음.</td></tr>
</table>

<table>
<tr><td rowspan="9">12</td><td rowspan="8">석사</td><td rowspan="8">김건우</td><td rowspan="8">정보보호</td><td rowspan="8">학술지
논문</td><td>① I You, G Kim, S Shin, H Kwon, J Kim, J Baek</td></tr>
<tr><td>② 5G-AKA-FS: A 5G Authentication and Key Agreement Protocol for Forward Secrecy</td></tr>
<tr><td>③ Sensors</td></tr>
<tr><td>④ 24(1), 159</td></tr>
<tr><td>⑤ 1424-8220</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2023</td></tr>
<tr><td>⑧ 10.3390/s24010159</td></tr>
<tr><td colspan="5">5G의 적용 범위가 넓어짐에 따라 프로토콜 단계에서 순방향 비밀성을 지원하고 보안 공격에 대응하는 것이 중요함. 이에 대응하여, 여러 프로토콜이 이러한 보안 도전 과제를 완화하기 위해 제안됨. 그러나 기존에 제안된 프로토콜들은 순방향 비밀을 완벽하게 보장하는 데에 한계를 겪었음. 이에 영감을 받아, 5G-AKA를 개선하여 순방향 비밀성 지원을 달성하고 연결성 공격을 무력화하는 프로토콜(5G-AKA-FS)을 제시하였음. 5G-AKA-FS에서 홈 네트워크 (HN)는 정적 ECIES 키 쌍을 사용하는 대신, 견고한 세션 키 협상을 통해 순방향 비밀성을 지원함. 5G-AKA-FS가 안전하다는 것을 철저하고 정확하게 증명하기 위해 BAN 논리와 ProVerif를 적용하여 형식적인 보안 검증을 수행했음. 결과적으로 5G-AKA-FS가 유효함을 입증하였고, 프로토콜 성능 비교를 통해 통신 및 컴퓨팅 파워가 효율적임을 확인했음. 종합적으로 해당 분석은 본 프로토콜이 보안과 효율성 사이의 효과적인 균형을 이루는 것을 보였음.</td></tr>
<tr><td rowspan="9">13</td><td rowspan="8">석사</td><td rowspan="8">오종민</td><td rowspan="8">정보보호</td><td rowspan="8">학술지
논문</td><td>① J Kim, J Oh, D Son, H Kwon, PV Astillo, I You</td></tr>
<tr><td>② APSec1.0: Innovative Security Protocol Design with Formal Security Analysis for the Artificial Pancreas System</td></tr>
<tr><td>③ Sensors</td></tr>
<tr><td>④ 23(12), 5501</td></tr>
<tr><td>⑤ 1424-8220</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2023</td></tr>
<tr><td>⑧ 10.3390/s23125501</td></tr>
<tr><td colspan="5">의료 사물인터넷기기 (MIoT)은 환자에게 의료를 제공하는 혁신적인 방법을 개발되어 왔음. 증가하는 수요를 보여주는 한 예는 제 1형 당뇨병 환자에게 편의와 신뢰할 수 있는 지원을 제공하는 인공 췌장 시스템임. 이러한 시스템의 명백한 혜택에도 불구하고, 잠재적인 사이버 위협을 피할 수 없었음. 이러한 보안 위험은 환자의 개인 정보를 보호하고 안전한 기능을 유지하는 것이 필요하다. 이에 영감을 받아, 우리는 APS 환경을 위한 보안 프로토콜을 제안하였음. 본 프로토콜은 필수 보안 요구 사항을 지원하고, 보안 컨텍스트 협상이 리소스 친화적이며, 비상 상황에 견고한 프로토콜임. 따라서 BAN 논리 및 AVISPA를 사용하여 보안 요구 사항과 설계 프로토콜의 정확성을 형식적으로 검증했으며, 상업용 장치를 사용하여 제어 환경에서 APS를 에뮬레이션하여 그 실행 가능성을 입증하였음. 또한, 성능 분석을 통해 제안된 프로토콜이 다른 기존 연구 및 표준보다 효율적임을 보였음.</td></tr>
</table>

<table>
<tr><td rowspan="9">14</td><td rowspan="8">박사</td><td rowspan="8">위한샘</td><td rowspan="8">정보보안</td><td rowspan="8">학술지
논문</td><td>① Hansaem Wi, Seyoon Lee, Okyeon Yi</td></tr>
<tr><td>② DIM-Based Random Number Generation Using Quantum Noise Resources</td></tr>
<tr><td>③ Wireless Communications and Mobile Computing</td></tr>
<tr><td>④ 1-12</td></tr>
<tr><td>⑤ 1530-8669</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2022</td></tr>
<tr><td>⑧ https://doi.org/10.1155/2022/8984789</td></tr>
<tr><td colspan="5">드론 신원 모듈(DIM)에서 사용되는 난수의 필요성을 설명하고, 드론 기반 연구에서 사용된 난수 생성기를 분석하며, 기존 드론 시스템에서 활용 가능한 소음 자원 생성 장치의 특성을 분석함. 특히, 기존 방법의 한계를 극복하고자 DIM에서 양자 소음 자원을 이용한 난수 생성 방법을 제안함. 이를 위해 물리적 사양의 소음 자원 생성 장치, DIM 프로토타입 및 기존 드론 시스템에서의 양자 소음 자원 발생기에 대한 분석을 수행함. 또한, 양자 난수 생성기에서 수집한 데이터를 이용한 NIST 800-90B 엔트로피 측정 결과를 제시하여 제안하는 방법의 우수성을 입증함. 이 연구는 향후 드론의 통합 관리 및 안전한 정보 교환을 위한 기술적 기반을 마련하며, 양자 기술을 활용한 보안 강화에 중요한 기여함.</td></tr>
<tr><td rowspan="9">15</td><td rowspan="8">박사</td><td rowspan="8">김현기</td><td rowspan="8">정보보안</td><td rowspan="8">학술지
논문</td><td>① Hyunki Kim, Donghyun Kim, Okyeon Yi</td></tr>
<tr><td>② Convolution Neural Network-Based Sensitive Security Parameter Identification and Analysis</td></tr>
<tr><td>③ Wireless Communications and Mobile Computing</td></tr>
<tr><td>④ 1-13</td></tr>
<tr><td>⑤ 1530-8669</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2022</td></tr>
<tr><td>⑧ https://doi.org/10.1155/2022/9584894</td></tr>
<tr><td colspan="5">암호학적 난수 생성기의 작동 과정을 엔트로피 수집 단계와 의사 난수 생성 단계로 나누어 설명함. 특히, 엔트로피 원을 구성하는 데 사용되는 소음 자원의 안전한 수집이 암호화의 안전성을 보장하는 데 중요하다고 강조하였음. 소음 자원이 예측 불가능성을 제공하는 자원을 수집하는 단계에서 식별될 수 있다면, 미래의 값들을 예측할 수 있어 암호 시스템의 보안이 취약해질 수 있음. 연구팀은 합성곱 신경망 모델을 이용하여 엔트로피 원으로 사용되는 소음 자원을 식별하고, 이를 통해 암호 모듈이 무작위로 획득되었을 때 난수를 분석할 수 있는 공격 시나리오를 설정하였음. 이 연구는 암호학적 난수 생성 과정의 취약점을 식별하고 이를 통해 보안을 강화할 수 있는 방안을 제시함으로써 암호화 기술의 발전에 기여함. 이는 암호화된 데이터의 보안을 위협할 수 있는 잠재적 위험을 줄이는 데 중요한 역할을 함.</td></tr>
</table>

<table>
<tr><td rowspan="9">16</td><td rowspan="8">박사</td><td rowspan="8">김예원</td><td rowspan="8">암호학</td><td rowspan="8">학술지
논문</td><td>① Yewon Kim, Yongjin Yeom</td></tr>
<tr><td>② Accelerated implementation for testing IID assumption of NIST SP 800-90B using GPU</td></tr>
<tr><td>③ PeerJ Computer Science</td></tr>
<tr><td>④ 7</td></tr>
<tr><td>⑤ 2376-5992</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2021</td></tr>
<tr><td>⑧ 10.7717/peerj-cs.404</td></tr>
<tr><td colspan="5">암호 시스템 및 암호 모듈에서 난수 생성기(RNG)의 입력으로 사용되는 잡음원의 엔트로피가 충분하지 않은 경우, 개인 키 공격과 같은 심각한 피해를 입을 수 있음. 따라서 잡음원의 엔트로피를 가능한 정확히 추정하는 것이 필요함. 국립 표준 기술 연구소(NIST)는 RNG의 입력이 되는 잡음원의 엔트로피 추정 방법을 설명하는 표준 문서로 특별 간행물(Special Publication, SP) 800-90B를 발행함. NIST는 SP 800-90B의 엔트로피 추정 과정을 실행하기 위한 두 프로그램을 제공하는데, 이는 Python과 C++로 구현됨. 두 프로그램의 동작은 한 시간 이상 소요지만, RNG의 보안을 분석하기 위해서는 엔트로피 추정 프로그램을 여러 번 실행해야 하므로 NIST 프로그램은 성능 개선이 필요함. 본 논문에서는 엔트로피 추정의 가장 시간이 많이 소요되는 부분인 독립항등분포(IID) 가정 검증 과정의 GPU 기반 병렬 구현을 제안함. 또한 GPU 구현 시험 항목에 대한 실험 결과를 통해 제안한 방법이 NIST 패키지보다 약 3에서 25배 빠름을 보임.</td></tr>
<tr><td rowspan="9">17</td><td rowspan="8">박사</td><td rowspan="8">박호중</td><td rowspan="8">암호학</td><td rowspan="8">학술지
논문</td><td>① Hojoong Park, Yongjin Yeom, and Ju-Sung Kang</td></tr>
<tr><td>② Mutual entity authentication of quantum key distribution network system using authentication qubits</td></tr>
<tr><td>③ EPJ Quantum Technology</td></tr>
<tr><td>④ 10(48), 1-16</td></tr>
<tr><td>⑤ 2196-0763</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2023</td></tr>
<tr><td>⑧ 10.1140/epjqt/s40507-023-00205-x</td></tr>
<tr><td colspan="5">엔티티 인증은 안전한 양자 통신을 보장하기 위하여 기밀 정보를 전송하기 전 참여자의 신원을 확인함. 본 논문은 인증 큐비트(pubit)를 사용하는 양자 키 분배(QKD) 네트워크 시스템을 위한 실용적인 엔티티 인증 프로토콜을 제안함. 이 프로토콜은 사전에 공유된 정보로 인코딩된 인증 큐비트를 생성하고 이를 교환하여 각 엔티티의 정당성(legitimacy)을 검증함. 참여자는 인증 큐비트를 사용함으로써 양자 채널을 통해 향상된 보안 수준으로 서로를 식별할 수 있게 됨. 나아가 제안 프로토콜은 추가 하드웨어 없이 기존 QKD 시스템과 쉽게 통합될 수 있음. 본 연구에서는 1xN QKD 네트워크 시스템을 사용하여 제안 방식의 효율성을 시연하고, 구축된 광 통신(fiber network)에서 동작의 안전성을 확인함. 또한, 본 논문은 제안한 엔티티 인증 프로토콜과 아키텍처의 보안 분석을 제공함.</td></tr>
</table>

<table>
<tr><td rowspan="9">18</td><td rowspan="8">석사</td><td rowspan="8">류지은</td><td rowspan="8">암호학</td><td rowspan="8">학술지
논문</td><td>① Hojoong Park</td></tr>
<tr><td>② IPCC7: Post-Quantum Encryption Scheme Based on a Perfect Dominating Set in 3-Regular Graph</td></tr>
<tr><td>③ IEEE Access</td></tr>
<tr><td>④ 12, 4575 - 4596</td></tr>
<tr><td>⑤ 2169-3536</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2024</td></tr>
<tr><td>⑧ 10.1109/ACCESS.2024.3349704</td></tr>
<tr><td colspan="6">양자 컴퓨터의 급속한 발전에 따라 국립 표준 기술 연구소(NIST)는 차세대 암호 표준을 확립하기 위한 공모전을 진행하고 있음. 이전의 공모전은 단일 암호 표준을 선정한 반면, 이번 공모전은 다양한 수학적 문제에 기반한 여러 양자내성암호 알고리즘을 표준화하는 것을 목표함. 3라운드 후보 알고리즘인 아이소제니(isogeny) 문제 기반 키 설정 알고리즘 SIKE가 공격된 사례는 다양한 문제에 기반한 암호 알고리즘의 연구 필요성을 강조함. 본 논문에서는 조합론에 기반한 Perfect Code 암호시스템(PCC)의 개선된 버전인 IPCC7을 연구하여, 새로운 양자내성암호 스킴을 제안함. 이 암호 시스템은 기존 PCC의 성능 문제를 극복하고 그래프 기반 암호화 스킴의 현실적인 실행 가능성을 입증함. IPCC7은 일반적인 용도의 양자내성암호로 사용하기에 메모리 크기와 같은 일부 제한이 있으나 상대적으로 작은 키 크기와 빠른 복호화 속도를 고려할 때, 메모리 제약이 적은 화이트박스 암호와 같은 환경에 활용할 수 있음.</td></tr>
<tr><td rowspan="9">19</td><td rowspan="8">석사</td><td rowspan="8">최영락</td><td rowspan="8">암호학</td><td rowspan="8">학술지
논문</td><td>① Youngrak Choi, Yongjin Yeom, and Ju-Sung Kang</td></tr>
<tr><td>② Practical Entropy Accumulation for Random Number Generators with Image Sensor-Based Quantum Noise Sources</td></tr>
<tr><td>③ MDPI Entropy</td></tr>
<tr><td>④ 25(7), 1056 - 1079</td></tr>
<tr><td>⑤ 1099-4300</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2023</td></tr>
<tr><td>⑧ 10.3390/e25071056</td></tr>
<tr><td colspan="6">고품질의 난수를 효율적으로 생성하는 것은 암호화 모듈의 운영에 필수적임. 진난수생성기의 품질은 출력 엔트로피 소스의 최소 엔트로피로 평가됨. 일반적으로 높은 최소 엔트로피를 갖는 출력 난수열을 만들기 위하여 사용되는 전형적인 방법은 해시 함수를 기반으로 한 엔트로피 축적 기법임. 이는 일반적으로 Leftover Hash Lemma에 근거하며, 출력 난수열의 최소 엔트로피에 대한 하한을 보장함. 그러나, 해시 함수 기반의 엔트로피 축적은 일반적으로 속도가 매우 느리다는 문제가 있음. 본 논문은 실용적인 관점에서 출력 난수열의 최소 엔트로피에 대한 이론적 배경과 함께 새로운 효율적인 엔트로피 축적 기법을 제안함. 해당 연구는 엔트로피 소스에서 입력 시퀀스가 독립적일 때 비트 단위 XOR 작업을 사용하여 매우 효율적인 엔트로피 축적을 수행하며, 이를 통해 출력 난수열의 최소 엔트로피에 대한 이론적 바운드를 얻음. 또한, 이미지 센서 기반 난수발생기의 이미지 센서 픽셀에서 발생하는 다크 샷 노이즈를 엔트로피 소스로 사용하는 양자 난수생성기에 이론 및 실험을 적용함으로써 결과의 타당성을 검토함. 본 연구는 다양한 암호학 분야 및 암호 모듈의 양자난수발생기와 기타 진난수생성기의 엔트로피 축적 효율성을 향상시키고 이를 통한 암호 시스템의 성능 향상에 기여 가능함.</td></tr>
</table>

<table>
<tr><td rowspan="9">20</td><td rowspan="8">박사</td><td rowspan="8">김영범</td><td rowspan="8">금융정보보안</td><td rowspan="8">학술지 논문</td><td>① 최용렬, 김민기, 김영범, 송진교, 진재환, 김희석, 서석충</td></tr>
<tr><td>② KpqBench: Performance and Implementation Security Analysis of KpqC Competition Round 1 Candidates</td></tr>
<tr><td>③ IEEE Access</td></tr>
<tr><td>④ (99):1-1</td></tr>
<tr><td>⑤ 2169-3536</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2023</td></tr>
<tr><td>⑧ 10.1109/ACCESS.2024.3361316</td></tr>
<tr><td colspan="6">2022년 2월, KpqC 대회는 PQC 알고리즘에 대한 제안을 요청했다. 2022년 11월까지 16개 후보(KEM 7개, DSA 9개)가 선정됨. 현재 1차 제출물은 다양한 환경에서의 보안성, 효율성, 확장성 측면에서 평가를 받고 있다. 본 논문에서는 외부 라이브러리의 의존성 없는 접근 방식을 기반으로 성능 및 구현 보안에 대한 분석 결과를 제시함. 즉, 빌드 프로세스를 복잡하게 만들 수 있는 외부 라이브러리를 하드 코딩으로 대체하여 종속성이 없는 분석을 위한 광범위한 테스트를 구성함. 성능 관점에서는 KpqC 후보별 성능 프로파일링, 실행 시간, 메모리 사용량 분석 결과를 제공함. 구현 보안 관점에서는 타이밍 공격에 대한 광범위한 테스트 범위와 상수 시간 구현을 포함할 수 있는 Metamorphic Testing 방법론인 Valgrind 소프트웨어를 사용하여 실제 구현의 버그와 오류를 검사함.</td></tr>
<tr><td rowspan="9">21</td><td rowspan="8">석사</td><td rowspan="8">안상우</td><td rowspan="8">금융정보보안</td><td rowspan="8">학술지 논문</td><td>① 안상우, 서석충</td></tr>
<tr><td>② Parallel Implementation of CRYSTALS-Dilithium for Effective Signing and Verification in Autonomous Driving Environment</td></tr>
<tr><td>③ ICT Express</td></tr>
<tr><td>④ Volume 9, Issue 1</td></tr>
<tr><td>⑤ 2405-9595</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2022</td></tr>
<tr><td>⑧ https://doi.org/10.1016/j.icte.2022.08.003</td></tr>
<tr><td colspan="6">자율주행 환경에서는 각 차량이 실시간으로 BSM(Basic Security Messages)을 주고받으며 수많은 서명과 검증을 수행함. 내장된 그래픽 처리 장치를 사용하여 각 서명 및 검증을 병렬로 신속하게 처리할 수 있는 최적화된 CRYSTALS-Dilithium 소프트웨어를 제시함. 효율성을 위해 더미 연산 기반 Warp Divergence 감소 기법, NTT(Number Theoretic Transform) 기반 다항식 곱셈 병렬 구현, 불량 시퀀스 테이블을 이용한 불량 샘플링 프로세스 최적화 등 여러 가지 최적화 기법을 제안함. 제안된 CRYSTALS-Dilithium 소프트웨어는 기성 자율주행차 OBU(On-Board Unit)인 NVIDIA Jetson AGX Xavier CPU의 Dilithium 소프트웨어에 비해 최대 19.41배의 성능 향상을 제공함.</td></tr>
</table>

<table>
<tr><td rowspan="9">22</td><td rowspan="8">석사</td><td rowspan="8">최호진</td><td rowspan="8">금융정보보안</td><td rowspan="8">학술지 논문</td><td>① 최호진, 서석충</td></tr>
<tr><td>② Efficient Parallel Implementations of PIPO Block Cipher on CPU and GPU</td></tr>
<tr><td>③ IEEE Access</td></tr>
<tr><td>④ VOLUME 10, 2022</td></tr>
<tr><td>⑤ 2329-4949</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2022</td></tr>
<tr><td>⑧ 10.1109/ACCESS.2022.3198707</td></tr>
<tr><td colspan="6">데이터 중심 ICT 환경에서 서버에 있는 고객의 데이터를 안전하게 관리하기 위해서는 데이터 암호화가 필수적임. 특히, 서버 환경은 클라이언트로부터 들어오는 수많은 데이터를 관리/처리하는 역할을 담당하기 때문에 대용량 데이터를 암호화하기 위해 많은 시간이 필요함. 본 논문에서는 CPU 환경과 GPU 환경에 각각 고도로 최적화된 두 종류의 PIPO 암호화 소프트웨어를 제시함. 최적화를 위해 우리는 CPU의 AVX 관련 명령과 GPU의 NVIDIA CUDA 플랫폼이라는 두 가지 병렬 처리 기술을 최대한 활용함. CPU 환경의 최적화와 관련하여 AVX2 및 AVX-512 명령어 세트와 제안된 산술 기법을 각각 적절하게 사용하여 32 및 64 블록과 같은 여러 일반 텍스트 블록을 처리함. GPU 환경 최적화에 관해서는 GPU 아키텍처의 특성을 고려한 데이터 정렬/데이터 결합 방법과 PTX 인라인 어셈블리 활용 방법을 제안함.</td></tr>
<tr><td rowspan="9">23</td><td rowspan="8">석사</td><td rowspan="8">송진교</td><td rowspan="8">금융정보보안</td><td rowspan="8">학술지 논문</td><td>① 김영범, 송진교, 윤택영, 서석충</td></tr>
<tr><td>② CRYSTALS-Dilithium on ARMv8</td></tr>
<tr><td>③ Security and Communication Networks (Hindawi)</td></tr>
<tr><td>④ Volume 2022</td></tr>
<tr><td>⑤ 1939-0114</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2022</td></tr>
<tr><td>⑧ https://doi.org/10.1155/2022/5226390</td></tr>
<tr><td colspan="6">본 논문은 ARMv8 기반 MCU에서 효율적인 Crystals-Dilithium 구현을 제시함. Dilithium의 성능을 향상시키기 위해 대규모 레지스터 세트 및 NEONengine과 같은 ARMv8의 아키텍처 속성을 활용하여 Dilithium의 핵심 연산인 NTT(Number Theoretic Transform) 기반 다항식 곱셈을 최적화함. NEON 엔진을 사용하여 NTT 기반 다항식 곱셈에 작업 병렬성을 적용함. 또한 제안된 병합 및 레지스터 유지 기술을 사용하여 NTT 기반 다항식 곱셈 중 메모리 액세스 수를 줄임. 마지막으로 ARM 프로세서와 NEON 엔진으로 동시에 실행되는 인터리브 NTT 기반 곱셈을 제시함.</td></tr>
</table>

<table>
<tr><td rowspan="9">24</td><td rowspan="8">박사</td><td rowspan="8">한재승</td><td rowspan="8">부채널
분석 및
대응법
설계</td><td rowspan="8">학술지
논문</td><td>① 한재승, 이태호, 권지훈, 이주희, 김일주, 조지훈, 한동국, 심보연</td></tr>
<tr><td>② Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-Based Profiling</td></tr>
<tr><td>③ IEEE Access</td></tr>
<tr><td>④ Vol.9, 166283-166292</td></tr>
<tr><td>⑤ 2169-3536</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2021</td></tr>
<tr><td>⑧ 10.1109/ACCESS.2021.3135600</td></tr>
<tr><td colspan="6">본 논문은 NIST 표준으로 선정된 격자 기반 디지털 서명 알고리즘인 CRYSTALS-DILITHIUM에 대한 단일 파형 부채널 공격을 제안하였음. 서명 생성과 키 생성 과정 중의 NTT 변환에서 누출되는 전력 파형을 기계학습 기반 프로파일링하여 공격 대상 파형의 비밀 키를 획득함. 제안한 공격은 서명 생성을 공격할 때 비밀 키 벡터 s1과 s2를 모두 복구할 수 있고, 키 생성을 공격할 때는 s1만 복구할 수 있으므로 두 과정의 공격 결과를 병합해 s1을 더 높은 정확도로 복구할 수 있음. 반면에 s2 서명 생성에서만 복구하므로 서명 생성 내의 샘플링, 덧셈, 반올림 및 패킹과 같은 네 가지 함수를 추가적으로 공격하여 s2의 복구 성공률을 향상시킴. ARM Cortex-M4 기반 STM32F3 마이크로컨트롤러에 CRYSTALS-DILITHIUM를 적용하여 실제 제안한 공격을 수행함.</td></tr>
<tr><td rowspan="9">25</td><td rowspan="8">석박사통합</td><td rowspan="8">이종혁</td><td rowspan="8">부채널
분석 및
대응법
설계</td><td rowspan="8">학술지
논문</td><td>① 이종혁, 한재승, 이상엽, 권지훈, 최건희, 허재원, 조지훈, 한동국</td></tr>
<tr><td>② Systematization of Shuffling Countermeasures With an Application to CRYSTALS-Dilithium</td></tr>
<tr><td>③ IEEE Access</td></tr>
<tr><td>④ Vol.11, 142862-142873</td></tr>
<tr><td>⑤ 2169-3536</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2023</td></tr>
<tr><td>⑧ 10.1109/ACCESS.2023.3342914</td></tr>
<tr><td colspan="6">본 논문은 대표적인 부채널 공격 대응기법 중 하나인 셔플링에 대한 프레임워크를 제안함. 셔플링은 암호 알고리즘에서 순서를 바꿀 수 있는 연산들의 순서를 무작위로 섞어 부채널 공격의 복잡도를 증가시키는 주요한 대응기법임. 하지만 대부분의 연구에서 셔플링은 단순한 기능으로써 등장할 뿐 체계적인 프레임워크가 부족한 상황임. 본 논문은 혁신적이고 체계적인 셔플링 프레임워크를 제안하여 개발자들이 특정 목표에 맞게 적절한 방법을 선택할 수 있도록 안내함. 또한, NIST PQC 전자서명인 CRYSTALS-DILITHIUM 알고리즘에 이 프레임워크를 적용하고, 12가지의 다양한 셔플링 방법을 제시하여 제안한 프레임워크의 실효성을 입증하였음.</td></tr>
</table>

<table>
<tr><td rowspan="9">26</td><td rowspan="8">석사</td><td rowspan="8">임성혁</td><td rowspan="8">부채널
분석 및
대응법
설계</td><td rowspan="8">학술지
논문</td><td>① 임성혁, 이종혁, 한동국</td></tr>
<tr><td>② Improved Differential Fault Attack on LEA by Algebraic Representation of Modular Addition</td></tr>
<tr><td>③ IEEE Access</td></tr>
<tr><td>④ Vol.8, 212794-212802</td></tr>
<tr><td>⑤ 2316-3536</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2020</td></tr>
<tr><td>⑧ 10.1109/ACCESS.2020.3039805</td></tr>
<tr><td colspan="6">본 논문은 ISO/IEC 국제 표준 경량 블록 암호 LEA에 대한 새로운 차분 오류주입 공격 방법을 제안함. 이전에 제안된 공격은 단일 비트 플립 오류 모델을 사용하여 실제적인 적용이 어려웠으나, 본 논문에서 제안하는 공격 방법은 랜덤 워드 오류 모델을 가정하여 더 현실적인 적용이 가능함. 실제 MCU에 전자파 오류주입 장비를 이용하여 공격이 실현됨을 입증함. 이 공격 방법은 워드 단위의 오류가 적용된 중간값이 LEA의 모듈러 덧셈 연산이 일어나 오류가 확산되는 것을 이용해 확산된 오류와 정상 출력의 차분을 이용해 비밀키를 복구함. 제안한 공격은 현재까지 제안된 방법 중에서 가장 약한 공격자 가정을 가지며, 필요한 오류주입 암호문 수와 그에 따른 키 후보 수가 가장 적음. 결과적으로 IoT 장치에 LEA 암호를 구현할 때는 결함 주입 공격에 대한 적절한 대책이 필요함을 보임.</td></tr>
<tr><td rowspan="9">27</td><td rowspan="8">석사</td><td rowspan="8">우지은</td><td rowspan="8">부채널
분석 및
대응법
설계</td><td rowspan="8">학술지
논문</td><td>① 우지은, 한재승, 한동국</td></tr>
<tr><td>② Deep-Learning-Based Side-Channel Analysis of Block Cipher PIPO With Bitslice Implementation</td></tr>
<tr><td>③ IEEE Access</td></tr>
<tr><td>④ Vol.10, 69303-69311</td></tr>
<tr><td>⑤ 2169-3536</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2022</td></tr>
<tr><td>⑧ https://doi.org/10.1109/ACCESS.2022.3187201</td></tr>
<tr><td colspan="6">본 논문에서는 비트슬라이스 구현된 블록암호에 대한 효과적인 딥러닝 기반 프로파일링 및 비프로파일링 부채널 공격을 제안함. 공격 대상은 경량 블록 암호 PIPO를 선택했으며, 각 딥러닝 기반 프로파일링, 비프로파일링 부채널 공격에서 효과적인 라벨링 기법을 제안함. 프로파일링 공격에서는 라벨링 기법을 값(ID), 최상위 비트(MSB), 해밍웨이트(HW) 3가지로 변경하며 부채널 분석을 수행함. 3가지 MCU에 대해 실험을 수행했을 때 ID가 가장 뛰어난 효과를 가짐. 비프로파일링 공격에서는 비트슬라이스 구현된 블록암호의 부채널 누출 경향을 파악하고, 이에 맞는 라벨링 기법인 이진 인코딩을 제안함. 3가지 MCU에 대해 실험을 수행하여 제안한 이진 인코딩 기법이 기존의 MSB, HW 라벨링보다 더 효과적임을 보임.</td></tr>
</table>

<table>
<tr><td rowspan="10">28</td><td rowspan="9">박사</td><td rowspan="9">염선호</td><td rowspan="9">박수현</td><td rowspan="9">학술지
논문</td><td>① 델핀 라즈 케사리 메리, 고은비, 김성근, 염선호, 신수영, 박수현</td></tr>
<tr><td>② A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things</td></tr>
<tr><td>③ sensors</td></tr>
<tr><td>④ 21(24), 8262</td></tr>
<tr><td>⑤ 1424-8220</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2021</td></tr>
<tr><td>⑧ https://doi.org/10.3390/s21248262</td></tr>
<tr><td colspan="5">최근의 수중 인터넷 사물에 관한 체계적 리뷰는 이 분야에서의 급속한 발전과 함께 나타난 다양한 도전 과제, 프라이버시, 그리고 보안 문제들을 깊이 있게 다루고 있음. 수중 IoT 기술이 해양 탐사, 환경 모니터링, 재난 감지 등 광범위한 응용 분야에서 중요한 역할을 하고 있음을 강조하면서, 이와 관련된 최신 경향을 종합적으로 분석함. 특히, 데이터 전송의 안정성과 신뢰성을 높이기 위한 기술적 진보와, 사용자 데이터 보호를 위한 프라이버시 증진 방안에 대해 상세히 설명하며, 이로 인해 수중 IoT 기술의 발전 가능성을 크게 향상시키고 있음. 이러한 근거에서, 이 논문은 수중 IoT 분야의 연구자 및 개발자들에게 중요한 지침과 영감을 제공하며, 미래 연구의 방향성을 제시하는 데 크게 기여하고 있음.</td></tr>
<tr><td rowspan="10">29</td><td rowspan="9">박사</td><td rowspan="9">델핀 라즈
케사리
메리</td><td rowspan="9">박수현</td><td rowspan="9">학술지
논문</td><td>① 델핀 라즈 케사리 메리, 고은비, 윤동진, 신수영, 박수현</td></tr>
<tr><td>② Energy Optimization Techniques in Underwater Internet of Things: Issues, State-of-the-Art, and Future Directions</td></tr>
<tr><td>③ water</td></tr>
<tr><td>④ 14(20), 3240</td></tr>
<tr><td>⑤ 2073-4441</td></tr>
<tr><td>⑥</td></tr>
<tr><td>⑦ 2022</td></tr>
<tr><td>⑧ https://doi.org/10.3390/w14203240</td></tr>
<tr><td colspan="5">수중 인터넷 사물의 에너지 최적화 기술에 관한 이 논문은 현재 이 분야에서 직면하고 있는 주요 이슈들과 최신 연구 동향, 그리고 미래의 발전 방향을 종합적으로 다루고 있음. 에너지 효율성은 수중 IoT 시스템의 성능과 지속 가능성에 있어 핵심적인 요소이며, 이 논문은 에너지 소비를 줄이면서도 효율적인 데이터 전송과 처리를 가능하게 하는 다양한 기술과 방법론을 심도 깊게 분석함. 특히, 저전력 통신 기술, 에너지 수확 기술, 그리고 에너지 관리 알고리즘 등의 최신 연구 성과를 소개하면서, 이들이 어떻게 수중 환경에서의 IoT 응용을 더욱 실용적이고 지속 가능하게 만들 수 있는지를 설명함. 또한, 논문은 에너지 최적화 분야에서 아직 해결해야 할 과제들을 지적하고, 이를 극복하기 위한 미래 연구의 방향을 제시함으로써, 수중 IoT 기술의 발전을 위한 중요한 기여를 하고 있음.</td></tr>
<tr><td colspan="2" rowspan="4">총 참여대학원생 수</td><td>석사</td><td>163</td><td rowspan="4">제출 요구량</td><td rowspan="4">26</td></tr>
<tr><td>박사</td><td>70</td></tr>
<tr><td>석박사통합</td><td>19</td></tr>
<tr><td>계</td><td>252</td></tr>
</table>

② 참여대학원생 학술대회 대표실적의 우수성

<표 2-6> 평가 대상 기간(2020. 9. 1. ~ 2024. 2. 29.) 내 참여대학원생 학술대회 발표실적

연번	학위과정 (석사/박사/ 석박사통합)	참여대학원생 성명	발표 형식 (구두, 포스터)	학술대회 발표실적 상세내용
1	박사	허욱	구두	① 허욱, 강수진, 김기윤, 김종성
				② A study on cloud data access through browser credential migration in Windows environment
				③ DFRWS USA 2023
				④ DFRWS
				⑤
				⑥ 2023. 07. (볼티모어, 미국)
				⑦ https://doi.org/10.1016/j.fsidi.2023.301568
2	박사	김한기	구두	① 김한기, 전용진, 김기윤, 김종성, 심보연, 한동국, 서화정, 김성겸, 홍석희, 성재철, 홍덕조
				② PIPO: A Lightweight Block Cipher with Efficient Higher-Order Masking Software Implementations
				③ ICISC 2020
				④ Korea Institute Of Information Security And Cryptology
				⑤
				⑥ 2020. 12. (서울, 대한민국)
				⑦ https://doi.org/10.1007/978-3-030-68890-5_6
3	박사	전용진	구두	① 전용진, 백승준, 김종성
				② A Novel Framework to Construct Quantum Circuits of S-Boxes : Application to 4-bit S-Boxes
				③ MobiSec 2023
				④ Korea Institute Of Information Security And Cryptology
				⑤
				⑥ 2023. 12. (오키나와, 일본)
				⑦
4	박사	백승준	구두	① 백승준, 김기윤, 전용진, 김종성
				② Enhancing the Related-Key Security of PIPO Through New Key Schedules
				③ ICISC 2023
				④ Korea Institute Of Information Security And Cryptology
				⑤
				⑥ 2023. 11. (서울, 대한민국)
				⑦ https://doi.org/10.1007/978-981-97-1235-9_1

5	석사	박종현	구두	① 박종현, 김종성
				② See-In-The-Middle Attacks on Blockciphers ARIA and DEFAULT
				③ ICISC 2022
				④ Korea Institute Of Information Security And Cryptology
				⑤
				⑥ 2022. 11. (서울, 대한민국)
				⑦ https://doi.org/10.1007/978-3-031-29371-9_1
6	석사	전창열	구두	① 전창열, 김동찬
				② Patterson 디코딩 기반 Classic McEliece 키복호 연산에 관한 연구
				③ 한국통신학회 학술대회논문집
				④ 한국통신학회
				⑤
				⑥ 2022.02. (평창, 대한민국)
				⑦
7	박사	고용호	구두	① G Kim, Y Ko, and I You
				② Formal Verification of 5GAKA-LCCO protocol supporting Forward Secrecy: Through expanded BAN Logic
				③ MobiSec 2023
				④ 한국정보보호학회
				⑤
				⑥ 2023
				⑦
8	석사	권호석	포스터	① H Kwon, Y Moon, S Son, Bonam Kim, and Ilsun You
				② Light weight data integrity verification with immutable merkle root on massive IIoT data
				③ MobiSec 2023
				④ 한국정보보호학회
				⑤
				⑥ 2023
				⑦
9	석사	손대현	구두	① D Son, H park, B kim, and I You
				② 5G 네트워크상에서 Braeken이 제안한 대칭키 기반의 5G-AKA 인증 프로토콜 BAN Logic 정형화 검증
				③ KCSA-S'22
				④ 한국융합보안학회
				⑤
				⑥ 2022
				⑦

10	석사	오종민	구두	① J Oh, I You
				② A Study on Security Protocol for establishing secure communication channels in 5G AKMA
				③ MobiSec 2023
				④ 한국정보보호학회
				⑤
				2023
				⑦
11	석사	김건우	구두	① D.G. Duguma, G Kim, B Kim, and I You
				② MUD for Infusion Pumps: An Attempt to Reduce Network-based Attacks
				③ WISA 2022
				④ 한국정보보호학회
				⑤
				⑥ 2022
				⑦
12	석사	정서우	구두	① Seowoo Jung, Seunghwan Yun, Okyeon Yi
				② Analysis of 5G AKA vulnerabilities through 5G simulator
				③ ICFICE 2022
				④ 한국정보통신학회
				⑤
				⑥ 2022
				⑦
13	석사	김태완	구두	① Taewan Kim, Seyoon Lee, Seunghwan Yun, Jongbum Kim, Okyeon Yi
				② Analysis of Radioactive Decay Based Entropy Generator in the IoT Environments
				③ WISA 2022
				④ 한국정보보호학회
				⑤
				⑥ 2022
				⑦
14	석사	이세윤	포스터	① Seyoon Lee, Taewan Kim, Changuk Jang, Okyeon Yi
				② Design of KEM-DEM on 6G Telecommunication for Quantum Computer
				③ WISA 2022
				④ 한국정보보호학회
				⑤
				⑥ 2022
				⑦

15	석사	권수진	구두	① Sujin Kwon, Ju-Sung Kang, Yongjin Yeom
				② Analysis of public-key cryptography using a 3-regular graph with a perfect dominating set
				③ 2021 IEEE Region 10 Symposium (TENSYMP)
				④ IEEE Region 10
				⑤
				⑥ 2021
				⑦ 10.1109/TENSYMP52854.2021.9550868
16	석사	임형신	구두	① Hyoungshin Yim, Ju-Sung Kang, Yongjin Yeom
				② An Efficient Structural Analysis of SAS and its Application to White-Box Cryptography
				③ 2021 IEEE Region 10 Symposium (TENSYMP)
				④ IEEE Region 10
				⑤
				⑥ 2021
				⑦ 10.1109/TENSYMP52854.2021.9550967
17	석사	박영재	구두	① Yeongjae Park
				② End-to-End PQC Encryption Protocol for GPKI-Based Video Conferencing Systems
				③ IEEE ICEIB 2023
				④ IEEE, IIKII
				⑤
				⑥ 2023
				⑦ 10.1109/ICEIB57887.2023.10170680
18	석사	신동현	구두	① 신동현, 김영범, 서석충
				② Optimized Kyber implementation on 16-bit MSP430 Microcontroller
				③ MobiSec 2023
				④ Korea Institute Of Information Security And Cryptology
				⑤
				⑥ 2023. 12. (오키나와, 일본)
				⑦
19	박사	김영범	구두	① 김영범, 서석충
				② Vectorized Implementation of Crystals-Kyber on NEON extension
				③ MobiSec 2023
				④ Korea Institute Of Information Security And Cryptology
				⑤
				⑥ 2023. 12. (오키나와, 일본)
				⑦

20	석사	김동천	구두	① 김동천, 서석충
				② GPU 환경을 고려한 HQC 내 이진 필드 상에서의 곱셈 구현 분석
				③ 2023 한국정보보호학회 동계학술대회
				④ 한국정보보호학회
				⑤
				⑥ 2023.12.02. (서울, 대한민국)
				⑦
21	석사	안상우	구두	① 안상우, 서석충
				② Study on Optimizing Block Ciphers (AES, CHAM) on Graphic Processing Units
				③ IEEE ICCE-Asia 2020
				④ IEEE Conference
				⑤
				⑥ 2020.11.01. (서울, 대한민국)
				⑦
22	석사	우지은	구두	① 우지은, 한재승, 김연재, 이태호, 한동국
				② Deep Learning-based Side-Channel Analysis on PIPO
				③ Information Security and Cryptology - ICISC 2021
				④ 한국정보보호학회
				⑤
				⑥ 2021.12.01. (서울, 대한민국)
				⑦ 해당 없음
23	석사	허재원	구두	① 허재원, 한동국
				② Differential Fault Attack on AES using Maximum Four Bytes Faulty Ciphertexts
				③ Information Security and Cryptology - ICISC 2022
				④ 한국정보보호학회
				⑤
				⑥ 2022.11.30. (서울, 대한민국)
				⑦ 해당 없음
24	박사	한재승	구두	① 한재승, 한동국
				② Side-Channel Attacks and Countermeasures on Digital Signature AIMer
				③ Symposium on Cryptography and Information Security - SCIS 2024
				④ IEICE Technical Committee on Information Security (ISEC)
				⑤
				⑥ 2024.01.23. (나가사키, 일본)
				⑦ 해당 없음

25	박사	임성혁	구두	① 임성혁, 한재승, 이태호, 한동국
				② Differential Fault Attack on Lightweight Block Cipher PIPO
				③ Information Security and Cryptology – ICISC 2021
				④ 한국정보보호학회
				⑤
				⑥ 2021.12.01. (서울, 대한민국)
				⑦ https://doi.org/10.1007/978-3-031-08896-4_15
26	박사	황아리	구두	① 황아리, 윤동진, 박수현
				② Polar Region Observation and Information Technology Network Requirements
				③ The 13th International Conference on Green and Human Information Technology
				④ 대한전자공학회
				⑤
				⑥ 2024.01, 하노이, 베트남
				⑦
27	박사	염선호	구두	① 염선호, 윤동진, 황아리, 박수현
				② Cross-layer design for Multi-Medium reliable channel switching in UHSDM
				③ ICGHIT 2024 (International Conference on Green and Human Information Tech 2024)
				④ 대한전자공학회
				⑤
				⑥ 2024.01, 하노이, 베트남
				⑦
28	박사	델핀라즈	구두	① 고은비, 델핀라즈, 신수영, 김승근, 박수현
				② International Standardization for Maritime, Underwater Internet of Things and Digital Twin Applications
				③ WuWNet 2021 (International Conference on Underwater Networks & Systems 2021)
				④ Advancing Computing as a Science & Profession
				⑤
				⑥ 2021.11, 광동, 중국
				⑦

29	박사	신하쉬르티카	구두	① 신하 쉬르티카, 권수연, 박수현	
				② A Survey of Deep/Machine Learning in Maritime Communications	
				③ ICUFN 2023 (International Conference on Ubiquitous and Future Networks 2023)	
				④ 한국통신학회	
				⑤	
				⑥ 2023.07, 제주, 대한민국	
				⑦	
총 참여대학원생 수		**석사**	163	**제출 요구량**	26
		박사	70		
		석박사통합	19		
		계	252		

- 참여학생 허욱은 국제 학술대회 DFRWS 2023에서 보안 API를 사용하여 암호화된 데이터를 재생성하는 방법으로 브라우저 데이터 마이그레이션 기법을 제안하였으며, 이를 활용하여 다양한 웹 서비스의 데이터를 수집하는 방법을 제시하였음
- 참여학생 김한기는 국제 학술대회 ICISC 2020에서 경량 블록암호 PIPO를 제안하여 기밀성 제공이 필요한 다양한 정보보호 환경에서 부채널 분석에 저항성을 갖는 암호를 활용할 수 있도록 하였으며, 대칭키 암호에 대한 국가 과학기술력 향상에 기여하였음
- 참여학생 전용진은 국제 학술대회 MobiSec 2023에서 4-bit S-box의 양자회로 구성 방법을 제안하여 대칭키 암호의 효율적인 양자회로를 구성할 수 있게 하였으며, 미래 양자컴퓨터 시대를 대비하여 양자암호 원천 기술 확보에 기여하였음
- 참여학생 백승준은 국제 학술대회 ICISC 2023에서 경량 블록암호 PIPO에 대한 새로운 키 스케줄을 제안함으로써 IoT 환경에서 사용될 수 있는 경량암호의 효율성을 유지함과 동시에 안전성을 향상시켰고, 안전한 초연결사회를 위한 암호기술 개발에 이바지함
- 참여학생 박종현은 국제 학술대회 ICISC 2022에서 국내표준 블록암호 ARIA와 해외 블록암호 DEFAULT에 대해 부채널 누출정보를 암호학적으로 활용한 See-in-the-Middle 공격을 제안하여 부채널 부분 마스킹에 대한 하한을 지정하였으며, 대칭키 암호에 대한 국가 과학기술력 향상에 기여하였음
- 참여학생 전창열은 국내 학술대회 2022 한국통신학회에서 Patterson 디코딩 기반 Classic McEliece 키복호 연산에 관해 연구하여, NIST 주관 PQC 4라운드 알고리즘 Classic McEliece에 개발진이 제안한 berlekamp massey 디코딩보다 우수한 연산 속도를 보이는 Patterson 디코딩을 적용함. 이는 양자내성암호에 대한 안전성을 유지함과 동시에 효율성을 향상시키는데 기여하였음
- 참여학생 고용호는 국제 학술대회 MobiSec 2023에서 잘 알려진 정형화 검증 양상논리 이론 BAN Logic을 향상 시킨 기법을 제안하였으며, 제안한 기법을 통해 5G 이동통신 Primary 인증 프로토콜 5GAKA-LCCO의 취약점을 도출해내어 국제적 보안성 검증 기술력 향상에 기여하였음
- 참여학생 권호석은 국제 학술대회 MobiSec 2023에서 massive IIoT 환경에서 Immutable merkle root를 통해 경량 데이터의 무결성을 검증하는 방안을 제안하였으며, 4차산업혁명 시대에 대규모의 산업용 IoT 환경에서의 보안성 향상에 기여하였음
- 참여학생 손대현은 한국융합보안학회 주관의 국내 학술대회 KCSA-S’22에서 잘 알려진 정형화 검

증 양상논리인 BAN Logic을 통해 5G 이동통신 Primary 인증 프로토콜인 대칭키 기반의 5G-AKA를 정형화 검증을 통해 취약점을 도출하고 이를 해결할 방안을 제시하여 국내 과학 기술에 기여하였음
- 참여학생 오종민은 국제 학술대회 MobiSec 2023에서 5G 이동통신 환경의 어플리케이션 보안 지원을 위한 2차인증 표준 프로토콜 AMKA(Authentication and Key Management for Applications)를 분석하여 향후 연구 진행 방향을 제시하여 이동통신 보안 분야의 과학 기술 발전에 기여하였음
- 참여학생 김건우는 한국정보보호학회 주관의 국내 학술대회 WISA 2022에서 대표적 의료 IoT인 인슐린 펌프에 대한 보안성을 검증하고 취약점 도출을 통해 향후 의료 IoT의 보안성 발전을 위한 방향성을 제시하여 의료 IoT 보안 분야의 과학 기술 발전에 기여하였음
- 참여학생 정서우는 국제 학술대회 ICFICE 2022에서 5G AKA(인증 및 키 협의) 과정의 취약점 분석과 데이터 분석을 진행하며, 5G 오픈 소스 시뮬레이터를 통해 알려진 취약점을 분석하고 위치 추적 공격에 대한 대책을 제안함으로써 5G 기술 연구에 기여하였음
- 참여학생 김태완은 국제 학술대회 WISA 2022에서 IoT 환경의 제한된 자원으로 인해 충분한 엔트로피를 수집하는 데 어려움이 있음을 나타내고 이 문제를 해결하기 위해 α 및 β 방사성 붕괴 소음 자원을 사용하고, 적절한 엔트로피 생성 방법을 이용해 엔트로피를 생성한 결과, β 방사성 붕괴 기반 소음 자원이 α 기반 소음 자원보다 약 32배 빠르게 엔트로피를 생성할 수 있음을 보임으로써 난수 및 엔트로피 연구에 기여하였음.
- 참여학생 이세윤은 국제 학술대회 WISA 2022에서 양자 컴퓨팅 기술의 발전이 5G에서의 보안 문제를 야기할 수 있음을 언급하고, 양자 저항성을 가진 포스트-양자 암호화(PQC)를 사용하여 5G의 중요 식별 값인 SUCI를 숨기는 과정에서 적절한 키 캡슐화 메커니즘(KEM)을 설계하고 KEM에 의해 공유된 키를 기반으로, 6G에서 기밀 정보를 안전하게 공유하기 위한 적절한 데이터 캡슐화 메커니즘(DEM)을 제안하였음
- 참여학생 권수진은 국제 학술대회 2021 IEEE Region 10 Symposium (TENSYMP)에서 그래프 기반 암호시스템의 구현 알고리즘 및 해당 알고리즘의 성능을 발표하였으며, 국내 양자내성암호 알고리즘 연구의 기반을 마련하는 데 기여하였음
- 참여학생 임형신은 국제 학술대회 2021 IEEE Region 10 Symposium (TENSYMP)에서 효율적인 화이트박스 암호 알고리즘 분석 기법인 SAS 구조와 해당 구조의 기법의 구현 성능에 대하여 발표하였으며, 국내 키 보호 시스템에 대한 기술력 향상에 기여하였음
- 참여학생 박영재는 국제 학술대회 IEEE ICEIB 2023에서 화상회의 시스템에 적용된 End-to-End 암호 프로토콜로의 양자내성암호 적용 가능성을 분석하고 국내 화상회의 시스템에 GPKI를 결합한 양자내성암호 적용 방향성을 제안함으로써 국가 암호 시스템 안전성 향상에 기여하였음
- 참여학생 신동현은 국제 학술대회 Mobisec 2023에서 NIST PQC 표준화 알고리즘인 Crystals-Kyber에 대한 MSP430장치에서의 최적화 방안을 제시함. 향후 세계적인 PQC 마이그레이션 도입 시, 리소스 자원이 제한된 클라이언트에서 성능 부하를 감소시킬 수 있음
- 참여학생 김영범은 국제 학술대회 Mobisec 2023에서 NIST PQC 표준화 알고리즘인 Crystals-Kyber에 대한 ARM 환경에서 최적화 방안을 제시함. NEON 명령어를 사용하여 병렬 연산을 통해 Kyber의 주 연산 부하지점을 고속화함. 향후 PQC 마이그레이션 시 클라이언트 연산 부하에 상당한 기여를 함.
- 참여학생 김동천은 국내 학술대회인 한국정보보호학회 2023 동계학술대회에서 GPU 환경을 고려하여 HQC 알고리즘을 분석함. HQC는 NIST PQC 공모전 후보 알고리즘임. 향후 PQC 마이그레이션 시, 다중 클라이언트와 통신해야 하는 서버에서 GPU 병렬 특징을 활용하여 연산 부하를 감소 시킬 수 있음
- 참여학생 안상우는 국제 학술대회 IEEE ICCE-Asia 2020에서 블록암호 AES, CHAM에 대한 분석을 GPU 환경에서 진행하였으며 고속화 방안을 제시함. 특히, GPU의 다중코어를 활용한 병렬 연산 활용을 극대화하여 GPU를 사용하는 클라이언트 및 서버 환경에서 성능 부하를 크게 감소시킴

- 참여학생 우지은은 국제 학술대회 ICISC 2021에서 경량 블록암호 PIPO에 대한 딥러닝 기반 부채널 분석을 제안하여 블록암호에 대한 딥러닝 기반 부채널 안전성 검증 기술을 발전 시켰으며, 대칭키 암호의 안전성 평가 기술 향상을 통해 국내 대칭키 암호의 안전성 향상에 기여하였음
- 참여학생 허재원은 국제 학술대회 ICISC 2022에서 블록암호 AES에 대한 최대 4바이트 오류를 이용한 차분 오류공격을 제안함. 제안된 공격은 특정한 1바이트 오류만을 이용한 이전 공격들과 달리 바이트 위치 및 워드내의 어떤 바이트가 바뀌어도 공격할 수 있어 공격 가정이 완화됨. 이를 통해 대칭키 암호의 오류주입 안전성 평가 기술 향상 및 안전성 향상에 기여하였음
- 참여학생 한재승은 국제 학술대회 SCIS 2024에서 KpqC, NIST PQC 후보인 AIMer 전자서명 알고리즘에 대한 전력 분석 취약점 및 마스킹 대응기법을 제안함. 다양한 공격 위치에 대한 공격 가능성을 제시했으며, 하나의 공격 위치는 실험을 통해 취약점을 입증했으며, 마스킹 대응기법은 알고리즘 수준으로 제시함. 이를 통해 미래 양자컴퓨터 시대를 대비하여 양자 내성 암호에 대한 원천기술 확보에 기여하였음
- 참여학생 임성혁은 국제 학술대회 ICISC 2021에서 경량 블록암호 PIPO에 대한 단일 비트 플립을 이용한 차분 오류 공격을 제시함. 제안된 공격은 마지막 이전 라운드의 입력에 오류를 주입하여 마지막 라운드키를 복구하고, 다시 그 이전 라운드의 입력에 오류를 주입하여 마지막 이전 라운드키를 복구했으며, 최종적으로 모든 비밀키를 복구함. 이를 통해 대칭키 암호의 오류주입 안전성 평가 기술을 향상시키고, 국내 대칭키 암호의 안전성 향상에 기여하였음
- 참여학생 황아리는 ICGHIT 2024에서 극한지 관측 및 탐사 데이터 확보를 위한 극한지 네트워크 인프라 구성과 그에 대한 요구사항을 제시함으로써 극한 조건에 맞는 네트워크 아키텍처를 개발하여 극지 연구, 군사 작전 및 상업 활동을 지원하는 튼튼한 통신 기반을 마련하고, 극지역에서의 과학적 탐사와 상업 활동을 위한 안정적이고 지속 가능한 커뮤니케이션 시스템의 필요성을 강조하며, 현재 기술이 충분히 해결하지 못하는 문제들을 극복하는데 기여하였음
- 참여학생 염선호는 ICGHIT 2024에서 다중 매체 채널 전환에 대한 획기적인 크로스 레이어 설계를 제안하고 UHSDM 기술을 이용하여 수중 환경에서의 다양한 통신 기술을 통합, 최적화하는 새로운 방법을 개발하여, 수중 통신의 효율성과 신뢰성을 크게 향상시키고, 수중 무선 통신에서 발생할 수 있는 다양한 환경적 도전을 극복하고, 더 빠르고 안정적인 데이터 전송을 가능하게 하는 솔루션을 제공함.
- 참여학생 델핀라즈는 WuWNet 2021에서 해양 및 수중 IoT 기술의 국제 표준화를 통해 해양 및 어업 산업에 큰 변화를 가져올 것으로 기대되며 전 세계 전문가들이 참여하여 고품질의 표준을 개발하고 있으며, 특히 IoT 기술뿐만 아니라 디지털 트윈 기술의 발전이 산업 혁신에 기여할 것으로 기대됨
- 참여학생 신하쉬르티카는 ICUFN 2023에서 ISO/IEC JTC1 SC41 수중 통신 국제 표준에 대한 동향을 발표함으로써 해양 및 수중 IoT 기술과 디지털 트윈을 표준화하여 해양 및 어업 산업에 혁신적인 변화를 가져올 것으로 기대하며 전 세계 전문가들이 참여하는 국제 표준 개발 과정에서 고품질의 표준을 개발하는 데 중요한 기여함. 또한 IoT 기술을 넘어 해양 및 수중 환경에서 디지털 트윈 기술의 발전을 이끌며 산업 전반의 혁신을 촉진하는 중요한 역할을 할 것으로 기대함

③ 참여대학원생 특허, 기술이전, 창업 실적의 우수성

<표 2-7> 평가 대상 기간(2020. 9. 1. ~ 2024. 2. 29.) 내 이공계열 참여대학원생 특허, 기술이전, 창업 실적

연번	학위과정 (석사/박사/ 석박사통합)	참여대학원생 성명	실적 종류	특허, 기술이전, 창업 실적 상세내용
1	박사	허욱	특허	① 김종성, 허욱, 박명서
				② FTS 색인데이터 기반의 삭제 채팅 메시지 복구 장치 및 방법
				③ 대한민국
				④ 10-2644076
				⑤ 2024
2	박사	김한기	특허	① 김종성, 김한기, 한동국, 김기윤, 전용진, 홍석희
				② 부채널 공격 대응이 용이한 128비트 경량 블록 암호화 방법 및 이를 이용한 장치
				③ 대한민국
				④ 10-2287962
				⑤ 2021
3	석박사통합	김기윤	특허	① 김종성, 이세훈, 허욱, 김기윤
				② 종단간 암호화가 적용된 파일에 대한 복호화 장치 및 방법
				③ 대한민국
				④ 10-2216869
				⑤ 2021
4	박사	전용진	특허	① 김종성, 전용진, 김기윤, 김한기
				② DLBN이 3 이상인 조건을 만족하는 확장 에스박스 및 이를 이용한 비트 연산 방법
				③ 대한민국
				④ 10-2424922
				⑤ 2022
5	박사	강수진	특허	① 김종성, 신수민, 김기윤, 강수진
				② 미디어 파일에 대한 안티 포렌식 해제 장치 및 방법
				③ 대한민국
				④ 10-2311996
				⑤ 2021
6	석사	이세훈	특허	① 김종성, 이세훈, 허욱, 김기윤
				② 캐시 파일을 이용한 삭제 메시지 복구 장치 및 방법
				③ 대한민국
				④ 10-2244504
				⑤ 2019
7	석사	신수민	특허	① 김종성, 김기윤, 신수민, 강수진
				② 데이터베이스 암호화 기반의 안티 포렌식 해제 장치 및 방법
				③ 대한민국
				④ 10-2319709
				⑤ 2021

8	박사	박호중	특허	① 박호중, 김예원, 염용진, 강주성
				② 독립성 측정을 이용한 엔트로피 관리 장치 및 방법, 이를 이용한 난수 생성 장치
				③ 대한민국
				④ 10-2155007
				⑤ 2020
9	박사	김예원	특허	① 염용진, 김예원, 박호중, 강주성
				② 안티-인버전 함수를 이용한 화이트 박스 암호 인코딩 장치 및 방법
				③ 대한민국
				④ 10-2319699
				⑤ 2021
10	석사	박한별	특허	① 한동국, 박한별, 심보연
				② 인공신경망을 이용한 RSA 암호에 대한 부채널 분석 방법 및 장치
				③ KR
				④ 10-2554852
				⑤ 2023
11	석사	이태호	특허	① 이태호, 한동국, 김일주, 심보연, 한재승
				② LAC에 대한 부채널 분석 장치 및 방법
				③ KR
				④ 10-2312379
				⑤ 2021
12	박사	한재승	특허	① 한동국, 김수진, 김연재, 심보연, 한재승
				② 블록암호에 대한 상관전력 분석 방법 및 장치
				③ KR
				④ 10-2308517
				⑤ 2021
13	박사	문재근	특허	① 이지우, 한동국, 심보연, 문재근, 김현숙, 신임섭
				② 부채널 정보 분석에 따른 암호 알고리즘 안전성 검증 시스템 및 그 시스템의 제어 방법
				③ KR
				④ 10-2297318
				⑤ 2021
14	석박사통합	이종혁	특허	① 한동국, 김주환, 이종혁, 임한섭
				② 오류 주입 공격 장치 및 방법
				③ KR
				④ 10-2344915
				⑤ 2021
15	석사	김일주	특허	① 한동국, 김일주, 심보연, 이태호, 한재승
				② NTRU LPRime 암호에 대한 부채널 분석 장치 및 방법
				③ KR
				④ 10-2280708
				⑤ 2021

16	석사	임한섭	특허	① 임한섭, 이종혁, 한동국
				② 오류 주입 공격 시스템
				③ KR
				④ 10-2331835
				⑤ 2021
17	박사	임성혁	특허	① 한동국, 이종혁, 임성혁
				② 차분 오류 공격 방법 및 장치
				③ KR
				④ 10-2306636
				⑤ 2021
18	박사	델핀 라즈	특허	① 박수현, 신수영, 케사리 마리 델핀라즈
				② 수중 네트워크 관리 시스템
				③ 대한민국
				④ 10-2434716
				⑤ 2022
19	박사	염선호	특허	① 박수현, 이정국, 이진영, 염선호, 임용곤, 신수영
				② 무선 통신 기기 및 이의 동작 방법
				③ 대한민국
				④ 10-2446356
				⑤ 2022
20	박사	위한샘	특허	① 이옥연, 이재훈, 윤승환, 위한샘, 장찬국
				② 5G SIDF 암호처리장치 및 그 방법
				③ 대한민국
				④ 10-2507160
				⑤ 2023
21	석사	김연재	기술이전	① 김연재,한동국
				② Glitch-Free threshold implementation PIPO에 대한 기술이전
				③ 에이치투씨글로벌㈜
				④ 5,500,000원
				⑤ 2023
22	석사	문혜원	기술이전	① 문혜원, 허재원, 한동국
				② 딥러닝 가속기 오류주입 검증 관련기술
				③ (재)한국기계전기전자시험연구원
				④ 5,500,000원
				⑤ 2023
23	석박사통합	김주환	기술이전	① 김주환, 한동국
				② 딥러닝 가속기 물리채널 기반 오류주입 취약성 검증 SW에 대한 기술이전
				③ 에이치투씨글로벌㈜
				④ 5,500,000원
				⑤ 2023

24	석사	김수진	기술이전	① 김수진, 이종혁, 한재승, 임성혁, 이태호, 김연재, 우지은, 안성현, 문혜원, 한동국
				② 대칭키 암호 오류주입 기반 암호키 취약성 검증 도구 개발 기술 및 Know-How
				③ 쿤텍 주식회사
				④ 110,000,000원
				⑤ 2021
25	석사	이세윤	기술이전	① 이세윤, 이옥연
				② 무인이동체 보안을 위한 암호장비 설계기술
				③ 시옷랩 주식회사
				④ 5,000,000원
				⑤ 2021
26	석사	윤혜진	기술이전	① 윤혜진, 이옥연
				② 양자암호모듈(qSIM) 모듈 기반 키주입 기술 / 양자암호모듈(qSIM) 모듈 기반 영상 보안 장비 연동 기술
				③ 신진아이앤씨(주)
				④ 100,000,000원
				⑤ 2023

총 이공계열 참여대학원생 수	**석사**	163	**제출 요구량**	26
	박사	70		
	석박사통합	19		
	계	252		

- 참여학생 허욱은 메신저, SNS를 포함한 다양한 서비스에서 활용되는 데이터베이스인 SQLite에서 내부 내용의 검색을 위해 생성된 색인데이터를 활용하여 삭제된 메시지를 복구하는 'FTS 색인데이터 기반의 삭제 채팅 메시지 복구 장치 및 방법' 을 개발하였으며, 실제 세계적으로 가장 많이 사용되고 있는 WhatsApp, WeChat 및 KakaoTalk에서 활용이 가능함을 보임
- 참여학생 김한기는 기밀성 제공이 필요한 다양한 정보보호 환경에서 부채널 분석에 저항성을 갖는 경량 블록암호 PIPO를 개발했음. '부채널 공격 대응이 용이한 128비트 경량 블록 암호화 방법 및 이를 이용한 장치' 의 특허 등록을 통해 PIPO 블록암호가 독창성이 있음을 밝히고 기존보다 더 넓은 범위의 경량 환경 디지털 기기에 보안 서비스를 제공가능한 포석을 만들어준 것으로 국내 보안 시장에 기여하였음
- 참여학생 김기윤은 최근 다양한 메신저에서 보안을 위해 도입하고 있는 종단간 암호화 기법의 매커니즘을 분석하여 키교환 과정에서 교환된 키를 획득하여 기기에 남아있는 암호화된 데이터를 복호화하는 '종단간 암호화가 적용된 파일에 대한 복호화 장치 및 방법'을 개발함. 이를 사용하여 암호화된 사용자 데이터를 복호화하는 것으로 디지털 포렌식 수사에 기여할 수 있음
- 참여학생 전용진은 경량 블록암호 프리미티브의 효율적이고 안전한 설계 방식인 'DLBN이 3 이상인 조건을 만족하는 확장 에스박스 및 이를 이용한 비트 연산 방법' 을 개발하였으며, 향후 적은 리소스를 갖는 경량 환경에서의 블록암호 설계를 위한 연구에 기여하였음
- 참여학생 강수진은 안티포렌식으로 작용할 수 있는 미디어 파일에 대한 암호화를 해제하는 방안을 개발함. 파일명 및 확장자 변경 또는 데이터 삽입을 통해 미디어 파일을 조작하는 것은 안티포렌식 기법으로 작용할 수 있음. 따라서 사용자 비밀번호 기반으로 암호화된 미디어 파일 복호화하고 암

호화에 사용된 사용자 입력 비밀번호 복구하는 ‘미디어 파일에 대한 안티 포렌식 해제 장치 및 방법’을 개발하였으며, 이는 디지털 포렌식 수사에 도움이 될 수 있음

- 참여학생 이세훈은 주요 개인정보 및 대화 정보를 암호화하는 보안 메신저인 SureSpot의 암호화된 데이터를 Android와 iOS 환경에서 복호화 연구를 수행하여 이를 기반으로 삭제된 데이터를 복구하는 방안인 ‘캐시 파일을 이용한 삭제 메시지 복구 장치 및 방법’을 개발함. 디지털 포렌식 수사에서사용자가 삭제한 대화내용을 복구하는 것은 중요한 연구 대상이며, 개발한 기술을 바탕으로 암호화 및 캐시화 된 데이터를 복구하여 메산저에서 삭제된 대화 내용의 일부를 복구할 수 있음. 이를 통해 원활한 디지털 포렌식 수사를 가능하게 함
- 참여학생 신수민은 SQLCipher 모듈을 통해 SQLite 기반의 데이터베이스 암호화 기능을 제공하는 두종류의 애플리케이션을 분석하여 ‘데이터베이스 암호화 기반의 안티 포렌식 해제 장치 및 방법’을 개발하였음. 이는 암호화된 데이터베이스에 존재하는 사용자 정보를 획득할 수 있는 기반 기술이 되며, 효율적인 디지털 증거 획득을 기반으로 효율적인 디지털 포렌식 수사를 가능하게 함
- 참여학생 박호중은 진난수생성기의 엔트로피 관리를 위한 독립성 검증을 위하여 필요한 엔트로피 소스 독립성 측정 장치의 관리 방법을 개발했음. ‘독립성 측정을 이용한 엔트로피 관리 장치 및 방법, 이를 이용한 난수 생성 장치’의 특허 등록을 통해 기존 독립성 측정 성능보다 개선된 진난수생성기의 엔트로피 소스 독립성 검증 기법 및 독립성 측정을 위한 시스템의 관리 방법을 개발하고 이를 실체화하기 위한 장치 구성을 설계함으로써 국내 암호 시스템 안전성 향상에 기여하였음
- 참여학생 김예원은 화이트 박스 암호에 필요한 인코딩 기법으로써 안티-인버전 함수에 대하여 연구하고 이를 적용하기 위한 구조를 개발하였음. ‘안티-인버전 함수를 이용한 화이트 박스 암호 인코딩 장치 및 방법’의 특허 등록을 통해 안티-인버전 함수가 기존 화이트박스 암호의 인코딩 기법과 비교하여 보다 효율적임을 보이고 이를 통해 화이트박스 암호가 다수 활용되는 핀테크 등의 국내 보안 시장에 기여함
- 참여학생 박한별은 인공신경망을 이용해 RSA 암호의 비밀키 지수를 복구하는 부채널 공격 방법인 ‘인공신경망을 이용한 RSA 암호에 대한 부채널 분석 방법 및 장치’ 특허를 개발함. 이 특허는 가장 많이 사용되는 공개키 암호 중 하나인 RSA에 대한 부채널 공격 기법으로 인공신경망을 통해 더 폭넓은 관점에서의 부채널 안전성 검증을 가능하게 함. 이를 통해 국내 공개키 암호 안전성 평가 기술과 국내 보안 시장에 기여하였음
- 참여학생 이태호는 양자 내성 암호 LAC에 대한 부채널 분석 방법인 ‘LAC에 대한 부채널 분석 장치 및 방법’ 특허를 개발함. 이 특허는 키 교환 메커니즘인 LAC의 교환되는 세션키를 복구하는 부채널 공격 방법을 제시하여 이를 통해 양자 내성 암호 LAC의 부채널 안전성 및 안전성 검증 방법에 활용될 수 있음. 이를 통해 국내 양자 내성 암호 기술 향상에 기여하였음
- 참여학생 한재승은 비트슬라이스 블록암호에 대한 상관전력 분석의 성능 향상 기법인 ‘블록암호에 대한 상관전력 분석 방법 및 장치’ 특허를 개발함. 이는 대상 암호의 구조를 통한 이론적 계산을 통해 대표적인 부채널 분석 방법인 상관전력 분석의 성능을 개선하는 공격 대상 비트를 선정하는 방법임. 이를 통해 블록암호의 부채널 안전성 평가 기술과 부채널 안전성 향상에 기여할 수 있음
- 참여학생 문재근은 대상 장치의 암호 알고리즘 부채널 안전성 검증 시스템을 운용하는 방법인 ‘부채널 정보 분석에 따른 암호 알고리즘 안전성 검증 시스템 및 그 시스템의 제어 방법’ 특허를 개발함. 이는 암호 장치의 부채널 정보 수집을 위한 트리거 신호 생성단계, 신호 수집 단계, 부채널 정보 분석 단계로 나뉨. 이를 통해 부채널 분석 안전성 평가 및 검증 기술 발전에 기여하였음
- 참여학생 이종혁은 블록암호 AES, ARIA의 차분 오류 주입 공격을 통한 암호 비밀키 복구 방법인 ‘오류 주입 공격 장치 및 방법’ 특허를 개발함. 이 특허는 블록암호 AES와 ARIA의 암호 알고리즘 구조에 오류 주입 시점 및 위치, 그리고 획득한 오류 암호문을 통해 암호의 비밀키를 복구하는 차분 오류 공격을 다룸. 이를 통해 블록암호 오류주입 공격 안전성 평가 및 검증 기술 발전에 기여하

였음
- 참여학생 김일주는 양자 내성 암호 NTRU LPRime에 대한 부채널 분석 방법인 ‘NTRU LPRime 암호에 대한 부채널 분석 장치 및 방법’ 특허를 개발함. 이 특허는 키 교환 메커니즘인 NTRU LPRime에서 교환되는 세션키를 복구하는 부채널 공격 방법을 제시하여 이를 통해 양자 내성 암호 NTRU LPRime의 부채널 안전성 및 안전성 검증 방법에 활용될 수 있음. 이를 통해 국내 양자 내성 암호 기술 향상에 기여하였음
- 참여학생 임한섭은 오류 주입 공격 대상 기기 제어, 트리거 신호 발생을 포함한 오류 주입 공격 시스템 구성 방법인 ‘오류 주입 공격 시스템’ 특허를 개발함. 이 특허는 오류 주입 공격을 위해 대상 기기의 제어 및 트리거 신호 발생, 오류 주입 및 출력 수집부를 포함하여 오류 주입 공격 수행의 전체 시스템 구성 방법을 다룸. 이를 통해 오류주입 공격 안전성 평가 및 검증 기술 발전에 기여하였음
- 참여학생 임성혁은 경량 블록암호 LEA의 차분 오류 주입 공격을 통한 암호 비밀키 복구 방법인 ‘차분 오류 공격 방법 및 장치’ 특허를 개발함. 이 특허는 LEA 암호 알고리즘의 특성에 따라 중간값의 대수적 표현을 통한 차분 오류 공격 논리를 포함하며, 최종적으로 오류 주입 시점 및 위치 그리고 획득한 오류 암호문을 통해 비밀키를 복구하는 차분 오류 공격을 다룸. 이를 통해 블록암호 오류주입 공격 안전성 평가 및 검증 기술 발전에 기여하였음
- 참여학생 델핀라즈는 다층적 관리 구조를 통해 수중 환경에서의 네트워크 및 장치 관리를 혁신적으로 개선하는 기술을 제시함. 리 스테이션, 게이트웨이, 마스터 및 서브 에이전트의 통합으로 복잡한 수중 조건에서도 효율적인 데이터 관리와 통신 네트워크 구성이 가능하며, 장치의 움직임에 기초한 실시간 정보 업데이트와 네트워크 재구성이 탁월한 자동화와 유연성을 제공함.
- 참여학생 염선호는 다양한 광 차단율을 가진 필터와 수광 소자를 활용하여 환경의 탁도를 정밀하게 측정하는 혁신적인 방법을 제공함. 무선 기기의 위치와 환경 조건을 감지하는 데 사용될 수 있어, 예를 들어 수중 통신 장비에서 매우 유용하게 사용 가능하며 무선 통신 기기의 환경적 적응력과 정확성을 향상시킴으로써 보다 안전하고 신뢰할 수 있는 통신 네트워크 구축에 기여함.
- 참여학생 위한샘은 5G 이동 통신망에서 SUPI를 ECIES로 암호화하여 SUCI를 생성하는 UE 단말들, 이를 받아 처리하는 SEAF 단위, 그리고 인증을 수행하는 AUSF 단위를 포함하는 보안 시스템과 여러 GPU 중 하나를 선택하여 개인키로 SUCI를 복호화하는 SIDF 유닛을 통해 대량의 UE 접속 시 SIDF의 부하를 감소시키고 처리 시간을 줄일 수 있는 방법에 대해 특허 등록을 진행함
- 참여학생 김연재는 하드웨어 부채널 분석 대응기법인 Threshold implementation을 국내 경량 블록암호 PIPO에 적용하는 방법을 ‘Glitch-Free threshold implementation PIPO에 대한 기술이전’을 통해 에이치투씨글로벌(주)에 기술이전함. 해당 기술을 이용하면 부채널 분석에 효율적인 블록암호 PIPO에 부채널 안전성을 확보할 수 있고 이를 사용한 데이터 보호를 통해 국내 보안 시장에 기여할 수 있음
- 참여학생 문혜원은 글로벌 회사인 Riscure 사의 오류 주입 장비 Inspector의 매뉴얼을 한글화하며 정리한 문서를 ‘Inspector User Manual – Fault Injection 한글화 매뉴얼’을 통해 에이치투씨글로벌(주)에 기술이전함. 해당 매뉴얼은 Inspector 장비를 이용한 오류 주입 시스템의 하드웨어 및 소프트웨어 구성 방법, 대상 기기에 대한 오류 주입 수행 방법을 다룸. 해당 기술은 오류 주입 안전성 평가 및 검증 기술에 활용될 수 있으며, 이를 통해 국내 보안 시장에 기여할 수 있음
- 참여학생 김주환은 딥러닝 가속기에 대한 오류주입 안전성 평가 방법인 ‘딥러닝 가속기 물리채널 기반 오류주입 취약성 검증 SW에 대한 기술이전’을 통해 에이치투씨글로벌(주)에 기술이전함. 해당 기술을 이용하면 딥러닝 가속기에 대한 오류주입 취약성 검증을 자동화할 수 있고 이를 통해 미래 기술인 딥러닝 기술의 보안성 평가 기술 및 안전성 향상에 기여할 수 있음
- 참여학생 김수진은 여러 대칭키 암호에 대한 차분 오류 공격 논리 및 공격 소프트웨어 도구 개발

기술, 오류주입 공격 시스템 구성 기술인 ‘대칭키 암호 오류주입 기반 암호키 취약성 검증 도구 개발 기술 및 Know-How’를 쿤텍 주식회사에 기술이전함. 해당 기술은 국내외 대칭키 암호들에 대한 여러 유형의 차분 오류 공격, 공격을 위한 소프트웨어 도구 및 시스템 구성 방법을 다룸. 이를 이용하면 대칭키 암호 모듈에 대한 오류주입을 통해 암호키 취약성을 검증할 수 있고 이를 통해 암호 모듈의 보안성 평가 기술 및 안전성 향상에 기여할 수 있음

- 참여학생 이세윤은 무인 이동체에 대한 보안을 위한 다양한 방안 중에서 암호 장비를 이용하는 보안을 위해 암호 장비에 대한 설계 및 설계 기술에 대해 개발하여 이를 시옷랩 주식회사에 설계 방안과 이에 대한 기술에 대해 기술이전을 실시함
- 참여학생 윤혜진은 양자암호모듈(qSIM)에 키를 주입하는 기술을 개발하고 양자암호모듈(qSIM)을 이용하여 영상 보안 장비를 연동하여 동작하는 기술을 개발하였으며, 이에 대해 신진아이앤씨(주)에 기술이전을 수행하였음

3.2 참여대학원생 연구 수월성 증진 실적

▣ 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 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 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

- 교육연구단의 원활한 연구수행을 위하여 2014년 10월 신축한 산학협력관에 교육연구단장 또는 사업참여교수의 요청에 따라 현재 산학협력관 306호(48㎡)를 연구공간으로 배정하여 지원하고 있음
- 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 수업 연한을 단축할 수 있도록 하고 있음
- 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
- 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 부여하고 있음

4. 참여교수의 교육역량 대표실적

4.1 참여교수의 교육역량 대표실적

<표 2-8> 해당 산업·사회 문제 해결분야 문제해결을 위한 참여교수의 교육역량 대표실적

<table>
<tr><th rowspan="2">연번</th><th>참여교수명</th><th>참여기간
(YYYYMMDD-
YYYYMMDD)</th><th>연구자등록번호</th><th>세부전공분야</th><th>대학원 교육 관련
대표실적물</th><th>DOI번호/ISBN/인
터넷 주소 등</th></tr>
<tr><td colspan="6">참여교수의 교육 관련 대표실적의 우수성</td></tr>
<tr><td rowspan="2">1</td><td>김종성</td><td>20200901-202
40229</td><td>10182694</td><td>정보보호/암호
학</td><td>디지털 포렌식 개론
강의</td><td></td></tr>
<tr><td colspan="6">디지털포렌식개론과목 개설을 통해 안티포렌식 기술에 대한 이해와 안티포렌식 기술을 우회하기 위한 안티안티포렌식 기술을 교육하고 실사례를 분석함으로써 원리를 교육함. 주요 내용으로는 다양한 OS 및 애플리케이션에 적용된 다양한 암호 기반 안티 포렌식 기술에 대한 분석을 수행함. 특히, 모바일 기기 제조사에서 제공하는 암호화 백업 기능을 분석하여 백업된 데이터의 복호화를 통해 모바일 OS의 데이터 보호 기능을 우회하여 데이터를 추출하고 분석하는 방법을 실습함. 또한, 일부 애플리케이션에 적용된 암호학적 취약점을 활용하여 암호화 키 획득 없이도 데이터 복호화 및 분석이 가능함을 Protonmail 및 카카오톡의 사례를 통해 소개함. 그 외에도 디지털 포렌식 분야 최신 논문에 관한 발표 세미나를 진행하여 최신 동향과 사례 연구 분석을 진행하였음.</td></tr>
<tr><td rowspan="2">2</td><td>김종성</td><td>20200901-202
40229</td><td>10182694</td><td>정보보호/암호
학</td><td>대칭키 암호 분석
강의</td><td></td></tr>
<tr><td colspan="6">대칭키 암호 분석 과목 개설을 통해 다양한 대칭키 암호의 설계 원리와 분석 기술을 교육하고 실제 사용되고 있는 다양한 암호 알고리즘에 대한 Crypt Analysis 실습을 진행함. 주요 내용으로는 암호화 과정에서의 근사적 선형 관계식을 찾는 선형 공격(linear cryptanalysis), 입력값의 변화에 따른 출력값의 변화를 분석하는 차분 공격(differential cryptanalysis)에 대한 이론 강의를 수행함. 또한, 차분 공격을 기반으로 하는 부메랑 공격 및 rectangle attack에 대하여 소개함. 이론적인 분석방법 외에도 무차별 대입 공격(brute-force attack)을 기반으로 하는 공격 기법과 효율적인 공격을 위한 사전 연산을 통한 Rainbow Table 및 TMTO (Time Memory Trade-Off) 최적화 기법에 대한 실습을 수행하였음. 그 밖에도 최신 암호분석 논문 세미나를 진행하여 양자 컴퓨팅 기술을 활용한 최신 암호 분석기술과 사례 분석을 진행하였음.</td></tr>
<tr><td rowspan="2">3</td><td>유일선</td><td>202303-현재</td><td>10146537</td><td>정보보안</td><td>금융네트워크보안</td><td></td></tr>
<tr><td colspan="6">금융네트워크보안 과목 개설을 통해 초연결 시대의 핵심분야인 이동통신과 사물인터넷을 위한 보안 프로토콜과 국제 표준기구 ISO/IEC에서 권고하는 보안 프로토콜의 정형화 검증기술을 강의함으로써 대학원생들의 전문·연구역량 강화에 기여함. 특히, 현재 전세계 8.5억명이 사용하고 있는 5G 네트워크를 중심으로 가능한 공격 시나리오 및 사례를 소개하였음.</td></tr>
<tr><td rowspan="2">4</td><td>김동찬</td><td>20200901-202
40229</td><td>11579260</td><td>암호학</td><td>논문</td><td>https://link.springer.com/chapter/10.1007/978-3-031-46495-9_8</td></tr>
<tr><td colspan="6">PALOMA는 부호 기반 키설정(key encapsulation mechanisom) 양자내성암호로, KpqC 양자내성암호 공모전 2라운드 암호로 선정되어 2024년 2라운드를 준비하고 있음. 본 연구를 통해 국제 부호 기반 암호학회 CBCrypto 2023에 채택되었고, 추가 심사를 거쳐 2023년 10월 논문으로 게재되었음. 본 연구 결과를 대학원 강의 ‘공개키암호 분석이론’의 교육자료로 활용하였으며, 양자 컴퓨팅 환경에서의 기존 암호체계의 문제점을 학생들에게 제시하여 우수한 교육 효과를 얻었음. 연구 결과를 교육에 적극적으로 활용함으로써, 학생들은 실무에 적용 가능한 기술과 그에 따른 보안적 고려 사항을 습득하였으며 이는 교육의 효과적인 전달과 지식의 실용적 활용을 도모하는 데 크게 기여하였음.</td></tr>
</table>

<table>
<tr><td rowspan="2">5</td><td>강주성</td><td>20200901-20240229</td><td>1012 7144</td><td>정보보호/암호학</td><td>난수성분석론 강의</td><td></td></tr>
<tr><td colspan="6">강주성 교수는 난수성분석론 과목 개설을 통해 암호 시스템의 다양한 분야에 활용되는 난수의 암호학적 생성 원리와 출력 난수의 엔트로피 평가 방법을 교육하고 잘못된 방법으로 생성된 난수에 의해 암호 시스템에 적용될 수 있는 공격 위협에 대하여 교육함. 특히 최근 양자내성암호에 사용되는 난수발생기를 조작함으로써 비밀키를 탈취하는 공격 기법이 재언급되기 시작함에 따라 해당 공격 사례를 분석하고 이러한 문제를 해결하기 위하여 난수 활용 시 고려해야 할 점들을 교육함. 암호학적으로 안전한 난수 생성과 관련한 주요 강의 내용으로 NIST의 국제 표준 특별 간행물 SP 800-22과 SP 800-90B에 명시된 난수성 평가 방법과 엔트로피 추정 기법 및 정보보안 프로토콜과 암호 알고리즘 사용 환경에 따른 난수 사용 주기에 대한 이론 강의를 수행함.</td></tr>
<tr><td rowspan="2">6</td><td>염용진</td><td>20200901-20240229</td><td>1009 0653</td><td>정보보호/암호학</td><td>보안기술표준분석 및 구현 강의</td><td></td></tr>
<tr><td colspan="6">염용진 교수는 보안기술표준분석 및 구현 과목 개설을 통해 국제표준화기구(ISO/IEC), 미국 국가표준기술연구원(NIST), IETF등에서 발간하는 보안기술 관련 표준을 학습함으로써 안전한 구현 기법과 ISO/IEC, IETF등의 국제표준기술에 대한 이해를 바탕으로 표준기술을 활용한 보안시스템을 안전하게 설계할 수 있는 능력을 배양함. 표준화기구에서 제공하는 검증/평가 문서들을 분석함으로써 암호 알고리즘들의 단순한 조합만으로는 막을 수 없는 시스템 공격자 유형에 대하여 설명하고, 이를 막기 위하여 각 암호 요소를 조합할 때 참고하는 가이드라인을 학습함으로써 전체 보안 인프라에 대한 공격 가능성을 파악하는 능력을 배양함. 또한 관련 분야 전문 인력을 초청하여 나아가 기업 및 기관에서 보안 인프라를 구축함에 있어 고려하는 전반적인 공격 대응 기법의 기반 원리를 교육하는 이론 강의를 수행함.</td></tr>
<tr><td rowspan="2">7</td><td>서석충</td><td>20210301-20221231</td><td>10875717</td><td>정보보호/암호학</td><td>암호소프트웨어구현 강의</td><td></td></tr>
<tr><td colspan="6">서석충 교수는 양자내성암호 분석 및 구현과 관련된 산업보안 기술과 관련하여 교과과정을 개설하였음. 양자내성암호 분석 및 구현 관점에서 NIST 양자내성암호 공모전에 제안되고 표준화 대상으로 선정된 알고리즘에 대한 구현적 관점의 분석을 교육함. 또한, 성능 및 메모리가 제한된 임베디드 환경에서의 구현 방법론 교육과 고성능 병렬 환경에서의 구현 방법론에 대한 교육을 진행하였음.</td></tr>
<tr><td rowspan="2">8</td><td>한동국</td><td>20200901-20240229</td><td>10128486</td><td>정보보호/암호학</td><td>금융디바이스공격론 강의</td><td></td></tr>
<tr><td colspan="6">한동국 교수는 금융디바이스공격론 과목 개설을 통해 암호 알고리즘이 수학적으로 안전하게 설계되어 있더라도 실제 디바이스에서 연산이 수행되면서 발생하는 부채널 정보(연산 수행 시간, 소비 전력, 방출 전자파 등)를 이용하여 비밀 키를 탈취하는 물리적인 취약점이 존재한다는 사실에 있어서 이에 대한 분석 방법과 대응기법을 설계함으로써 원리와 실습을 교육함. 대응기법 교육시, 실험실 환경에 비해 부채널 정보 수집 단계에서 어려움이 존재하는 경우 대응기법을 극복하기 위한 방법 또한 교육함으로써 역공학 역량을 향상시킴. 이러한 교육을 통해 부채널 정보를 통해 비밀 정보를 탈취하는 것 뿐만 아니라 디바이스 역공학 및 이상 탐지에 활용 가능함을 보임으로써, 백도어 탐지, 금융 IC 카드와 USIM 등에 대한 물리적 보안과 관련된 많은 산업/사회 문제 해결에 기여함.</td></tr>
</table>

9	박수현	20200901-20240229	10056675	통신네트워크	시물지능망특론 강의	
	사물지능망특론 과목을 통해 IoT 및 엣지 컴퓨팅 시스템을 구현하는 방법을 학습함으로써, 정보보안 관점에서 산업 및 사회 문제를 해결하는 데 있어 중요한 실적을 달성함. 특히, 이 과정에서 학습한 보안 기술과 프로토콜은 데이터의 기밀성과 무결성을 보장하는 동시에, IoT 기기들 간의 안전한 통신을 가능하게 함. 이를 통해, 산업 자동화, 스마트 홈, 건강 관리 시스템 등 다양한 분야에서의 보안 취약점을 해결하고, 사용자의 프라이버시를 보호하는 데 기여함. 또한 사물인터넷 및 디지털 트윈, 엣지 컴퓨팅시스템에 대한 최신 논문 관련 발표 세미나를 진행함으로써 최신 동향과 사례 연구 분석을 진행하였음.					
총 환산 참여교수 수		10.57		**제출 요구량**	3 ~ 5	

5. 교육의 국제화 전략

5.1 교육 프로그램의 국제화 실적

▶ 유일선 교수팀

- 필리핀의 최초 대학인 산카를로스 대학과 협력하여 국제 저널에 논문을 발표하였으며, 더 나아가 해당 주제를 통해 인슐린 펌프를 위한 경량의 비정상 행위탐지를 주제로 초청강연을 함.
- 전 세계 암호분야에서 최정상급에 위치하고 있는 오세아니아 월런공대학교와 국제 공동 연구를 수행 중임.
- 일본의 최고 연구기관 AIST와 지속적인 연구협력을 수행해왔으며, AIST의 신성한 연구원과 국제 협력 멘토를 채결하여 지속적인 국제 협력을 수행해옴.
- 본 교육연구단은 국제적 경쟁력을 갖춘 정보보안 전문인력 양성을 위해 국제학회 참석 및 논문 발표를 독려하고 있음.
- 해당 기간 국제 저널 36건, 국제 학회 20건의 논문을 발표하였음.

▶ 이옥연 교수팀

- 참여학생 장찬국, 위한샘, 김현기는 국내 2개 대학(국민대학교, 순천향대학교), 해외 1개 대학(Georgia State University)의 2개 연구실로 총 3개 대학이 참여하는 국제 공동연구를 수행하였음.

▶ 한동국 교수팀

- 참여학생 이종혁, 김일주, 박한별, 임한섭, 이태호, 임성혁, 한재승, 김수진, 김연재, 문혜원, 안성현, 우지은, 허재원은 국내 기관(국민대학교, 한국시스템보증(주))와 프랑스 기관(Texplained)이 참여하는 국제 공동연구 “딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발”을 수행하였음.
- 2021년 3월에 싱가폴 난양기술대학교 연구원을 초청하여 Cold boot attack과 Machine Learning 기반 부채널 분석 주제로 연구 교류를 수행하였음.

▶ 박수현 교수팀

- 참여학생 황아리, 신하 쉬르티카는 핀란드 savonia 대학과 협력하여 국제 저널에 논문을 발표하였음.

▶ 최은미 교수팀

- 최은미 교수팀은 인도의 VIT 벨로레 공과 대학교와 융합보안 핵심인재 양성사업 성과 활용을 위한 협력확인서 MOU 계약을 체결하였음.

5.2 참여대학원생 국제공동연구 실적

<표 2-9> 평가 대상 기간(2020. 9. 1. ~ 2024. 2. 29.) 내 참여대학원생 국제공동연구 실적

연번	공동연구 참여자			상대국/소속기관	연구주제	연구기간 (YYYYMM-YYYYMM)
	교육연구단		국외 공동연구자			
	참여 대학원생	지도교수				
1	고용호; 권호석; 손대현; 오종민; 김건우	유일선	Willy Susilo	호주/월런공대학교	본 연구는 호주 월런공대학교의 Institute of Cybersecurity and Cryptology (iC2)와 협력하여 진행하는 국제공동연구과제로 안전한 차세대 IoT 통신 환경 구축을 위한 양자내성 암호 최적화 및 보안 프로토콜 적용 연구를 수행하였음	202205-202402
2	김현기	이옥연	김동현	미국/조지아 주립대학교	UTM 5G 엣지 드론 내 보안 파라미터의 딥러닝 기반 생성 및 탐지 연구	202108-202204
3	위한샘	이옥연	Zhipeng Cai	미국/조지아 주립대학교	UTM 5G MEC 환경에서 블록체인 기반 데이터 보안 및 인증체계 연구	202108-202204
4	장찬국	이옥연	Yingshu Li	미국/조지아 주립대학교	UTM과 5G 엣지 클라우드 융합환경에서의 End-to-End 보안 설계 연구	202108-202204
5	김수진; 김연재; 김일주; 문혜원; 박한별; 안성현; 우지은; 이종혁; 이태호; 임성혁; 임한섭; 한재승; 허재원	한동국	Olivier Thomas	프랑스/Texplained	본 연구는 국제공동연구 과제 “딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발”을 통해 수행됨	201912-202211

- 유일선 교수팀의 참여학생 김건우는 차세대 네트워크 환경에 대응하기 위한 인증 프로토콜 설계 및 검증을 목표로 하는 국제 공동연구 ‘안전한 차세대 IoT 통신 환경 구축을 위한 양자내성암호 최적화 및 보안 프로토콜 적용 연구’ 를 수행함.
- 본 공동연구는 국내 1개 대학(국민대학교)의 3개 연구실과, 해외 대학 (월런공대학교 Institute of Cybersecurity and Cryptology)이 참여함.
- 참여학생 김건우는 국제공동연구를 위해 2023년 2월 호주 월런공대학교에 방문하여 국제 협력 방안 논의 및 추후 연구방향에 대한 논의함.
- 참여학생 장찬국, 위한샘, 김현기는 국제공동연구를 위해 21년 8월 1일부터 22년 4월 29일까지 총 9개월 동안 미국 Georgia State University에서 협업을 위한 파견 근무를 수행하였음.
- 국민대학교는 조지아 주립대학교의 Cai 교수팀과의 파견연구를 통해 기존 국민대학교가 보유하지 못한 블록체인을 통한 인증 시스템 설계 기술 및 딥러닝 기반 식별기술을 접목하여 UTM의 드론 및 end 노드에서 사용하는 보안 파라미터 생성 및 탐지 연구와 UTM에서 필요한 인증 시스템 및 저장 데이터 보안 연구를 수행했음. 각 참여대학원생은 파견 기간 내에 총 SCIE급 논문 2건, 국내 학술대회 1건, 기술문서 6건의 정량적 실적을 달성함.
- 한동국 교수팀의 참여대학원생 김수진, 김연재, 김일주, 문혜원, 박한별, 안성현, 우지은, 이종혁, 이태호, 임성혁, 임한섭, 한재승, 허재원은 산업통상자원부에서 관리하는 국제공동연구 과제 “딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발”을 2019년 12월부터 2022년 11월까지 수행함. 본 과제는 RISC-V 하드웨어에 대한 보안 시스템 설계 및 개발을 다루며 세부 연구개발 목표는 통합시스템 개발, 전력 분석, 칩 보안 분석으로 나뉨. 한동국 교수팀은 전력 분석 부분을 맡아 RISC-V에 대한 전력 및 전자파 측정 시스템, 측정 전력으로부터 이상동작 탐지 및 비밀 정보 복구 시스템을 연구 개발함.

4단계 BK21사업

Ⅲ. 연구역량 영역

Ⅲ. 연구역량 영역

1. 참여교수 연구역량

1.1 국내 및 해외기관 연구비 - 시스템 직접 입력

1.2 연구업적물

① 참여교수 대표연구업적물의 우수성 - 시스템 직접 입력

② 참여교수 대표연구업적물의 적합성 - 시스템 직접 입력

③ 참여교수 특허, 기술이전, 창업 실적의 우수성 - 시스템 직접 입력

④ 연구의 수월성을 대표하는 연구업적물 (최근 10년)

<표 3-5> 최근 10년간 참여교수의 해당 산업·사회 문제 해결분야 대표연구업적물

연번	대표연구업적물 설명
1	▶ 산업·사회 문제 해결을 위한 랜섬웨어 대응 연구 진행 - 김종성 교수과 그 연구팀은 2018년도부터 6년간 한국인터넷진흥원과 랜섬웨어 분석에 관한 연구를 지속적으로 진행하고 있음. - 약 100여 종의 랜섬웨어 상세 동작 과정을 분석하였으며, 그중 랜섬웨어 취약점을 이용하여 20종의 랜섬웨어 복호화 도구를 개발함. - 2019년, 상반기 점유율이 높은 랜섬웨어 3종(Gandcrab v5, Clop, Sodinokibi)과 신규 랜섬웨어 2종(Phobos, LooCipher)을 역공학 분석하여 암호화 프로세스를 분석하고, 그중 LooCipher 랜섬웨어의 취약점을 기반으로 복호화가 가능함을 제시하였음. - 2019년, 오픈소스 랜섬웨어 변종 중 하나인 Donut 랜섬웨어의 연구를 수행하여 메모리 분석을 통한 복호화 방법을 제안하고, 프로그램 구현 및 실험을 통해 복호화 방안의 검증을 수행함. - 2019년 하반기에 등장한 Ragnar Locker 랜섬웨어를 상세 분석하여 파일 암호화 시 사용하는 스트림 암호에 동일한 키를 재사용하는 취약점을 밝혀냄. 이를 기반으로 복호화 방안을 제시하고 취약점 활용 방안을 제안함. - 2020년, 주요하게 활동한 랜섬웨어인 5ss5c와 Immuni 랜섬웨어의 암호화 프로세스를 분석하고 각각 볼륨 섀도 복사본과 암호키 생성에 필요한 seed 전수 조사를 통한 데이터 복구 방안을 제시함. - 2020년, 국내를 타겟으로 공격을 수행한 Magniber v2 랜섬웨어를 분석하여 자체 개발한 의사 난수 생성기의 취약점을 밝혀냄. 이를 통해 암호화된 데이터를 복호화하는 방법과 복호화 여부를 검증할 수 있는 방법을 제시함. - 2022년, 국내·외를 타겟으로 다수의 공격을 수행하여 FBI의 경고를 받은 Hive 랜섬웨어를 분석하여 취약점을 발견함. 해당 취약점을 통해 감염 파일의 90% 이상을 복구하는 데 성공하였음. - 2023년, 국내·외에서 활발히 공격을 수행한 Rhysida 랜섬웨어를 분석하여 암호키 생성 과정에 사용되는 seed를 예측할 수 있는 취약점을 발견함. 이를 기반으로 암호화된 데이터의 복구에 성공함. - 자체 개발한 랜섬웨어 복호화 도구는 한국 인터넷 진흥원 및 과기정통부와의 협업을 통하여 배포하고 있으며, 이를 통해 세계적인 랜섬웨어 피해 완화에 기여함. - 연구팀에서 수행한 랜섬웨어 연구 결과를 국가정보원과 국가보안기술연구소에 소개하기 위

	해 강연을 진행함 - 랜섬웨어 대응 및 복호화 기술 (2023.03.09.), 국가정보원 - 랜섬웨어 공격, 대응 및 복호화 기술 (2023.07.12.), 국가정보원 - 랜섬웨어 대응 및 복호화 기술 (2023.08.04.), 국가보안기술연구소 - 특히, 산업체와 학계 간의 랜섬웨어 대응을 위한 정보 공유의 장을 만들기 위해 ‘랜섬웨어대응연구회’ 회장직을 연임하고 있으며, 2023년 제 1회 랜섬웨어대응연구회 워크숍을 개최하였음. - 사이버 위협 대응에 기여한 업적으로 제29회 정보통신망 정보보호 컨퍼런스(NetSec-KR 2023)’에서 과학기술정보통신부 장관 표창을 수상함.
2	**▶ 산업・사회 문제 해결을 위한 연구조직 및 학술대회 운영** - 유일선 교수는 5G 보안연구회 위원장으로 2018년부터 매년 5G보안 워크숍을 주관하여 2024년 02월 29일 기준 총 6회 개최하였음. 급변하는 사이버 보안 상황에 대응하기 위하여 각 분야의 전문가를 초청하여 제로트러스트, 암호화 트래픽 관제, 6G 보안 등과 같은 미래 기술을 논의하고, 5G 및 6G 환경에서 다변화되는 보안 요구사항에 대응하기 위해 사이버 보안기술이 나아가야 하는 방향성에 대한 논의를 진행함 - 유일선 교수는 2016년부터 매년 한국정보보호학회 주관 국제 학술대회 MobiSec를 2024년 02월 29일 기준 총 6회 개최하였음. 이동통신환경에서의 다양한 환경에 대응하기 위하여 각국의 전문가를 초청하여 5G 및 6G환경에서의 보안 요구사항을 대응하기 위한 사이버 보안 전문가 관점에서의 방향성에 대해 논의하였음. 또한, 이동통신환경에서의 다양한 정보보안 논문을 출판하여 5G 초연결사회의 문제에 대해 해결하고자 하였음
3	- 이옥연 교수와 그 연구팀은 이동통신 보안과 KCMVP, IoT 보안에 관한 연구를 지속적으로 진행하고 있음. - 2020년, 군용 드론의 안전성을 보장하기 위한 드론보안 가이드라인을 제정을 주도하여, 국방에 활용되는 드론의 보안체계 수립에 기여함. - 2020년, 한국정보보호학회 수석부회장을 맡아 국내 정보보호 학계를 대표하는 역할을 수행하였고, 한국암호포럼 의장을 맡아서 국내 암호학의 발전에 노력하였고, 국내 암호산업의 활성화와 관련 정책을 수립하는데 기여하였음. - 2021년, 군용 드론 보안과 이동통신 보안 연구를 꾸준히 진행하고 있으며, 이를 양자 엔트로피 기반 난수 발생기 등의 양자보안과 융합시키는 연구를 진행함. - 2021년, 한국암호포럼 의장을 맡아서 국내 암호학의 발전에 노력하였고, 국내 암호산업의 활성화와 관련 정책을 수립하는 데에 기여하였음 - 2022년, 한국정보보호학회 회장을 맡아 국내 정보보호 학계를 대표하는 역할을 수행 중이며, 국방암호기술특화연구센터 제3실장, 대검찰청디지털수사자문위원, 5G보안협의회 의원 등 다양한 국내 산업 및 사회를 위한 정보보안 전문가로써 우리 사회를 위협하는 정보보안 문제해결을 위한 정책자문과 기술발전에 기여함. - 연구팀에서 수행한 각 분야의 연구 동향에 대한 내용을 소개하기 위해 강연을 진행함 - 5G+ 6G를 향한 양자보안과 KCMVP 암호 발전 동향(2021.05.17.), 한양대 - 5G+ 기반 CPS를 위한 KCMVP 암호와 Quantum 암호의 도입 전략(2021.05.21.), CPS 보안 워크숍 - QRNG 기반 암호모듈 활용 방안(2021.07.21.), 국가보안기술연구소 - 드론에서의 경량 암호(2021.07.29.), 세종대 - IoT 보안 디바이스 개발 고려 사항 및 기술 소개(2021.08.16.), 한양대

4	**▶ 양자 시대 암호의 안전성 문제 해결을 위한 양자내성암호 설계 연구 진행** - 김동찬 교수와 그 연구팀은 2018년도부터 6년간 부호기반 암호와 구현 기법, 기반문제에 관한 연구를 진행하고 있음. - 특히 Goppa 부호와 이를 기반으로 하는 NIST PQC 4라운드 암호 Classic McEliece에 관한 연구를 지속적으로 수행하였음. - 2022년 “Patterson 디코딩 기반 Classic McEliece 키 복호 연산에 관한 연구”를 통해 통신학회 우수논문상을 수여함. - Classic McEliece의 단점을 개선할 다양한 설계 방식을 연구하였으며, 이를 바탕으로 202년 한국 양자내성암호연구단(이하, KpqC) PQC 공모전에 부호기반 키설정 PALOMA를 제안하였음. PALOMA는 KpqC PQC 공모전 2라운드 암호로 선정되었음. - KpqC PQC 공모전은 표준 제정을 목표로 하며, PALOMA는 이에 적합한 암호라고 평가함. - 2023년 7월, 국가정보원과 과학기술정보통신부는 행정안전부 등 관계부처와 함께 국내 암호체계를 KpqC PQC 공모전이 선정한 암호로 2035년까지 전환하는 마스터플랜을 발표하였음. - PQC의 기반문제는 양자 연산에 대해 내성을 가지는지 아직 증명되지 않았음. - 따라서 시급히 PQC를 준비해야하는 현 시점에서, 새로운 양자 알고리듬의 등장 가능성을 배제할 수 없기 때문에 특정 문제를 기반으로 한 암호만을 PQC 표준으로 제정할 수 없음. - KpqC는 이러한 상황을 고려해서 각 기반 문제별 최소 1종을 PQC 표준으로 선정할 가능성이 높음. - 부호기반 키설정 PALOMA는 안전성을 바탕으로, 양자 시대를 준비하는데 있어 한국의 국가 경쟁력을 제고하는데 큰 역할을 할 것으로 기대함. - KpqC는 네덜란드 Tanja Lange 교수 연구팀에 PALOMA의 안전성 분석을 의뢰했고, 연구팀은 현재까지 안전성의 치명적인 결함이 발견되지 않았다고 평가하였음. - 안전성 분석 연구를 추가하여 국제 부호기반 암호학회 CBCrypto 2023에 채택되었고, 추가 심사를 거쳐 2023년 10월 논문으로 게재되었음. 국제 부호 기반 학회에 인정받은 PALOMA는 그 안전성을 엄밀히 분석하였음. - 2023년 “부호 기반 키체결 PALOMA의 섞음 연산 SHUFFLE에 관한 연구”를 통해 PALOMA의 안전성과 직결되는 섞음 연산의 충돌쌍이 존재하지 않음을 증명하였음. 본 연구는 제6회 부채널정보분석 워크숍 차세대 정보보호 여성 과학기술인상을 수여함.
5	**▶ 산업・사회 문제 해결을 위한 양자난수발생기 분석 연구 진행** - 강주성 교수와 그 연구팀은 2014년도부터 10년간 한국과학기술연구원 등과 함께 양자암호와 양자난수발생기에 관한 연구를 지속적으로 진행하고 있음 - 난수발생기 평가에 관한 표준 제정에 참여하였으며, 국제 난수발생기 평가 표준의 문제점에 관한 논문을 게재하여 표준 개정에 기여함 - 2016년, 소프트웨어 환경에서의 잡음원 엔트로피 검증 알고리즘 표준을 개발함. 본 표준은 엔트로피 검증 후보 알고리즘의 통계적 테스트에 대한 알고리즘과 엔트로피 측정 알고리즘을 제시함 - 2016년, 소프트웨어 환경에서 주로 사용하는 잡음원 분석을 위해 윈도우 환경에서 동작하는 잡음원 수집용 도구를 구현하고 데이터를 수집하여 잡음원 검증용 도구를 개발함. 또한 엔트로피 평가가 필요한 암호모듈 개발자가 참고할 수 있는 검증용 소프트웨어에 대한 구현 가이드를 작성함 - 2017년, 하드웨어 잡음원 수집이 어려운 환경에서의 효율적인 난수발생 방법을 통한 암호 시스템 안전선 향상을 위해 운영환경(OS)별 잡음원 내부 종속성 특징을 분석하고 엔트로피

	평가방법을 통한 안전한 시드 구성 기법을 제시함 - 2019년, 1xN QKD 양자암호 네트워킹 시스템에서 사용되는 난수발생기의 엔트로피 평가를 위한 CAVP 도구를 개발함. 이는 QKD 시스템에서 의사난수발생기 시드(seed)의 안전성 및 필요한 시드 크기를 계산하는 데 사용 가능함 - 2020년, 예측통계량 기반 난수성 분석 기술과 미지의 분포에 대한 IID/Non-IID 판정법 분석을 통해 새로운 암호학적 난수성 분석 기법을 설계하고 시계열분석을 이용한 프리틱터 엔트로피 추정법 연구를 통해 엔트로피 추정법의 개선 정확도를 개선함으로써 보안 시스템 안전성 향상에 기여함 - 2020년, 표준화 기관별 QKD 평가 관련 표준문서와 제시하고 있는 모델에 대하여 파악한 후 분석을 진행함으로써 각 기관이 제시하는 시험평가 항목을 기반으로 QKD 시스템 적용 범위를 파악하고 안전성 분석 및 검증모델 연구를 수행함. 이러한 연구는 국가/공공기고나 뿐만 아니라 사업계에서 QKD 관련 시스템의 안전성 분석에 기반 연구로 기여함 - 2022년, 단일 병렬잡음원인 이미지센서 기반 진난수생성기의 잡음원 붙포 특성을 활용한 양자난수발생기의 헬스 테스트 기법을 개발함. 또한 병렬잡음원에 특화된 후처리 알고리즘을 개발하고 안전성을 증명함으로써 양자난수발생기의 고속화에 기여함 - 2023년, 이미지센서가 사용되는 IP 카메라 환경 내부에서 자체 생성한 난수를 고속 후처리하고 경량 의사난수발생기로 안전한 난수를 생성하는 연구를 수행함. 이는 최근 대두되고 있는 지능형 CCTV 보안 문제를 해결하는 데 활용될 것으로 기대됨 - 2023년, QKD의 후처리 절차에 대한 표준 개발에 참여함. QKD는 그 자체에 대한 표준은 존재하나 후처리에 대한 표준의 부재로 최종 생성되는 비밀키에 대한 안전성을 평가할 수 없는 상황이었으므로, 본 연구 활동이 차세대 양자암호 시스템의 안전한 키 공유에 기여할 것으로 기대됨
6	**▶ 산업·사회 문제 해결을 위한 양자내성암호 분석 및 활용 연구 진행** - 염용진 교수와 그 연구팀은 2018년도부터 6년간 국가보안기술연구소 등과 함께 양자내성암호에 관한 연구를 지속적으로 진행하고 있음 - 국내 양자내성암호 표준화 및 전환 정책 개발에 참여하고 있으며, 격자기반 양자내성암호 및 기타 양자내성암호 알고리즘의 구조를 수학적으로 분석하며 원천 기술에 대한 연구를 수행함 - 2018년, 산업계 세미나를 통해 양자내성암호 적용 현황을 분석하고, 양자내성암호를 제품 및 프로토콜에 적용할 때의 고려사항과 주요 양자내성암호 활용 국가에 대한 관련 정책을 파악하는 연구를 수행함 - 2019년, NIST 양자내성암호 표준화 공모사업의 2라운드 후보 알고리즘 중 격자 기반 알고리즘 FrodoKEM과 Round 5의 구조를 파악하고 에러 샘플링 방법을 분석함. 또한 2 종의 플랫폼에서 두 알고리즘의 최적화 요소를 분석하여 구현함으로써 개선 성능을 확인함 - 2020년, NIST 양자내성암호 표준화 공모사업의 3라운드 후보 알고리즘 중 격자 기반 알고리즘 NTRU와 CRYSTAL-Kyber, SABER의 구조를 파악하고 CPU 성능을 비교하여 주요 연산의 소요 시간을 측정함. 또한 NTRU의 GPU 구현을 통한 병렬화 가능성을 파악하여, 본 연구 결과가 향후 표준 알고리즘 고속화 구현 기법 개발에 기여할 것으로 기대됨 - 2021년, NIST 표준 문서 SP 800-131A와 SP800-57을 분석하여 알고리즘 전환 정책 및 승인 상태를 분석하고, 이전 암호 알고리즘 공모 사업의 진행 과정 및 알고리즘 평가 기준을 파악하여 국내에서 진행 중인 신규 양자내성암호 알고리즘 공모사업의 추진 방향을 제시하고 평가 기준 및 절차를 수립함

	- 2022년, 양자내성암호 NTRU가 적용된 하이브리드 데이터 암호화 기술 제품 QSafefE2E를 개발하여 산업계 제품 공급 계약을 체결하고 차세대 뱅킹 서비스 구축 프로젝트에 솔루션 도입을 확정함. 이 연구를 통해 차세대 원천 암호 기술을 확보함으로써 해외 기술 의존 없이 자체 기술로 국내 금융시장에 관련 제품을 공급할 수 있을 것으로 기대됨 - 2022년, 미국과 프랑스의 양자내성암호 전환 정책을 분석하고 암호 알고리즘 전환 시 고려사항을 파악함. 또한 하이브리드 용어를 정리하고 인증서, 프로토콜과 같은 응용 시스템으로의 적용 방안을 분석함. 본 연구를 국내 전환정책에 대한 가이드라인으로 활용함 - 양자내성암호 산학연 컨퍼런스를 개최하여 국내 암호전환정책 적용 및 확산에 관하여 학계, 연구기관, 산업계가 함께 논의할 수 있는 대화의 장을 마련함. 양자내성암호 활용 가능성, 국가 주도 로드맵 하에서 각 기관이 고려해야 할 사항 등을 논의함 - 양자내성암호 산학연 워크숍 (2022.08.10) - 제 2회 양자내성암호 산학연 컨퍼런스 (2023.08.29) - 2023년, 양자내성암호 Kyber를 양자암호 QKD 시스템과 연동하는 하이브리드 키 교환 프로그램을 개발하고 해당 공유 키를 사용하여 일대다 실시간 보안 통신을 시연함. 본 연구의 결과는 향후 양자내성암호와 양자암호, 양자난수발생기를 안전하게 연동하여 하나의 보안 인프라를 구축할 때 활용할 수 있을 것으로 기대됨
7	**▶ 국외 표준 양자내성암호 구현적합성 검증기법 연구** - 서석충 교수는 암호 알고리즘 최적 구현 및 구현적합성 검증기법의 국내 전문가로 활동하며, 다양한 환경에서의 암호 최적 구현 연구와 구현적합성 검증기법 개발에 기여함 - 2023년 “국외 표준 양자내성암호 구현적합성 검증기법 연구”라는 국가과제를 수행하여 양자내성암호의 KCMVP 마이그레이션을 위한 최적화 연구를 진행함 - 본 연구에서는 국내 암호 알고리즘 구현적합성 검증기법인 KCMVP에 NIST 표준화 대상 양자내성암호를 병합하고, 프리미티브별 구현적합성 검증 라이브러리를 최적 구현함 - KCMVP는 현재 암호 알고리즘 구현에 대해 일반적으로 수행되는 구현적합성 검증기법임 - 향후 양자 컴퓨팅 환경에서 현재의 소인수분해 및 이산로그문제 기반의 공개키 암호는 안전성을 유지하지 못하기 때문에, 양자 컴퓨팅 환경에서도 안전한 양자내성암호의 개발 및 표준화가 진행되었음 - 국내에서도 양자 컴퓨팅 시대가 도래하면 양자내성암호를 사용해야 하지만, 이를 위해서는 KCMVP에 양자내성암호의 마이그레이션이 필요함 - 현재 KCMVP 제도에서는 블록 암호, 공개키 암호, 그리고 해시 함수만을 포함하며, 양자내성암호는 아직 적용되지 않음 - 본 연구는 NIST 표준화 대상 양자내성암호 알고리즘의 프리미티브별 구현적합성 검증방법론을 연구하고, 단순 KAT를 확장하는 새로운 검증 기법 연구를 수행하여 보안 강도 및 랜덤 함수와 같은 알고리즘 옵션을 고려한 테스트 케이스를 도출하였음 - 또한, 프리미티브별 구현적합성 검증 라이브러리를 최적 구현하였으며, 국내 검증대상 알고리즘과 연동 시 효율성 비교와 알고리즘 중간 구현 참조값을 도출하였음 - 국내 검증대상 알고리즘과의 연동은 양자내성암호에서 사용하는 해시 함수를 국내 검증대상 알고리즘으로 대치하는 것임 - 예를 들어, CRYSTALS-Kyber에서 해시함수 기반 PRF에 SHA-256 또는 LSH를 사용하는 것을 고려하고, AES 대신 ARIA, LEA 등의 알고리즘을 사용하는 것임 - 따라서 본 연구를 통해 NIST 표준화 대상 양자내성암호의 CAVP 시험 방법론을 개발하여 향후 양자내성암호의 KCMVP 탑재에 활용될 수 있음 - 또한, 최적 구현한 라이브러리를 통해 최신 최적화 기법이 적용된 검증 라이브러리를 사용

	할 수 있음 - 근미래에 도래할 것으로 예상되는 양자 컴퓨팅 환경을 미리 대비하여 KCMVP에 양자내성암호를 탑재 가능하게 함 - 양자내성암호의 구현적 안전성을 검증할 수 있는 기반을 설계하여 향후 양자내성암호의 상용화가 이루어졌을 때 받아야 할 KCMVP 검증의 초석이 됨
8	**▶ 산업·사회 문제 해결을 위한 부채널 분석 취약성 검증 및 대응 기술 연구 진행** - 한동국 교수는 부채널 분석의 국내 전문가로 활동하여, 한동국 교수와 그 연구팀은 물리적 보안을 요구하는 다양한 보안 기기에 대한 안전성 검증 역량 발전에 기여함 - 2016년 Mifare 카드 복제 가능 취약점을 제기하여 실제 사용되는 IC 카드의 부채널 검증을 수행함 - 공공기관 및 호텔 등에서 출입 통제를 위해 Mifare 카드가 수 분 내에 복제 가능하다는 취약점을 제기함 - 보안이 취약한 카드를 기반으로한 출입 통제 시스템에 대한 취약점을 보이고 이를 실질적으로 적용가능함을 선보였으며 이를 통해 대응 기법 설계 등 취약점 제거 방안 검토의 필요성을 강조함 - KCMVP 암호에 해당되는 블록 암호 알고리즘 SEED에 대한 효율적 부채널 분석 기법을 제시함 - 2018년 국내 금융 IC 카드에 사용되는 블록 암호 알고리즘 SEED에 대한 보다 효율적인 부채널 분석 방법을 제시함 - 기존의 금융 IC 카드의 취약점 검증(안전성 테스트)에서 고려하고 있지 않는 신규 분석 방법으로 금융 IC 카드에서 발생가능한 개인정보 탈취 문제를 방지하는데 기여함 - 2016년부터 최근까지 주요 양자내성암호 부채널 공격 취약성을 분석함 - Ring-LWE 기반 암호 알고리즘, 다변수 기반 서명 알고리즘, 부호 기반 암호 알고리즘 등 양자내성암호에 대한 신규 부채널 분석 방법들을 제안함으로써 양자 컴퓨터의 개발로 대두된 공개키 암호 알고리즘의 취약성 문제 해결에 기여함 - 2019년 12월부터 2021년 11월까지 총 3년간 산업통상자원부 주관 국제공동기술개발사업의 ‘딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발’ 연구를 수행함 - 이를 통해 머신러닝 기술과 부채널 분석 기술을 접목하여 자동화된 이상행위 탐지 도구를 개발하여 국사 산업을 보호할 것으로 기대함 - 부채널 분석을 이용한 백도어 탐지 기술을 개발하여 국가 산업을 보호하기 위한 연구를 수행함. - 다 기종의 마이크로프로세서(예, AVR, MSP, ARM 등)를 대상으로 부채널 정보 특성이 어떻게 차등화되는지 연구하여 다양한 환경에 유연하게 적용 가능한 이상행위 탐지 도구를 개발함 - 전 세계적으로 주요 보안 문제 사항으로 대두되는 백도어를 탐지하여 국가 산업 보호에 기여함 - 세계적인 하드웨어 보안 연구 대회에서 다수의 수상을 하는 등 물리적인 취약성 검증에 대한 기술력을 확보하고 이를 바탕으로 국내 취약점 검증 연구를 수행함 - Conference on CryptoGraphic Hardware and Embedded System 2016 (CHES 2016) - 2022년 HACK@SEC 2022에서 2등을 수상 - 국내의 부채널 분석 전문 인력을 양성하여 인재를 확보하고, 산업체, 학교, 연구소 간의 교류의 장을 만들고 연구 내용을 공유하는 등의 기회를 제공하기 위해 부채널 연구회 회장직

	을 연임하고 있음. - 특히 부채널 연구회에서 2018년도부터 현재까지 지속적으로 ‘부채널정보분석워크숍’을 개최하여 전문 인력 양성 및 연구 개발 내용 공유의 기회를 제공하여 국내의 물리적 보안에 대한 기술력 증진에 기여함.
9	**▶ 산업·사회 문제 해결을 위한 특수 통신 융합 서비스 관련 연구 진행** - 박수현 교수님 연구팀은 2015년부터 수중, 해양, 극지와 같은 특수한 환경에서의 통신 네트워크에 대한 연구를 수행하고 있음. - 2015년, “수중네트워크 상호호환 연계기술개발“에 관한 연구는 수중 초음파 센서 네트워크 기술 연구개발 성과를 국내 및 국제 산업 그리고 단체 표준화 문서의 개발 및 제정을 추진함 - 2017년, “지상 IoT 연계형 경량 UIoT 스마트 서비스 프레임워크” 기술 개발에 관한 연구는 수중음파통신 원천기술을 기반으로 지상 IoT 연계형 경량 UIoT 스마트 서비스 프레임워크 관련 원천기술(TRL 4 목표) 확보함 - 2017년, “분산형 수중 관측 제어망 개발“에 관한 연구는 호서대학교와 해양수산부가 추진하는 초음파 수중통신을 활용한 광범위한 수중 무인 모니터링 및 제어기술 개발에 관한 네트워크 관리 기술의 개발 및 확보 기술의 국내 및 국제 표준화에 관한 것으로서 6년간 위탁연구 참여하였으며 다수의 저널과 표준화 문서 개발을 수행함 - 2017년, “Seamless DTN을 이용한 진보된 다이버 네트워크 개발“에 관한 연구는 수중에서 정보처리 요구사항이 높은 인간과 로봇을 대상으로 지상에 위치한 서비스 코어로 부터 수중 네트워크 까지의 서비스 Seamless를 달성하기 위한 독창적인 네트워크 레퍼런스 모델의 개발과 개념 구현함 - 2019년, “수중 광역 이동통신 시스템 기술개발“에 관한 연구는 선박해양플랜트연구서와 해양수산부가 추진하는 세계 최초의 수중이동통신망 기술 개발 및 개념 구현함 - 2021년, “수중 SNS 포스팅을 지원하는 다이버 데이터 심리스 커뮤니케이션 개발“에 관한 연구를 해양수산과학기술진흥원으로 부터 주관연구기관 자격으로 수임하였음. 본 기술은 ’Seamless DTN을 이용한 진보된 다이버 네트워크 개발“의 연구성과를 산업화하기 위한 스케일업 기술 및 비즈니스 모델링에 관한 연구로서 TRL6 성과를 수행함 - 2021년, “극한지 관측 및 정보처리 기술 개발“에 관한 연구는 극지연구소와 해양수산부가 추진하는 남극 장보고과학기지 반경 100Km이내에 Smart 무인관측제어 기술을 개발 및 실증할 예정임 - 2022년, “AI기반 어선안전 설계 데이터플랫폼 개발 및 실증-운항안전 표준모듈“에 관한 연구는 1차산업인 수산업의 경쟁력 강화와 산업 안전지표의 고도화를 목표로 차세대 연안어선 및 어선 안전기술 개발에 관한 것으로서 통계 지표와 현장 사망만인율의 불일치 정도를 분석할 예정임 - 2020년, 세계 해양도시의 공동 성장을 목표로 산업 및 기술의 발전 방향을 공개 토의하는 성격의 “제 1 회 인천국제해양포럼”의 IoT-스마트 해양 세션의 ‘수중통신 세계표준화’ 주제 토론 진행을 주도함. - 연구팀은 2012년부터 국제/국내 수중 통신 표준화 관련 활동함. - ISO/IEC JTC1 SC41 IoT/Underwater Communication Project Leader/Editor/Co-editor - 한국정보통신기술협회(TTA) ICT 표준화 전략맵 수립을 위한 유무선통신 기술표준기획전담반 위원 - 한국정보통신기술협회(TTA) PG903 부의장/WG9031 의장 - 국립전파연구원정보통신표준 전문위원회(SC41K) 위원(IoT 및 디지털 트윈 관련 기술)

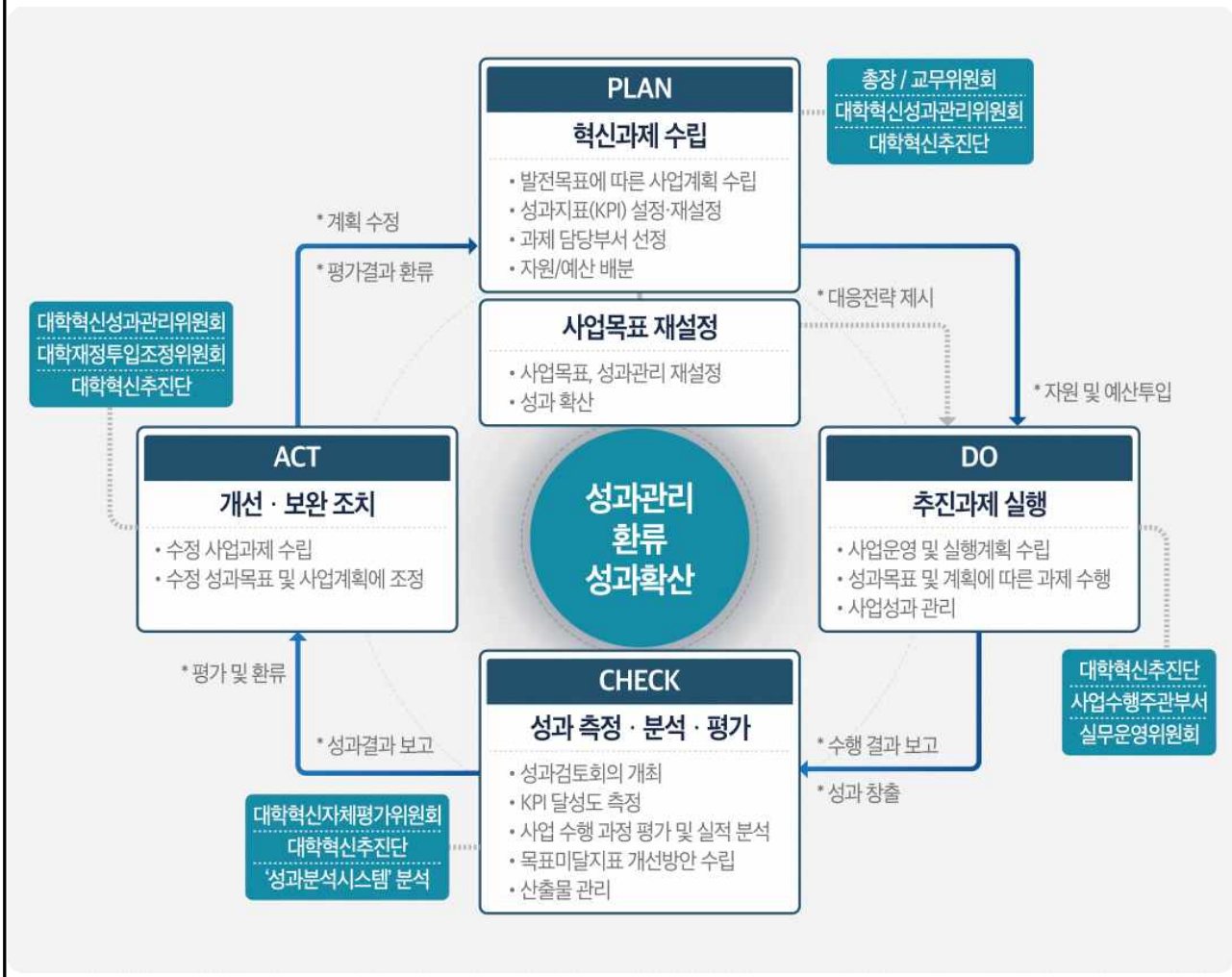
	- 2021년, 국제 공적 표준 SDO(Standard Development Organization) ISO(International Organization for Standardization), 수중통신, 해양통신, 디지털트윈 분야 ISO/IEC JTC 1/SC 41 WG7이 신설되었으며, 해당 WG의 Convener로 선정되어 활동하였음 - 국제 표준화 업무에 기여한 업적으로 2021년 과학기술정보통신부 장관 표창을 수상함.
10	**▶ 인공지능 분야에서 클라우드 기반의 고차원 데이터를 활용한 딥러닝 기술** - 윤상민 교수님 연구팀, 딥러닝 기술이 많은 각광을 받고 있으나, 클라우드와의 통신 과정에서 데이터의 훼손, 개인정보의 보안, 처리의 효율성적인 측면에서 많은 문제를 야기할 수 있어 온디바이스 환경에서의 인공지능 기술이 요구되고 있음. 모델의 경량화뿐만 아니라 데이터의 경량화를 개발함으로써 온디바이스 환경에서의 인공지능 활용 가능성을 높이고 개인정보 보안 및 안정성을 높일 수 있음

1.3 교육연구단의 연구역량 향상 실적

▣ 산업사회문제 해결에 초점을 맞춘 연구 성과관리 체계 조성

▶미래 지향적 지원체계 운영

- 대학의 혁신 비전 및 중장기 발전계획 <KMU Vision 2030+α>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 의사소통 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

▶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 전공분야 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 성과 보수를 제공하며, 박사과정 대학원생은 (석박사통합과정 대학원생 포함) 학술대회 10편 또는 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

▶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 연구책임자

의 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 우수 특허 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 노력 지속 예정

▶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, 평가항목별 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 창업멘토링 제공과 세계

시장 진출 지향형 보육 환경을 지원함

- 성과나 실적이 우수한 참여 교수와 대학 동문들이 (가칭) 국민엔젤펀드를 결성하여 자금지원을 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・사회 문제 해결 기여 실적

<표 3-6> 사업 참여 기간 내 참여교수 산업・사회 문제 해결 기여 실적

연번	실적명	참여교수명	실적 해당 분야	실적 요약
1	랜섬웨어 대응 워크숍 개최	김종성	미래/글로벌 대응 학문의 개방화/대중화	사업 참여 기간을 포함하여 한국인터넷진흥원과 다년간의 연구를 진행하여 랜섬웨어 분석에 관한 연구를 지속적으로 진행하고 있음. 자체 평가기간 동안 국내・외에 다수의 피해를 입힌 Hive와 Rhysida 랜섬웨어에 대한 복호화 방법을 개발하여 세계적인 관심을 받고 있음. 이를 논문으로 발표하고 한국인터넷 진흥원 및 과기정통부와 협업하여 복호화 도구 제작 및 배포 작업을 통해 랜섬웨어 피해를 완화하는데 도움이 될 것으로 기대됨.
2	블록암호 기반 해시함수에 대한 양자 안전성 분석 방법 제시	김종성	미래/글로벌 대응	현재 IBM을 선두로 한 양자컴퓨터의 개발은 전 세계적인 관심을 받고 있음. 해시함수는 데이터 익명성 보장과 무결성 검증 등 다양한 곳에 사용되며, 양자컴퓨터를 사용한 공격은 보안에 치명적이 될 수 있음. 김종성 교수는 국제표준암호인 AES를 활용한 해시모드들과 국내표준암호인 ARIA를 활용한 해시모드에 대한 분석을 진행했으며, 이에 대한 연구는 미래 암호분석 공격에 대비하는 연구의 초석이 됨.
3	부호 기반 키설정 PALOMA 개발	김동찬	미래/글로벌 대응 정책 기여 거버넌스 구축	한국 양자내성암호연구단은 양자내성암호 표준 제정을 위한 PQC 공모전을 진행 중이며, 부호기반 키설정 PALOMA는 2라운드 암호로 선정됨.

4	5G보안연구회 운영	유일선	거버넌스 구축	한국정보보호학회 주관의 5G보안연구회 운영을 통해 매년 워크샵을 추진하여 국내 5G보안 취약점 문제에 대한 심도 깊은 토의와 해결책을 제시하여 미래 이동통신 네트워크 발전에 기여하였음.
			학문의 개방화/대중화	
			미래/글로벌 대응	
5	학술대회 운영 (MoblSec)	유일선	거버넌스 구축	한국정보보호학회 주관의 국제학술대회 MobiSec 운영을 통해 매년 학술대회를 추진하여 국내외 전반적인 이동통신 보안 문제에 대한 학술의 발전에 기여하였음.
			학문의 개방화/대중화	
			미래/글로벌 대응	
6	공공시설용 이동 영상감시의 무선 데이터 기밀성 보장 WiFi 장비 개발 및 상용화	이옥연	기업현안 해결	군 주요시설 온도, 습도 및 영상 데이터 기밀성 보장 WiFi 장비, 교통신호제어기용 LTE 기반 SSL VPN 보안 표준과 호환성 장비 개발 및 상용화 등 각 기관에 필요한 기술을 제시하고 기관에서 가진 문제 해결에 기여함.
			정책 기여	
7	정책 자문	이옥연	정책 기여	국방암호기술특화연구센터 제3실장, 대검찰청디지털수사자문위원, 5G 보안협의회 의원 등 다양한 국내 산업 및 사회를 위한 정보보안 전문가로 활동하면서 우리 사회를 위협하는 정보보안 문제해결을 위한 정책자문과 기술발전에 기여하고 있음.
			인력 재교육	
8	온디바이스 인공지능 기술의 고도화 및 데이터 경량화 방법 제시	윤상민	미래/글로벌 대응	온디바이스 인공지능 기술의 고도화와 데이터 경량화 방법을 제시하여 인공지능의 실제 사용성을 향상시킴.
			일자리 창출	
			기업현안 해결	

9	양자암호 및 난수발생기 표준 제정 참여	강주성	미래/글로벌 대응 정책 기여	QKD 시스템 적용 범위를 파악하고 안전성 분석 및 검증모델 연구를 기반으로, QKD의 후처리 절차에 대한 표준 개발에 참여하여 차세대 양자암호 시스템의 안전한 키 공유에 기여함. 또한 소프트웨어 모듈 난수발생기 안전성 평가를 위한 엔트로피 검증 후보 알고리즘의 통계적 테스트에 대한 알고리즘과 엔트로피 측정 알고리즘을 제시함.
10	양자내성암호 정책 개발을 위한 산학연 워크숍 개최	염용진	미래/글로벌 대응 정책 기여	양자내성암호 산학연 컨퍼런스를 개최하여 국내 암호전환정책 적용 및 확산에 관하여 학계, 연구기관, 산업계가 함께 논의할 수 있는 대화의 장을 마련함. 양자내성암호 활용 가능성, 국가 주도 로드맵 하에서 각 기관이 고려해야 할 사항 등을 논의하여 해당 내용을 분석함으로써 향후 정책 마련의 기반 조성에 기여함.
11	자율주행 V2X 서명 검증 속도 고속화 기술 개발	서석충	미래/글로벌 대응 기업현안 해결	V2X는 차량과 사물 간의 통신 프로토콜임. V2X에서 차량은 고속으로 이동하며 임베다드 장치에서 연산을 수행하기 때문에 프로토콜 고속화가 필요함. 이는 차세대 자율주행 차량에서 효율적으로 V2X를 사용할 수 있게 하며, 현재 자율주행 기술을 연구하는 기업들이 실제 프로토콜 적용에 사용할 수 있음.

12	부채널 분석 워크숍 개최	한동국	미래/글로벌 학문의 개방화/대중화	매년 부채널 분석 연구회 회장으로서 암호뿐만 아니라 디바이스 보안 분야의 다양한 부채널 정보를 이용한 공격 및 대응기술의 중요성을 알리며 학생, 연구소, 그리고 기업 간의 지식 공유의 장을 생성하는 데 기여하고 있음.
13	Special Communication & Convergence Services 2024 워크샵 개최	박수현	미래/글로벌 대응	NTN를 중심으로 한 특별 통신 및 시스템 분야의 최신 연구 성과를 논의함. 인공지능 기반 NTN, NTN과 TN 간의 연결, 해양 및 수중 통신 시스템, 극한지 정보 기술 등 다양한 주제가 다뤄짐. 워크샵은 특수 환경에서의 통신 및 시스템 개발이 연구와 기술 발전에 있어 정보보안 문제 해결에 기여함
총 환산 참여교수 수		10.57	**제출 요구량**	3~5

연번	교육연구단 참여교수 산업·사회 문제 해결 기여 실적 설명
1	김종성 교수는 2023년부터 한국정보보호학회 산하의 랜섬웨어 보안 연구회의 위원장으로 연구회를 운영하면서 산업, 사회 및 국가 인프라 위협하는 랜섬웨어 감염에 의한 문제를 해결하기 위해 한국인터넷진흥원, 안랩 및 SK쉴더스 등 국내 기관 및 기업과 협업하고 있음. 특히, 한국인터넷진흥원과 다년간의 공동 연구를 수행하였으며, 다수의 랜섬웨어 복구도구를 개발하여 국내·외 감염 피해 복구에 기여하였음. 자체 평가 기간 동안 개발된 Hive와 Rhysida 랜섬웨어 복구도구는 세계적으로 천문학적인 피해를 입힌 랜섬웨어의 복구도구로 한국 인터넷 진흥원 및 과기정통부와 협업하여 복호화 도구 제작 및 배포 작업을 수행하였음. 해당 복구 도구는 공격자 검거를 통한 개인키 획득을 기반으로 하는 기존 대부분의 랜섬웨어 복구도구와 달리 사용된 암호화 매커니즘의 취약점 분석을 기반으로 개발되었다는 특징이 있음. 이는 단순한 보안 취약성 분석이 아닌 암호 매커니즘의 심층 분석에 의한 성과로 랜섬웨어 감염 데이터에 대한 문제를 해결하기 위해 새로운 방법을 제시함으로써 랜섬웨어 감염으로 인한 기업, 기관 및 인프라 피해 문제를 해결하는데 기여함.
2	현재 IBM을 선두로 한 양자컴퓨터의 개발은 전 세계적인 관심을 받고 있음. 미국 저명 컨설팅 회사인 맥킨지&컴퍼니는 2022년 68억 달러 수준 규모이던 세계 양자기술 시장이 2040년에는 최대 1060억 달러로 급성장할 것으로 예상하였음. 해시함수는 데이터 익명성 보장과 무결성 검증 등 정보보호 차원에서 다양한 곳에 사용되는 함수임. 양자컴퓨터를 사용한 해시함수에 대한 공격은 네트워크 및 컴퓨터 보안에 치명적이 될 수 있음. 김종성 교수는 AES와 ARIA를 활용한 해시모드들에 대해 양자컴퓨터 환경에서의 암호분석을 진행했음. AES는 현재까지 가장 많이 사용되는 국제표준 블록암호이며, 이에 대한 분석은 “Quantum cryptanalysis of the full AES-256-based Davies-Meyer, Hirose and MJH hash functions“ 논문에 수록되어 있음. ARIA는 국내표준 블록암호이며, 이에 대한 분석은 “Quantum rebound attacks on reduced-round ARIA-based hash functions“ 논문에 수록되어 있음. 이에 대한 연구는 미래 암호분석 공격에 대비하는 연구의 초석이 됨.
3	2023년 7월, 국가정보원과 과학기술정보통신부는 행정안전부 등 관계부처와 함께 국내 암호체계를 KpqC PQC 공모전이 선정한 암호로 2035년까지 전환하는 마스터플랜을 발표함. 과정 중 하나로 한국 양자내성암호연구단은 2022년부터 PQC 공모전을 진행 중임. 본 연구에서 개발한 부호기반 키설정 PALOMA는 KpqC 공모전 2라운드 암호로 선정됨. 따라서 공개키 크기가 상대적으로 크다는 단점이 있지만, 안전성 분석 성숙도가 높고, 연산 속도가 빠르며, 복호 실패 확률이 0이라는 장점을 가지고 있는 부호기반 암호가 최소 1종 PQC 표준으로 제정될거라고 기대함.KpqC는 네덜란드 Tanja Lange 교수 연구팀에 PALOMA의 안전성 분석을 의뢰했고, 연구팀은 현재까지 안전성의 치명적인 결함이 발견되지 않았다고 평가하였음. 또한 이후 연구한 안전성 분석 내용을 추가해 국제 부호기반 암호학회 CBCrypto 2023에 채택되었고, 추가 심사를 거쳐 2023년 10월 논문으로 게재되었음. 국제 부호 기반 학회에 인정받은 PALOMA의 안전성을 엄밀히 분석하고, 산업계의 활용도를 높일 수 있는 라이브러리 개발을 통해, 양자 시대를 준비하는데 있어 한국의 국가 경쟁력을 제고하는데 큰 역할을 할 것으로 기대함.

4	유일선 교수는 한국정보보호학회 주관의 5G보안연구회 운영을 통해 매년 워크샵을 추진하여 국내 5G보안 취약점에 따른 사회적 문제 대한 심도 깊은 토의와 해결책을 제시하고 논의하며 미래 이동통신 네트워크 산업 발전에 기여하였음. 매년 워크샵 진행을 통해 앞으로 대한민국의 이동통신 산업이 나아가야할 방향을 제시하고 있음.
5	유일선 교수는 한국정보보홍가회 주관의 국제학술 대회 MobiSec 운영을 통해 국내외 전반적인 이동통신 보안의 최신 기술과 보안 요구사항 및 문제 해결에 대한 논의로 보안 문제에 따른 사회적 문제의 해결책 제시와 논의하며 미래 이동통신 네트워크 학문의 발전에 기여하고 있음. 또한, 각 국의 대학원생들이 논문을 게재하고 출판할 수 있도록 하며 학문의 개방화 및 대중화에 기여하였음.
6	군 훈련장용 영상/센서정보 실시간 무선 WiFi 보안장비 개발 및 상용화, 군 주요시설 온도, 습도 및 영상 데이터 기밀성 보장 WiFi 장비, 교통신호제어기용 LTE 기반 SSL VPN 보안 표준과 호환성 장비 개발 및 상용화 등 다양한 기관에서 보안을 적용해야하는 통신 구간의 문제를 해결하기 위한 다양한 형태의 장비를 개발하고 기술을 제시함으로써 각 기관에서 가진 문제 해결에 기여함.
7	국방암호기술특화연구센터 제3실장, 대검찰청디지털수사자문위원, 5G 보안협의회 의원 등 다양한 국내 산업 및 사회를 위한 정보보안 전문가로 활동하면서 각 분야에서 발생하는 우리 사회를 위협하는 정보보안 문제해결을 위한 정책자문과 기술발전에 기여하고 있음. 특히, 이옥연 교수는 2020년 11월까지 군용 드론의 안전성을 보장하기 위한 드론보안 가이드라인을 제정을 주도하여, 국방에 활용되는 드론의 보안체계 수립에 기여하였으며, 2020년에는 한국정보보호학회 수석부회장을 맡아 국내 정보보호 학계를 대표하는 역할을 수행하였고, 한국암호포럼 의장을 맡아서 국내 암호학의 발전에 노력하였고, 국내 암호산업의 활성화와 관련 정책을 수립하는데 기여하였음. 또한, 5G보안포럼, 5G보안협의회, 대한전기협회 전력보안통신설비분과위원장 등의 다양한 국내 산업 및 사회를 위한 정보보안 전문가로써 우리 사회를 위협하는 정보보안 문제해결을 위한 정책자문과 기술발전에 기여하고 있음.
8	딥러닝 모델의 발전에 따라 지역적-전역적 특징을 검출하고 강화하기 위한 end-to-end 모델을 개발함으로써 제한된 하드웨어 환경에서의 효과적인 인공지능 모델을 적용하여 성능향상과 보안성을 확보하고자 함. 또한, 데이터 경량화를 통하여 차원의 저주를 해결하기 위한 방안을 제시함으로써 향후 다양한 기기에서의 보안성과 안정성이 요구되는 인공지능 및 데이터 경량화에 기여할 수 있도록 함.

9	양자 키 분배(Quantum Key Distribution, QKD)는 두 사용자가 양자(quantum)를 이용하여 안전하게 키를 공유하는 절차임. 기존 재정 표준은 QKD의 절차를 원시키 생성, 걸러진 키 생성, 비밀 키 생성 단계로 나누고 있으나, 걸러진 키로 비밀 키를 생성하는 절차에 관하여 구체적인 절차 및 요구사항이 명시되지 않음. 강주성 교수는 2023년 QKD 후처리에 관한 표준화에 참여하여 안전한 QKD 비밀 키 공유에 기여하고 있음. 특히 후처리 절차 중 오류정정 프로토콜에 관한 이론적 안전성 근거를 제시함으로써 QKD 후처리에 대한 보안 요구사항을 구체화하고 설계한 각 보안 요구사항에 대응되는 벤더 요구사항과 시험자 시험방법을 제시하여 QKD 후처리 안전성 검증의 체계성에 기여함.
10	최근 국내 양자내성암호 도입을 위한 공모전 및 전환 정책에 관한 연구가 수행되고 있음. 양자내성암호로의 전환은 현 산업계의 현황을 반영하면서 안전한 차세대 보안 인프라를 구축해야 하므로 학계, 연구계의 입장을 두루 살펴야함. 염용진 교수는 2022년과 2023년 양자내성암호 산학연 컨퍼런스를 개최하여 국내 암호전환정책 적용 및 확산에 관하여 학계, 연구기관, 산업계가 함께 논의할 수 있는 대화의 장을 마련함. 또한 해당 활동을 통해 양자내성암호 활용 가능성, 국가 주도 로드맵 하에서 각 기관이 고려해야 할 사항 등을 논의한 뒤 해당 내용을 분석함으로써 향후 정책 마련의 기반 조성에 기여함. 현재 국내 양자내성암호 공모전의 최종 라운드가 진행되고 있으므로, 본 활동에서의 분석을 기반으로 제시한 정책 마련 시 고려사항들이 향후 보안 인프라 구축에 기여할 것으로 기대됨.
11	V2X(Vehicle to Everything)는 차량과 모든 사물 간의 통신 프로토콜이며, 차세대 자율주행 차량에 적용되어야 할 프로토콜임. V2X가 적용되는 자율주행 차량은 해당 프로토콜을 가용 자원이 매우 제한적인 임베디드 장치에서 수행함. 또한, 차량이 고속으로 이동할 경우 V2X 프로토콜을 고속으로 수행하여야 정상적인 동작을 기대할 수 있음. 따라서 임베디드 환경을 고려하여 V2X 프로토콜의 가속화는 필수적이며, 본 연구에서는 V2X의 서명 검증 속도를 고속화함. 자율주행 자동차는 현재 많은 기업에서 연구하고 있으며, 근미래에 완전한 자율주행 자동차가 상용화될 것으로 예상됨. 자율주행 자동차는 도로와 그 주변의 물체들과 통신하며 주변 상황을 확인하기 때문에 V2X는 반드시 필요하며, 실제로 상용화 되었을 때 자율주행 자동차에 탑재될 것으로 예상됨. 서명 검증 속도가 느리다면 자동차는 각 Entity마다 검증을 느린 속도로 진행해야 하고, 중요한 Entity에 대해 검증의 우선순위가 밀리게 될 수 있음. 본 연구의 결과를 통해 서명 검증 속도를 가속화하고, 실제 자율주행 차량에서 효율적으로 V2X를 사용할 수 있도록 함. 이는 현재 자율주행 기술을 연구하는 기업에서 필요한 기술이며, 해당 기술을 개발함으로써 V2X 고속화의 시발점이 됨.
12	매년 부채널 분석 연구회 회장을 맡아 매년 부채널정보분석 워크숍을 주관하여 현재 6회째 개최하였음. 암호뿐만 아니라 디바이스 보안 분야의 다양한 부채널 정보를 이용한 공격 및 대응기술의 중요성을 알리고 있음. 특히 최근에는 코드 안티탬퍼링 기술, 양자 내성 암호 안전성 및 최적화 등의 다양한 분야에서 부채널 보안 기술의 중요성을 알리고 있음. 또한 부채널정보분석 경진대회를 개최하여 학생들의 부채널 분석 연구를 장려하고, 연구소, 기업, 학계 사이에 부채널 보안에 대한 지식 공유의 장을 생성하는 데 기여하고 있음.

13	박수현 교수는 수중, 해상 정보통신 분야에서 국내외의 단체 및 공적 표준화 활동을 수행하고 있으며 TTA WG9031 의장과 TTA PG903 부의장을 수임하고 있음. 최근 성과로서 2023년 6월에 개최된 ISO/JTC1/SC41 제 13차 회의에서 “eco-friendly multi medium underwater wireless communication“에 대한 발표를 통해 미국, 중국, 인도, 호주, 노르웨이 등의 National body로부터 차세대 수중 통신 기술에 대한 큰 관심과 긍정적인 반응을 얻음. 해당 기술은 해양 생태계 친환경적인 산업 수중 통신 방법에 관한 것으로 세계적인 ESG(Environment, Social, Governance) 경제 활동 확산에 따른 수중, 해상 기술 디지털전환 발전 방향에 부합하는 기술로서 표준화 성공시 국내 수중, 해상 산업 고도화에 크게 기여할 것으로 기대됨.

3. 연구의 국제화 현황

3.1 참여교수의 국제적 학술활동 참여 실적 및 현황

▶ 김종성 교수
- ACM CCS 2021 국제 학술대회의 Registration Chairs로 활동함
- The 24th Annual International Conference on information Security and Cryptology (ICISC, 2021) 국제 학술대회의 Program Committee로 활동함
- The 25th Annual International Conference on information Security and Cryptology (ICISC, 2022) 국제 학술대회의 Program Committee로 활동함
- The 26th Annual International Conference on information Security and Cryptology (ICISC, 2023) 국제 학술대회의 Organizing Committee로 활동함
- The 23th World Conference on Information Security and Applications (WISA, 2022) 국제 학술대회의 Organizing Committee로 활동함
- The 24th World Conference on Information Security and Applications (WISA, 2023) 국제 학술대회의 Program Committee로 활동함
- 2021 International Conference on Platform Technology and Service (PlatCon-23) 국제 학술대회의 Publication Chairs, Steering Committee 및 Organizing Committee로 활동함
- 2022 International Conference on Platform Technology and Service (PlatCon-23) 국제 학술대회의 Industry Liaison Chairs 및 Steering Committee로 활동함
- 2023 International Conference on Platform Technology and Service (PlatCon-23) 국제 학술대회의 Steering Committee 및 Banquet Chair로 활동함
- DFRWS APAC 2023 (3rd Annual Digital Forensics Research Conference) 국제 학술대회의 Technical Program Committee로 활동함

▶ 유일선 교수
- 세계 Elsevier-Stanford University의 세계 상위 2% 과학자에 선정됨
- 국제 컨퍼런스 Mobile Internet Security의 General Chair로 활동함
- 제9회 ACM 아시아 공개키 암호 워크숍 (APKC 2022)에서 인슐린 펌프를 위한 경량의 비정상 행위탐지를 주제로 초청강연을 함
- SCIE 저널 Intelligent Automation & Soft Computing(IF: 3.401, JCR Q2)의 Associate Editor-in Chief로 활동함
- SCIE 저널 Information Sciences(IF: 8.233, JCR Q1)의 Associate Editor로 활동함
- SCIE 저널 IEEE Access(IF: 3.476, JCR Q2)의 Associate Editor로 활동함
- Scopus 저널 Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (Scopus Q2)의 Editor-in Chief로 활동함
- 국제 저술 활동: Mobile Internet Security (Springer CCIS, Volume 1544) ISBN: 978-981-16-9576-6
- IFIP Working Group 8.4 member로 활동함
- 유럽의 정상급 보안 연구그룹인 오스트리아 Secure Business Austria (SBA)의 Academic Member로 활동함
- Information Science Associate Editor로 활동함
- 국제 저널인 IEEE Access의 Associate Editor로 활동함
- Springer의 국제 저널인 Soft Comouting의 Associate Editor로 활동함

- 국제 저널인 Information Sciences의 Associate Editor로 활동함

▶ 이옥연 교수
- SCIE 저널 Hindawi WCMC(IF: 2.146)의 Associate Editor로 활동함
- SCIE 저널 MDPI Applied Sciences(IF: 2.838)의 Associate Editor로 활동함
- SCIE 저널 IEEE ACCESS(IF: 3.367)의 Associate Editor로 활동함

▶ 서석충 교수
- 2022년부터 2024년까지 한국정보보호학회 27~29대 이사를 역임하여, 국내 정보보호 발전에 기여함
- 2022년부터 국가정보원 암호모듈 검증 위원으로 활동하며, 국내 KCMVP 검증을 담당함
- 2022년부터 2023년까지 CISC-S/W 프로그램 위원장, WISA 프로그램 운영위원, Mobisec 프로그램 운영위원으로 활동하며, 정보보호 관련 국내/국제 학회 발전에 기여함
- 2020년부터 2023년까지 ICISC 프로그램 운영위원으로 활동하며 국제 정보보호 학회 발전에 기여함

▶ 한동국 교수
- The 23rd Annual International Conference on information Security and Cryptology (ICISC, 2020) 국제 학술대회의 Program committee로 활동함
- Cryptographic Hardware and Embedded Systems (CHES, 2021) 국제 학술대회의 Program committee로 활동함
- The 24th Annual International Conference on information Security and Cryptology (ICISC, 2021) 국제 학술대회의 Program committee로 활동함
- Cryptographic Hardware and Embedded Systems (CHES, 2022) 국제 학술대회의 Program committee로 활동함
- The 25th Annual International Conference on information Security and Cryptology (ICISC, 2022) 국제 학술대회의 Program committee로 활동함
- Fault Diagnosis and Tolerance in Cryptography (FDTC, 2023) 국제 학술대회의 Program committee로 활동함
- The 26th Annual International Conference on information Security and Cryptology (ICISC, 2023) 국제 학술대회의 Program committee로 활동함
- 한국정보보호학회 제 24회 정보보호응용 국제 컨퍼런스 (WISA, 2023) Organizing committee으로 활동함

▶ 박수현 교수
- 한국멀티미어학회 편집운영위원으로 활동함
- 대한전자공학회 컴퓨터소사이어티 부회장으로 활동함
- 한국시뮬레이션학회 논문지편집위원회 자문위원으로 활동함

3.2 참여교수의 국제공동연구 실적

<표 3-7> 사업 참여 기간 내 참여교수 국제공동연구 실적

연번	공동연구 참여자		상대국/ 소속기관	국제공동연구 실적	DOI 번호/ISBN 등 관련 인터넷 link 주소
	교육연구단 참여교수	국외 공동연구자			
1	유일선	Willy Susilo	호주/ 월런공대학교	안전한 차세대 IoT 통신 환경 구축을 위한 양자내성암호 최적화 및 보안 프로토콜 적용 연구	
2	이옥연	Laxmi Lydia	India / Vignan's Institute of Information Technology	3.367의 IF를 갖는 Hindawi WCMC에 "Rider Optimization with Deep Learning Based Image Encryption for Secure Drone Communication" 논문을 게재함. 본 논문은 긴급 모니터링 시나리오에서 효과적인 보안 통신 및 분류 프로세스를 위해 이미지 암호화 기반 보안 드론 통신(ODLE-SDC) 기법을 통한 최적의 딥러닝을 제안함	
3	한동국	Olivier Thomas	프랑스/Texplained	본 연구는 국제공동연구 과제 "딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발"을 통해 수행됨	https://www.ntis.go.kr/project/pjtInfo.do?pjtId=1415177709&pageCode=TH_PJT_PJT_DTL
총 환산 참여교수 수			10.57	**제출 요구량**	3~11

3.3 외국 대학 및 연구기관과의 연구자 교류 실적

- 유일선 교수팀은 일본의 연구기관 산업기술총합연구소(AIST; National Institute of Advanced Industrial Science and Technology)과 3차례 공동연구 협력을 통해 국제 저널에 논문을 게재하였음
- 유일선 교수팀은 인도네시아의 대학교 Udayana University와 연구 협력을 통해 국제적인 5G 네트워크 보안 기법에 대해 교류하고 AI 보안 및 블록체인 등과 같은 신규 기술을 적용할 수 있는 방안에 대하여 논의함
- 유일선 교수팀은 호주의 월런공대학교와 국제 공동연구 진행을 통해 IoT 통신 환경에 맞는 양자내성암호 최적화 및 보안 프로토콜을 적용할 수 있는 연구를 수행하고 있음
- 유일선 교수팀은 필리핀의 University of San Carlos와 연구협력을 통해 IoT 통신 환경에서의 양자내성암호를 실제로 구현하는 방안에 대하여 논의하였음
- 유일선 교수팀은 매년 국제 학술대회 MobiSec을 개최하여 교육연구단 소속 학생들의 정보보안 분야의 국제적 학문발전 경험을 지원하였음
- 한동국 교수팀은 2021년 3월에 싱가폴 난양기술대학교 PACE 연구팀의 연구원을 초청하여 Cold boot attack과 Machine Learning 기반 부채널 분석 주제로 연구 교류를 수행하였음
- 박수현 교수팀은 핀란드의 Savonia 대학교와 국제 공동 연구 활동을 통해 수중 통신 관련 최신 동향에 대해 분석하여 국제 학술대회에 논문을 게재하였음
- 박수현 교수팀은 ICGHIT 2024(국제 녹색 및 인간 정보 기술 학회)에서는 Special Communication & Convergence Services 2024 워크샵을 성공적으로 주최함으로써, 소속 학생들이 특별한 환경에서의 통신 네트워크와 정보보안 분야에 있어서의 국제적인 학문적 발전에 기여하는 경험을 얻을 수 있도록 지원하였음.