『4단계 BK21사업』 혁신인재 양성사업(산업·사회 문제 해결분야)
교육연구단 자체평가보고서

<table>
<tr><td colspan="2">접수번호</td><td colspan="8">-</td></tr>
<tr><td>사업 분야</td><td>혁신인재
양성사업</td><td>신청분야</td><td colspan="2">산업·사회
문제 해결분야</td><td>단위</td><td>전국</td><td>구분</td><td colspan="2">교육연구단</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="2">관련분야</td><td colspan="2">관련분야</td></tr>
<tr><td>중분류</td><td>소분류</td><td>중분류</td><td>소분류</td><td>중분류</td><td>소분류</td></tr>
<tr><td>분류명</td><td>컴퓨터학</td><td>정보보호</td><td>수학</td><td>응용수학</td><td>전자/정보통신공학</td><td>정보통신</td></tr>
<tr><td>비중(%)</td><td colspan="2">50%</td><td colspan="2">30%</td><td colspan="2">20%</td></tr>
<tr><td>교육연구
단명</td><td colspan="9">(국문) 안전한 초연결사회를 위한 문제해결형 정보보안 교육연구단
(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="7">국민대학교 과학기술대학 정보보안암호수학과</td></tr>
<tr><td colspan="2">직 위</td><td colspan="7">교수</td></tr>
<tr><td rowspan="4">성명</td><td>국문</td><td colspan="2">이옥연</td><td>전화</td><td colspan="3"></td></tr>
<tr><td></td><td></td><td>팩스</td><td colspan="3"></td></tr>
<tr><td>영문</td><td colspan="2">Yi, Okyeon</td><td>이동전화</td><td colspan="3"></td></tr>
<tr><td></td><td></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>4차년도
('23.3~'24.2)</td><td>5차년도
('24.3~'25.2)</td><td>6차년도
('25.3~'26.2)</td><td>7차년도
('26.3~'27.2)</td><td>8차년도
('27.3~'28.2)</td></tr>
<tr><td colspan="2">국고지원금</td><td>258,720</td><td>562,301</td><td>517,440</td><td>517,440</td><td>517,440</td><td>517,440</td><td>517,440</td><td>258,720</td></tr>
<tr><td colspan="3">총 사업기간</td><td colspan="7">2020.9.1.-2027.8.31.(84개월)</td></tr>
<tr><td colspan="3">자체평가 대상기간</td><td colspan="7">2020.9.1.-2021.8.31.(12개월)</td></tr>
</table>

본인은 관련 규정에 따라, 『4단계 BK21』 사업 관련 법령, 귀 재단과의 협약에 따라 다음과 같이 자체평가보고서 및 자체평가결과보고서를 제출합니다.

2021년 9월 17일

작성자	교육연구단장	이옥연	(인)
확인자	국민대학교 산학협력단장	오하령	(인)

<자체평가 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
달성정도</td><td colspan="3">▶ 본 교육연구단은 초연결사회의 정보보안을 선도하는 전문가 양성을 목표로 함
■ 목표 달성을 본 교육연구단은 단계별 인력양성 프로그램 로드맵을 세워 추진 중임
■ 1단계(2020~2021) 기간에서의 목표를 정보보안 교육체계 수립으로 선정하여, 이를 위해 다양한 교육과정과 연구를 수행하였으며, 기존 대학원생을 중심으로 정보보안 협동과정의 교과목 및 AI 융합과정 개발을 수행하였음
■ 자체평가 대상 기간(2020.9.1.~2021.8.31.)동안 신청서에 작성된 37개의 교과 구성 중 11개 교과를 운영하였으며, 이는 전체 교과 구성 중 약 30%를 달성한 것임
■ 교육연구단의 참여교수들은 교과과정 외에도 운영하는 랩을 통해 통신 보안, 디바이스 보안, 암호기술, AI 응용 분야에 관한 심화 연구를 수행 중임
■ 연구를 통해 얻은 연구성과는 국내외 학술대회와 논문지에 발표하였으며, 공모전 참여, 특허출원 등의 추가적인 성과를 내었음</td></tr>
<tr><td>교육역량 영역
성과</td><td colspan="3">▶ 교육과정의 개편을 통해 우수 인재 양성에 힘쓰고 있음
■ 참여교수인 이옥연, 박수현 교수는 통신 분야의 5G / 6G와 수중통신 환경의 정보보안 구현, 초연결 통신환경을 위한 정보보안 서비스 신뢰성 확보를 위한 교육을 추진함
✓ 고급정보통신론, 임베디드시스템, 실시간시스템, 무선보안특강, 클라우드컴퓨팅, 이동통신보안, 정보시스템개발방법론, IoT네트워크 과목을 주요 과목으로 선정하고 연차별로 과목 개설하였으며, 5G에서 6G에 이르는 보안 관련 기술의 표준화 분야 전문가들을 초청하여 워크숍 및 콜로키움 개최 예정임
■ 참여교수인 한동국, 김종성, 서석충 교수는 디바이스 보안 분야의 다양한 부채널 정보를 이용한 공격 및 대응기술 개발, 디지털 포렌식 기술을 이용한 증거획득 기술 및 산업보안 기술, 디바이스별 암호 소프트웨어 및 하드웨어 고속 구현기술 확보를 위한 교육을 주진함
✓ 부채널공격론, 보안구현개발방법론, 디지털포렌식개론, 부채널공격대응론, 디지털포렌식특수연구, 디바이스공격대응론 과목을 주요 과목으로 선정하고 연차별로 과목 개설을 하고 있음
■ 참여교수인 강주성, 염용진, 김동찬 교수는 안전한 양자내성암호의 개발 및 안전성 검증, 안전하고 효율적인 구현을 통한 보안제품의 개발기술 확보를 위한 교육을 추진함
✓ 해시함수와데이터인증, 병렬암호구현, 정보보안프로토콜, 공개키 암호분석이론, 암호소프트웨어구현, 대칭키암호분석, 난수성분석론, 증명가능안전성론, 암호모듈평가및검증 과목을 주요 과목으로 선정하고 연차별로 과목 개설을 하고 있음
■ 참여교수인 최은미, 윤상민 교수는 데이터마이닝, 분산지능화 시스템, 인공지능 기술, 빅데이터 분석 및 적대적 공격 / 방어 시스템 개발기술 확보를 위한 교육을 추진함
✓ 데이터마이닝, 인공지능과 보안 이론, 모델기반시스템설계, 자율성장 인공지능 특론, 인공지능 융합기술 특강 과목을 주요 과목으로 선정하고 연차별로 과목 개설을 하고 있음
▶ 교육과정 편찬 추진 외에도 우수 인재 양성을 위해 보안강연 및 워크숍 등을 진행하고 있음</td></tr>
</table>

	■ 5G+ 6G를 향한 양자보안과 KCMVP 암호 발전 동향(2021.05.17.), 한양대 ■ QRNG 기반 암호모듈 활용 방안(2021.07.21.), 국가보안기술연구소 ■ Collision Search and its Applications (2021.1.26.), 고려대 ■ 외 5건의 강연 및 2건의 워크숍 진행 ▶ 선정평가 당시 본 연구단에서 제안한 연구 역량 향상을 위한 대학원생 지원을 계획하였음 ■ 결과 자체 평가 기간 내에 국제 저널 21건, 국내 저널 16건, 국제 학회 8건, 국내 학회 34건, 수상 13건을 달성하였음
연구역량 영역 성과	▶ 지속 가능한 발전을 선도하기 위해 본 연구단에서는 학부 및 대학원생에 대한 교육과 함께 다양한 연구를 진행하였음 ■ 자체평가 기간 내에 정부 48건, 산업체 8건 총 56건의 연구를 진행하였음 ■ 총 56건의 연구를 통해 56.6억에 해당하는 연구비를 수주해냈음 ■ 이 외에도 국제 저널 23건, 국내 저널 17건, 국제 학회 11건, 국내 학회 40건, 대표연구업적물 9건 등 많은 연구 결과를 내었음 ■ 상기 결과들을 토대로 현재 14건의 특허를 등록한 상태이며 22건이 출원된 상태임 ▶ 연구 결과를 기반으로 3건의 기술이전을 시행하였으며 다양한 매체를 통해 산업·사회에 대한 기여하였음 ▶ 총 6건의 국제적 학술활동에 참여하고 국제 공동연구 및 연구자 교류를 진행함으로써 연구역량의 확대를 진행하고 있음
달성 성과 요약	▶ 세부목표 달성을 위해 공통기초 분야, 기반이론 분야, 핵심역량 분야, 심화응용 분야, 산업·응용 분야로 교과목을 나누어 공통기초 과정부터 실용과정까지 단계별로 체계화된 교과과정을 구성함 ▶ 현재 암호알고리즘, 해시함수와데이터인증, 정보보호프로토콜, 부채널공격대응론, 대칭키 암호분석, 비즈니스정보통신, 이동통신보안, 증명가능안정성론, 융합보안특강, 보안기술표준분석및구현 과목을 개설해 융합교육을 실현 중임 ▶ 다양한 융합교육 및 랩별 심화 연구를 통해 다양한 연구성과를 내었음 ▶ 자체평가 대상 기간(2020.9.1.~2021.8.31.)동안 국제 저널 23건, 국내 저널 17건, 국제 학회 11건, 국내 학회 40건, 특허 등록 14건, 특허 출원 22건, 기술이전 3건, 연구비 수주 56건, 국내외 수상 13건, 강연 8건, 워크숍 2건의 실적을 달성하였음 ▶ 해당 기간 동안 석사 15명, 박사 5명, 석·박사 통합 1명을 확보하였으며, 석사 졸업생 8명, 박사 졸업생 2명을 배출하였음
미흡한 부분 / 문제점 제시	▶ 코로나19(COVID-19)로 인해 국제적 교류 및 산학협력에 미진했음
차년도 추진계획	▶ 본 교육연구단의 2단계(2022~2024) 기간에서의 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

Ⅰ 교육연구단의 구성, 비전 및 목표

1. 교육연구단장의 교육・연구・행정 역량

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

▶ 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

▶ 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

✓ 교육연구단장은 IoT, 스마트미터 등 6G에 포함될 수 있는 다양한 환경에서 보안 서비스 개발을 위한 다수의 암호 및 보안 라이브러리 기술 및 개발, KCMVP 검증 실적, 상용화 실적을 보유하고 있음

✓ 이러한 기술을 바탕으로 한국전력공사 전력연구원과 공동으로 2016년 3월과 2017년 11월에 스마트그리드용 검증필암호모듈(CM-112-2021.03, CM-132-2022.11) 개발에 성공하여, 2016년 2,500억 규모의 200만 가구 및 2017년 3,000억원 규모의 300만 가구용 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. 대학원 학과(부) 소속 전체 교수 및 참여연구진

<표 1-1> 교육연구단 대학원 학과(부) 전임 교수 현황 (단위: 명, %)

대학원 학과(부)	학기	전체교수 수	참여교수 수	참여비율(%)	비고
금융정보보안학과	20년 2학기	10	10	100	
	21년 1학기	10	10	100	

<표 1-2> 최근 1년간(2020.9.1.~2021.8.31.) 교육연구단 대학원 학과(부) 소속 전임 교수 변동 내역

연번	성명	변동 학기	전출/전입	변동 사유	비고
1	-	-	-	-	-

<표 1-3> 교육연구단 대학원 학과(부) 대학원생 현황 (단위: 명, %)

대학원 학과(부)	참여 인력 구성	대학원생 수											
		석사			박사			석·박사 통합			계		
		전체	참여	참여 비율 (%)	전체	참여	참여 비율 (%)	전체	참여	참여 비율 (%)	전체	참여	참여 비율 (%)
금융정보 보안학과	20년 2학기	19	10	52.6	12	12	100	2	1	50	33	23	69.6
	21년 1학기	26	14	53.8	11	11	100	3	3	100	40	28	70
참여교수 대 참여학생 비율		1 : 2.5											

▶ 교수진의 변화 없었음
▶ 본 교육연구단 대학원은 20년 2학기 석사 19명, 박사 12명, 석·박사 통합 2명 재학 중이었으며, 전체 참여 비율 69.6%를 달성하였음
▶ 본 교육연구단 대학원은 21년 1학기 석사 26명, 박사 11명, 석·박사 통합 3명 재학 중이었으며, 전체 참여 비율 70%를 달성하였음

2. 교육연구단의 비전 및 목표 달성정도

▶ 본 교육연구단은 초연결사회의 정보보안을 선도하는 전문가 양성을 목표로 정보보안 교육과정을 운영중임
- ■ 목표달성을 위해 암호이론 / 정보보안 / AI 분야의 융합교육을 실현하고 있음
- ■ 자체평가 대상 기간(2020.9.1.~2021.8.31.)동안 신청서에 작성된 37개의 교과 구성 중 11개 교과를 운영하였으며, 이는 전체 교과 구성 중 약 30%를 달성한 것임
- ■ 교육연구단의 참여교수들은 교과과정 외에도 운영하는 랩을 통해 통신 보안, 디바이스 보안, 암호기술, AI 응용 분야에 관한 심화 연구를 수행 중임
- ■ 연구를 통해 얻은 연구성과는 국내외 학술대회와 논문지에 발표하였으며, 공모전 참여, 특허출원 등의 추가적인 성과를 내었음
- ■ 자체평가 기간 내에 국제 저널 23건, 국내 저널 17건, 국제 학회 11건, 국내 학회 40건, 수상 13건을 달성하였음
- ■ 자체평가 기간 내에 정부 48건, 산업체 8건 총 56건의 연구를 진행하였음

▶ 코로나19(COVID-19)로 인해 국제적 교류 및 산학협력에 미진했음

II 교육역량 영역

□ 교육역량 대표 우수성과(자체평가 대상 기간 2020.9.1.~2021.8.31.)

▶ 자체평가 대상 기간 내 국제 저널 19편, 국내 저널 16편, 국제 학회 8편, 국내 학회 34편의 논문 발표, 수상 13건, 특허 17건 등의 성과를 냄

▶ 국제 저널

- “Privacy Preservation in Edge Consumer Electronics by Combining Anomaly Detection with Dynamic Attribute-Based Re-Encryption”, Eunmok Yang, Velmurugan Subbiah Parvathy, P.pandi Selvi, K.shankar, Changho Seo;Gyanendra Prasad Joshi, Okyeon Yi, MDPI Mathematics (SCIE, IF=1.747)
- “A methodology for the decryption of encrypted smartphone backup data on android platform: A case study on the latest samsung smartphone backup system”, Myungseo Park, Okyeon Yi, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, IF=1.660)
- “Single-Trace Attacks on Message Encoding in Lattice-Based KEMs”, Bo-Yeon Sim, Jihoon Kwon, Joohee Lee, Il-Ju Kim, Tae-Ho Lee, Jaeseung Han, Hyojin Yoon, Jihoon Cho, Dong-Guk Han, IEEE Access(3.367)
- “Improved Differential Fault Attack on LEA by Algebraic Representation of Modular Addition”, Seonghyuck Lim, Jonghyeok Lee, Dong-Guk Han, IEEE Access(3.367)
- “Efficient Implementation of a Crypto Library Using Web Assembly”, Bosun Park, JinGyo Song, Seog Chung Seo (Corresponding), MDPI Electronics (SCIE, IF=2.412)
- “Efficient Implementation of ARX-based Block Ciphers on 8-bit AVR Microcontrollers”, YoungBeom Kim, Hyeokdong Kwon, SangWoo An, Hwajeong Seo, Seog Chung Seo(Corresponding), MDPI Mathematics (SCIE, IF=1.747)
- “Parallel Implementations of ARX-based Block Ciphers on Graphic Processing Units”, SangWoo An, YoungBeom Kim, Hyeokdong Kwon, Hwajeong Seo, Seog Chung Seo(Corresponding), MDPI Mathematics (SCIE, IF=1.747)
- “Efficient Parallel Implementations of LWE-based Post-Quantum Cryptosystems on Graphics Processing Units”, SangWoo An, Seog Chung Seo(Corresponding), MDPI Mathematics (SCIE, IF=1.747)
- “Secure and Fast Implementation of ARX-Based Block Ciphers Using ASIMD Instructions in ARMv8 Platforms”, JinGyo Song, Seo Chung Seo(Corresponding), IEEE ACCESS (SCIE, IF=3.745)
- “Designing a CHAM Block Cipher on Low-End Microcontrollers for Internet of Things”, Hyeokdong Kwon, SangWoo An, YoungBeom Kim, Hyunji Kim, Seung Ju Choi, Kyoungbae Jang, Jaehoon Park, Hyunjun Kim, Seog Chung Seo, Hwajeong Seo, MDPI Electronics (SCIE, IF=2.412)
- “Efficient Implementation of NIST LWC ESTATE Algorithm using OpenCL and Web Assembly for Secure Communication in Edge Computing Environment”, BoSun Park and Seog Chung Seo(Corresponding), MDPI Sensors (SCIE, IF=3.275)
- “Efficient Parallel Implementation of CTR mode of ARX-based Block ciphers on ARMv8 Microcontrollers”, JinGyo Song and Seog Chung Seo(Corresponding), MDPI Applied Sciences (SCIE, IF=2.474)
- “Chaining optimization methodology: A New SHA-3 Implementation on Low-End Microcontrollers”, YoungBeom Kim, Taek-Young Youn, and SeogChung Seo(Corresponding), MDPI Sustainability (SSCI, IF= 2.576)

- “Forensic analysis of instant messaging apps: Decrypting Wickr and private text messaging data.“, Giyoon Kim, Soram Kim, Myungseo Park, Younjai Park, Insoo Lee, and Jongsung Kim, Forensic Science International: Digital Investigation 37 (2021): 301138. (SCIE, IF=1.66)
- “Research on Note-Taking Apps with Security Features.“, Myungseo Park, Soram Kim, and Jongsung Kim, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications Vol.11(4),(2020):63-76 (SCOPUS)
- “Magniber v2 Ransomware Decryption: Exploiting the Vulnerability of a Self-Developed Pseudo Random Number Generator.“, Sehoon Lee, Myungseo Park, and Jongsung Kim, Electronics Vol.10(1), (2020): 16. (SCIE, IF=2.412)
- “Smart Home Forensics—Data Analysis of IoT Devices“, Soram Kim, Myungseo Park, Sehoon Lee, Jongsung Kim, Electronics, Vol.9(8), (2020): 1215. (SCIE, IF=2.412)
- “A study on the decryption methods of telegram X and BBM-Enterprise databases in mobile and PC“, Giyoon Kim, Myungseo Park, Sehoon Lee, Younjai Park, Insoo Lee, Jongsung Kim , Forensic Science International: Digital Investigation Vol.35 (2020): 300998. (SCIE, IF=1.66)
- “Generating Cryptographic S-Boxes Using the Reinforcement Learning“, Giyoon Kim, Hangi Kim, Yeachan Heo, Yongjin Jeon, Jongsung Kim, IEEE ACCESS. (SCIE, I.F=3.745)

▶ 국내 저널

- “양자 엔트로피 기반 난수 발생기를 이용한 드론 제어 데이터 보안 연구” , 김태완, 이세윤, 정서우, 위한샘, 이옥연, 정보보호학회논문지 2021년 4월 호
- “5G+ 초연결 환경을 위한 암호기술 연구” , 장찬국, 김현기, 윤승환, 이옥연, 정보보호학회지 2020년 12월 호
- 다중 사용자 환경에서 효과적인 키 교환을 위한 GPU 기반의 NTRU 고속구현” , 성효은, 김예원, 염용진, 강주성, 2021 한국통신학회논문지 31호
- “CHES 2020을 중심으로 살펴본 SW/HW 암호 분석 및 구현 기술 연구 동향“, 안상우, 송진교, 박보선, 서석충, 정보보호학회지 2020년 12월 호
- “GPU를 활용한 고속 소프트웨어 암호모듈 설계 및 구현“, 송진교, 안상우, 서석충, 정보보호학회논문지(KCI) 2020년 12월 호
- “NIST PQC Round 3 격자 기반 암호의 부채널 대응 기법 동향 분석“, 송진교, 김영범, 곽유진, 서석충, 정보보호학회지 2021년 2월 호
- “ARM/NEON 프로세서를 활용한 NIST PQC SABER에서 Toom-Cook 알고리즘 최적화 구현 연구“, 송진교, 김영범, 서석충, 정보보호논문지(KCI) 2021 6월 호
- “32-bit RISC-V 프로세서에서 국산 블록 암호 성능 밴치마킹“, 곽유진, 김영범, 서석충, 정보보호논문지(KCI) 2021 6월 호
- “블록암호 RECTANGLE에 대한 DLCT를 이용한 차분-선형 공격“, 조세희, 백승준, 김종성, 정보보호학회논문지, 31권, 2호, pp. 123-132, 2021.
- “OBD 스캐너 애플리케이션 INFOCAR 데이터 분석을 통한 차량 포렌식 기법“, 허욱, 김기윤, 김종성, 디지털포렌식연구, 15권 2호, pp. 137-147, 2021.
- “협업 툴 아티팩트 분석 및 삭제된 데이터 복구 연구“, 신수민, 최용철, 김소람, 김종성, 디지털포렌식연구, 15권 2호, pp. 235-259, 2021.
- “키 재사용 공격을 통한 RAGNAR LOCKER 랜섬웨어 감염 파일 복호화 및 활용 방안 연구“, 강수진, 이세훈, 김소람, 김대운, 김기문, 김종성, 정보보호학회논문지, 31권 2호, pp. 221-231, 2021.
- “샤오미 스마트 홈 아티팩트 분석 및 활용방안 연구“, 강수진, 신수민, 김소람, 김기윤, 김종성, 디지털포

렌식연구, 15권 1호, pp. 54-67, 2021.

- "Windows에서의 Wire 크리덴셜 획득 및 아티팩트 분석", 신수민, 김소람, 윤병철, 김종성, 정보보호학회 논문지, 31권 1호, pp. 61-71, 2021.
- "5ss5c와 Immuni 랜섬웨어의 암호화 프로세스 분석 및 복구방안 연구", 신수민, 김소람, 윤병철, 허욱, 김대운, 김기문 김종성, 디지털콘텐츠학회논문지, 21권 10호 pp. 1895-1903, 2020
- "안드로이드 악성코드 탐지를 위한 머신러닝 기술 활용 동향 및 권한정보를 활용한 악성코드 탐지", 김기윤, 김소람, 전용진, 김종성, 디지털포렌식연구, 14권 3호, pp. 316-326, 2020.

▶ 국제 학회

- "Analysis of public-key cryptography using a 3-regular graph with a perfect dominating set", 권수진, 강주성, 염용진 ,IEEE Region 10 Symposium, 2021 Best Paper 수상
- "Fault Injection Method for Hardware-implemented AES without Artificial Triggering", 임한섭, 이태호, 임성혁, 한재승, 한동국, 2020 ACM International Conference on Intelligent Computing and Its Emerging Applications
- "Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-based Profiling", 김일주, 이태호, 한재승, 한동국, 2020 ACM International Conference on Intelligent Computing and Its Emerging Applications
- "Machine Learning-Based Profiling Attack Method in RSA Prime Multiplication", 박한별, 한동국 , 2020 ACM International Conference on Intelligent Computing and Its Emerging Applications
- "PIPO: A Lightweight Block Cipher with Efficient Higher-Order Masking Software Implementations", Hangi Kim, Yongjin Jeon, Giyoon Kim, Jongsung Kim, Bo Yeon Sim, Dong Guk Han, Hwajeong Seo, Seonggyeom Kim, Seokhie Hong, Jaechul Sung, Deukjo Hong (ICISC 2020)
- "Parallel Implementation of PIPO Block Cipher on 32-bit RISC-V Processor", Yujin Kwak, YounngBeom Kim, Seog Chung Seo, 22st World Conference on Information Security Applications (WISA 2021)
- "High-Speed Software of Karatsuba Multiplication for SABER Round 3 on ARMv8-A Series", JinGyo Song, YounngBeom Kim, Seog Chung Seo, 22st World Conference on Information Security Applications (WISA 2021)
- "XTS-AES Parallel Optimization Implementation Technique for Fast FDE", SangWoo An and Seog Chung Seo, 22st World Conference on Information Security Applications (WISA 2021)

▶ 국내 학회

- "5G-AKA 및 SMC의 RAN 취약점 분석", 김태완, 김현기, 이옥연, 2021 한국정보보호학회 하계학술대회
- "6G 보안을 위한 5G 코어 오픈소스 프로젝트 분석", 이세윤, 위한샘, 윤승환, 이옥연, 2021 한국정보보호학회 하계학술대회
- "Lua 스크립트 기반 5G AKA wireshark 플러그인 제작", 정서우, 장찬국, 이옥연, 2021 한국정보보호학회 하계학술대회
- "IoT 보안 인증 제도 기반 홈 IoT 기기 애플리케이션의 취약점 분석 및 대응책 제시", 윤혜진, 김은주, 최지원, 위한샘, 이옥연, 2021 한국정보보호학회 하계학술대회
- "모의 공격을 통한 MAVLink 프로토콜 취약점 분석", 한주홍, 위한샘, 이옥연, 2020 한국정보보호학회 동계학술대회
- "CSFC 내 MSC 솔루션 보안요구사항 비교분석", 정서우, 오진혁, 장찬국, 이옥연, 2020 한국정보보호학회 동계학술대회
- "UAS 보안인증 시험을 위한 보안 요구사항", 이세윤, 장찬국, 이옥연, 2020 한국정보보호학회 동계학술대회

- “클라우드 컴퓨팅 서비스 보안 인증제도 개선사항”, 김태완, 김현기, 장찬국, 이옥연, 2020 한국정보보호학회 동계학술대회
- “이진 Goppa 부호 구현에 관한 연구”, 전창열, 김동찬, 2021 한국통신학회 하계학술대회
- “GPU 환경에서의 효율적인 Number Theoretic Transform 최적화 구현“, 안상우, 서석충, 2020 정보보호학회 동계학술대회
- “NEON을 활용한 NIST 양자암호 Saber에서 다항식 곱셈기반 Toom-Cook 알고리즘 최적화 연구“, 송진교, 김영범, 서석충, 2020 정보보호학회 동계학술대회
- “RISC-V 환경에서 Curve25519의 Reduction 연산 최적화 연구“, 김영범, 송진교, 서석충, 2020 정보보호학회 동계학술대회
- “ARM Cortex-M4 환경에서 SIMD 명령어를 이용한 CHAM-64/128 최적화 연구“, 이정민, 송진교, 서석충, 2020 정보보호학회 동계학술대회
- “격자기반 양자내성암호에서 RST를 이용한 기각 샘플링 병렬 최적화“, 안상우, 서석충, 2021 한국컴퓨터종합학술대회
- “타원곡선 암호의 최적화 구현, 부채널 대응기법 동향 분석 및 벤치마킹“, 송진교, 서석충, 2021 한국컴퓨터종합학술대회
- “GPU 환경에서의 NIST PQC 3-round Lattice 및 Symmetric 기반 전자서명 최적화 구현 동향“, 최호진, 서석충, 2021 한국컴퓨터종합학술대회
- “Metamorphic Testing기반 암호알고리즘 구현 정확성 검증 기술 동향 분석“, 김영범, 서석충, 2021 한국컴퓨터종합학술대회
- “Web Assembly를 이용한 국산 블록 암호 알고리즘 벤치마킹“, 박보선, 서석충, 2021 한국컴퓨터종합학술대회
- “중간값 참조 테이블을 활용한 CPU-GPU 하이브리드 AES-XTS 최적화 기법”, 안상우, 서석충, 2021 정보보호학회 하계학술대회
- “ARMv8-A Series에서 Crystal-Dilithium Round 3의 NTT 곱셈 병렬 구현”, 송진교, 김영범, 서석충, 2021 정보보호학회 하계학술대회
- “GPU 환경에서의 SHA-3(512) 병렬 최적 구현”, 최호진, 서석충, 2021 정보보호학회 하계학술대회
- “8-bit AVR 환경에서 PIPO 최적 구현”, 김영범, 서석충, 2021 정보보호학회 하계학술대회
- “OpenCL, OpenMP 병렬처리를 사용한 PIPO 알고리즘 구현”, 박보선, 서석충, 2021 정보보호학회 하계학술대회
- “확장된 RNBP 알고리즘“, 박종현, 전용진, 김종성, 정보보호학회 하계 학술대회, 2021.
- “축소 라운드 GIFT의 향상된 차분 선형 특성“, 백승준, 김한기, 김종성, 정보보호학회 하계 학술대회, 2021.
- “NIST 경량암호 공모사업 후보 알고리즘 HyENA의 안전성 분석 동향“, 김주헌, 김시은, 박종현, 백승준, 김종성, 한국정보보호학회 동계 학술대회, 2020.
- “NIST 경량암호 공모사업 후보 알고리즘 COMET의 안전성 분석 동향“, 조세희, 백승준, 김종성, 한국정보보호학회 동계 학술대회, 2020.
- “ARIA에 대한 Shifting Retracing 부메랑 공격”, 백승준, 박종현, 김종성, 한국정보보호학회 동계 학술대회, 2020.
- “디지털 포렌식 관점에서 협업 및 화상회의 애플리케이션 분석“, 신수민, 김소람, 강수진, 김종성, 한국디지털포렌식학회 하계 학술대회, 2021.
- “사진 및 동영상/은닉 암호화 특정 애플리케이션 분석“, 최용철, 김기윤, 김종성, 정보보호학회 하계 학술대회, 2021.
- “윈도우 환경에서 Pinngle 및 미스리 메신저 아티팩트 분석“, 박귀은, 김수빈, 김현재, 이민정, 옥정수, 신

수민, 김종성, 정보보호학회 하계 학술대회, 2021.

- “2020년 및 2021년 국내·외 랜섬웨어 대응 정책 동향“, 강수진, 김수빈, 이민정, 김소람, 김종성, 정보보호학회 하계 학술대회, 2021.
- “Ragnar Locker 랜섬웨어 데이터 복호화 방안 연구”, 강수진, 이세훈, 김소람, 김종성, 정보보호학회 동계 학술대회, 2020.
- “디지털 포렌식 관점에서의 샤오미 스마트 홈 아티팩트 분석”, 강수진, 신수민, 김소람, 김기윤, 김종성, 한국디지털포렌식학회 동계 학술대회, 2020.

▶ 수상

- 2021 한국정보보호학회 하계학술대회 우수논문상
- 2021 한국컴퓨터 종합학술대회 우수발표논문상 (KCC 2021)
- 2020 국가암호 공모전 최우수상 1건, 장려상 1건, 특별상 3건 수상
- 2020 한국정보보호학회 동계학술대회 한국전자통신연구원 원장상 수상
- 2020 한국디지털포렌식학회 동계학술대회 디지털포렌식학회 학회장상 수상
- 2020 부채널 분석 경진대회 학회장상 수상
- 2020 국가암호공모전 특별상 수상
- 2020 암호분석경진대회 대상 수상
- 2020 디지털 포렌식 챌린지 Tech Contest 입상 (2위)

▶ 참여교수 교육대표실적

- 보안 강연
  - ✓ 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
  - ✓ Code-based Cryptography (2020.11.12.), NSHC
  - ✓ Collision Search and its Applications (2021.1.26.), 고려대
  - ✓ Code-based Cryptography (2021.7.19.), 한성대
- 워크숍
  - ✓ 제3회 부채널 분석 워크숍(2020.10.29.~2020.10.30.)
    - 부채널 분석 워크숍을 주관하여 개최함
  - ✓ 부채널 공격 대응이 용이한 경량암호 PIPO 개발 및 응용(2021.05.20.), CPS 보안 워크숍
    - 부채널 공격 대응기법 설계가 용이한 경량암호 PIPO 개발에 대한 강연
- 토론회
  - ✓ 수중통신 세계 표준화 (인천국제해양포럼 개최)
    - IoT-스마트 해양 세션의 ‘수중통신 세계표준화’ 주제로 온/오프라인 하이브리드 토론을 주도함
- 표준화 활동
  - ✓ 박수현 교수는 지난 10년간 ISO/IEC JTC 1/SC 41에서 ’수중통신’ 기술 국제 공적 표준화 위원으로 활동하였음

▶ 국내 특허

- DUSS 지원 가능한 양자난수 엔트로피 암호화용 코드 발급 장치 및 방법
- 구명용 비상신호 발신장치 및 방법

■ 경량 엔트로피 관리 장치 및 방법
■ 경량 블록 암호화에 대한 고차 부채널 공격에 대응하는 방법 및 이를 이용한 장치
■ 경량 블록 암호화에 대한 1차 부채널 공격에 대응하는 방법 및 이를 이용한 장치
■ NTRU LPRime 암호에 대한 부채널 분석 장치 및 방법
■ 부채널 공격 대응이 용이한 128비트 경량 블록 암호화 방법 및 이를 이용한 장치
■ 수중 사물 인터넷의 온톨로지 기반 통신 매체 선택 방법 및 이를 수행하는 수중 통신 장치
■ 무선 통신 기기 및 이의 동작 방법
■ 수중 네트워크 관리 시스템 및 그의 동작 방법
■ TUM-IoT에서의 심리스 서비스 기반 경로 설정 기법
■ 수중 네트워크 관리 시스템
■ 수중 네트워크 관리 시스템 및 그의 동작 방법
■ 종단간 암호화가 적용된 파일에 대한 복호화 장치 및 방법
■ 캐시 파일을 이용한 삭제 메시지 복구 장치 및 방법
■ 부채널 공격 대응이 용이한 128비트 경량 블록 암호화 방법 및 이를 이용한 장치

▶ 기술이전
■ 양자난수 기반 UAV용 LTE 암호장비 개발 기술
■ KMULIB v2.1 Windows용 KCMVP 검증필암호모듈
■ 하이브리드 수중무선통신 장치 및 그 통신 방법

▶ 국제 특허 등록
■ Apparatus and Method for Inspecting Side Channels of Combined Smartcard (EP3232375B1)
✓ 콤비형 스마트카에 대한 부채널 분석 방법을 개발한 특허임

▶ 국제 공적 표준
■ 국제 공적 표준 SDO(Standard Development Organization) 수중통신, 해양통신, 디지털트윈 분야 ISO/IEC JTC 1/SC 41 WG7이 신설되었으며, 해당 WG의 Convener로 박수현 교수 선정, 앞으로 3년간 미래 디지털전환, 해상, 수중통신 도메인 기술 촉진에 필요한 표준화를 주도할 기회를 획득함('21.06)

1. 교육과정 구성 및 운영

1.1 교육과정 구성 및 운영 현황과 계획

▶ 대학원 교육과정 구성 및 학사관리 운영계획
■ 암호알고리즘, 해시함수와데이터인증, 정보보호프로토콜, 부채널공격대응론, 대칭키암호분석, 비즈니스정보통신, 이동통신보안, 증명가능안정성론, 융합보안특강, 보안기술표준분석및구현 과목을 개설해 운영하였으며, 이는 신청서 대비 약 30%의 실적 달성임
■ 향후 신청서에 명시된 과목들을 추가로 개설하여 목표달성에 힘쓸 예정임

▶ 교육단의 교육 목표 달성 방안
■ 본 교육단의 최종 목표는 미래통신/ 디바이스 / 암호 / AI 분야의 정보보안 문제 해결형 융합 교육의 실현 및 전문인력 양성임
■ 본 교육단은 목표 달성을 위해 다음 세부목표를 세워 진행중임

- ✓ 암호이론/정보보안/AI 분야의 융합교육 실현
- ✓ 미래 초연결 환경의 지속 가능한 발전을 선도하는 정보보안 전문인력 양성
- ✓ 보안위협에 대한 선제적 대응을 위한 원천기술 개발 및 상용화를 통한 실무형 인재 교육
- ✓ ICT 기술의 융합을 통한 새로운 미래 비즈니스 모델 창출형 인재 교육
  - 위 세부 목표 달성을 위해 공통기초 분야, 기반이론 분야, 핵심역량 분야, 심화응용 분야, 산업·응용분야로 교과목을 나누어 공통기초 과정부터 실용과정까지 단계별로 체계화된 교과과정을 구성함
  - 현재 암호알고리즘, 해시함수와데이터인증, 정보보호프로토콜, 부채널공격대응론, 대칭키암호분석, 비즈니스정보통신, 이동통신보안, 증명가능안정성론, 융합보안특강, 보안기술표준분석및구현 과목을 개설해 융합교육을 실현 중임
  - 참여 대학원생의 전문역량을 기르기 위해 다양한 연구과제에 참여하도록 하고 있으며, 연구를 통해 얻은 독창적인 연구성과를 국내외 학술대회와 논문지에 발표하였으며, 공모전 참여, 특허출원 등의 성과를 내었음
  - 해당 기간 동안 국제 저널 23건, 국내 저널 17건, 국제 학회 11건, 국내 학회 40건, 특허 등록 14건, 특허 출원 22건, 기술이전 3건, 연구비 수주 56건, 국내외 수상 13건, 강연 8건, 워크숍 2건의 실적을 달성하였음
  - 교육단으로부터 배출된 취·창업 인력들과 지속적인 협력, 교류를 통해 문제 해결을 위한 인적 네트워크를 형성하고, 실무에서의 지식을 공유하고 있음
- ✓ 참여교수인 이옥연, 박수현 교수는 통신 분야의 5G / 6G와 수중통신 환경의 정보보안 구현, 초연결 통신환경을 위한 정보보안 서비스 신뢰성 확보를 위해 다음과 같은 교육과정을 추진하고 있음
  - 고급정보통신론, 임베디드시스템, 실시간시스템, 무선보안특강, 클라우드컴퓨팅, 이동통신보안, 정보시스템개발방법론, IoT네트워크 과목을 주요 과목으로 선정하고 연차별로 과목 개설을 하고 있음
  - 유무선 통신 및 5G에서 6G에 이르는 보안 관련 기술의 표준화 분야 전문가들을 초청하여 워크숍 및 콜로키움 개최 등과 같이 특화된 교육 프로그램을 제공할 예정임
  - 또한, 6G 적응형 Underwater IoT의 글로벌 표준화를 주도하기 위하여 표준화 활동을 하는데 필요한 사항 등의 교육을 함께 제공하고 있으며, 연구와 교육의 질적 향상으로 이어지는 선순환 구조를 실행하고 있음
- ✓ 참여교수인 한동국, 김종성, 서석충 교수는 디바이스 보안 분야의 다양한 부채널 정보를 이용한 공격 및 대응기술 개발, 디지털 포렌식 기술을 이용한 증거획득 기술 및 산업보안 기술, 디바이스별 암호 소프트웨어 및 하드웨어 고속 구현기술 확보를 위해 다음과 같은 교육과정을 추진하고 있음
  - 부채널공격론, 보안구현개발방법론, 디지털포렌식개론, 부채널공격대응론, 디지털포렌식특수연구, 디바이스공격대응론 과목을 주요 과목으로 선정하고 연차별로 과목 개설을 하고 있음
  - 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 실시하고 있음
  - 수집되는 부채널 정보의 질을 높이기 위한 노이즈 최소화 기법, 노이즈 제거 기법에 대한 심화 과정에 대해 교육함
  - 또한, 오실로스코프와 스펙트럼 분석기 같은 고성능 장비를 활용한 부채널 정보 수집 환경을 제공할 뿐만 아니라, 노이즈를 제거하여 유의미한 신호를 증폭시키기 위한 압축 및 정렬과 같은 기초 전처리 기법부터 주파수 필터 등과 같은 다양한 신호처리 기법에 대해 교육하고 있음
  - 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 기

기 등의 디지털 기기에 대한 기본적인 이해를 위해 OS, 메모리, 저장공간 등의 전반적인 컴퓨터 이론을 교육함

- 다양한 암호화 알고리즘을 소프트웨어상에서 구현할 수 있는 프로그래밍 기술과 함께 각 환경에서의 최적화 방법론을 교육함

✓ 참여교수인 강주성, 염용진, 김동찬 교수는 안전한 양자내성암호의 개발 및 안전성 검증, 안전하고 효율적인 구현을 통한 보안제품의 개발기술 확보를 위해 다음과 같은 교육 과정을 추진하고 있음

- 해시함수와데이터인증, 병렬암호구현, 정보보안프로토콜, 공개키 암호분석이론, 암호소프트웨어구현, 대칭키암호분석, 난수성분석론, 증명가능안전성론, 암호모듈평가및검증 과목을 주요 과목으로 선정하고 연차별로 과목 개설을 하고 있음
- 자체평가 기간(2020.9.1.~2021.8.31.)동안 신청서에 명시되어 있는 목표달성을 위한 주요 과목 중 해시함수와데이터인증, 정보보호프로토콜, 대칭키암호분석, 증명가능안전성론 과목에 대한 교육을 완료하였음
- 양자내성암호의 수학적 배경은 격자, 부호, 다변수함수, 해시함수, 타원곡선동종의 5가지 로 분류되며, 이중 격자와 부호기반 암호가 표준으로 선정될 유력한 후보이므로, 이에 대한 안전성 분석과 구현기법에 대한 교육을 중점적으로 추진함
- 암호시스템의 안전성에 필수적인 난수발생기의 설계, 분석, 평가기술의 체계적인 교육을 진행함
- 상용 보안시스템에 내장된 표준 난수발생기에 대한 증명가능안전성 교육과 함께 통계적 난수성 분석 등을 적용할 수 있는 역량을 갖추도록 함

✓ 참여교수인 최은미, 윤상민 교수는 데이터마이닝, 분산지능화 시스템, 인공지능 기술, 빅데이터 분석 및 적대적 공격 / 방어 시스템 개발기술 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
- 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 적용할 수 있는 역량을 갖추도록 함
- 실제 사회에 활용되는 데이터를 기반으로 한 실습 및 분석을 통하여 학생들 스스로 사회 문제에 이해할 수 있도록 교육함
- 지능형 시스템 환경에서 꾸준히 취합되는 다양한 데이터를 기반으로 문제 해결 능력을 향상함과 동시에 지속적으로 생산되는 데이터에 대한 문제를 분석하는 역량을 교육함

▶ 전임교수 대학원 강의 계획대비 최근 1년간의 실적

■ 공통기초 분야

✓ 김동찬 교수는 암호알고리즘(Cryptographic Algorithm)과목 개설을 통해 고전 암호, Shannon의 이론에 기초한 스트림 암호와 블록 암호의 안전성 이론, 사용방법에 따른 문제점, 설계방법 등을 교육함

■ 기반이론 분야

✓ 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

✓ 강주성 교수는 정보보호프로토콜(Information Security Protocols)과목 개설을 통해 다양한 암호 알고리즘의 역할과 안전성 개념을 정확히 인식하여 키교환 프로토콜, 위탁 프로토콜, 식별 프로토콜, 영지식 프로토콜, 다자간 계산 프로토콜 등의 보안 목적에 부합하는 정보보안프로토콜의 안전성과 효율성 분석에 관해 교육함

■ 핵심역량 분야

✓ 한동국 교수는 부채널공격대응론(Countermeasures of Side Channel Attacks)과목 개설을 통해 부채널공격에 안전한 S/W 및 H/W 기반 대응방법의 설계 및 구현에 대하여 교육함

✓ 염용진 교수는 대칭키암호분석(Tophics in Symmetric Key Cryptanalysis)과목 개설을 통해 블록암호 및 스트림암호 해시함수 등에 대한 안전성 분석을 위한 기본기술과 사용환경에 따라 안전한 알고리즘의 선택, 활용능력을 교육함

✓ 서석충 교수는 암호소프트웨어구현(Implementation of Cryptographic S/W)과목 개설을 통해 국제표준 대칭키 암호 및 공개키 암호의 소프트웨어 구현기술에 대해 교육함

■ 심화응용 분야

✓ 박수현 교수는 비즈니스정보통신과목 개설을 통해 TCP/IP 프로토콜 제품군의 프로토콜 계층을 사용한 네트워크킹 원리에 관해 교육함

✓ 이옥연 교수는 이동통신보안(Mobile Security)과목 개설을 통해 3G, 4G, 5G 등의 이동통신망의 최신 보안 구조 및 그 응용 기술에 대해 교육함

✓ 강주성 교수는 증명가능안전성론(Provable Security)과목 개설을 통해 Pseudo-randomness, 정보이론 관점의 안전성, 계산복잡도 측면의 안전성 등 암호 알고리즘 및 프로토콜에 대한 증명가능 안전성 이론에 관해 교육함

■ 산업·융합 분야

✓ 염용진 교수와 이옥연 교수는 융합보안특강(IT Convergence and Security)과목 개설을 통해 IT와 타 산업의 융합기술과 그 응용에 필요한 보안기술에 대해 교육함

✓ 김동찬 교수는 보안기술표준분석및구현(Analysis and Implementation of Security Technical Standards)은 IETF(Internet Engineering Task Force), 국제표준화기구(ISO), 미 국가표준기술연구원(NIST)에서 발간하는 보안기술과련 표준을 이해하고 구현과 관련한 지식에 대해 교육함

▶ 향후 추진계획

■ 본 교육연구단의 1단계(2020~2021) 기간에서의 목표는 정보보안 교육체계 수립이었음

✓ 따라서, 1단계에서는 교육 목표 및 비전 수립을 위한 다양한 교육과정과 연구가 수행되었으며, 기존 대학원생을 중심으로 정보보안 협동과정의 교과목 및 AI 융합과정 개발이 이루어짐

■ 본 교육연구단의 2단계(2022~2024) 기간에서의 목표는 정보보안 대외협력체계 강화임

✓ 이를 위해 산업계의 전문가를 중심으로 한 정보보안 실무과정 운영과 재학생의 인턴파견 추진을 계획 중임

✓ 또한, 정보보안 기술개발과 커뮤니케이션의 활성화를 위한 보안기술 통합 테스트베드를 구축할 예정임

✓ 연구소, 산업계 전문가와 함께 하는 교육과정 개설 및 산업계의 정보보안 문제 해결을 위한 컨소시엄 구축을 계획하고 있음

■ 본 교육연구단의 3단계(2025~2027) 기간에서의 목표는 CISO급 인재 양성체계 완성임

✓ CISO급 인재 양성을 위해 현장 경력자 전문 위탁 교육을 추진할 계획임

✓ 공공기관 임직원을 위한 경력자 단기 전문교육 프로그램을 운영할 계획임

✓ 이러한 전문교육을 통한 연구개발 성과의 활발한 활용을 위한 지재권확보 및 기술이전을 추진할 계획임

✓ 창업을 통한 산업문제 해결을 지원하기 위해 창업 교육 및 인큐베이터를 운영할 계획임

1.2 과학기술산업·사회 문제 해결과 관련된 교육 프로그램 현황과 구성 및 운영 계획

▶ 과학기술, (지역)산업 또는 (지역)사회 문제 해결에 관련된 교육 프로그램 현황(2020.9.1.~2021.8.31.)

■ 강연

- ✓ 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
- ✓ Code-based Cryptography (2020.11.12.), NSHC
- ✓ Collision Search and its Applications (2021.1.26.), 고려대
- ✓ Code-based Cryptography (2021.7.19.), 한성대

■ 워크숍

- ✓ 제3회 부채널 분석 워크숍(2020.10.29.~2020.10.30.)
- ✓ 부채널 공격 대응이 용이한 경량암호 PIPO 개발 및 응용(2021.05.20.), CPS 보안 워크숍

■ 토론회

- ✓ 수중통신 세계 표준화 (인천국제해양포럼 개최)

▶ 본 교육연구단의 참여교수들은 1차년도 기간 동안 8건의 강연, 2건의 워크숍, 1건의 토론회를 통해 과학기술산업에 기여하였으며, 향후 교육 프로그램 구성 및 과학기술산업·사회 문제해결을 위한 노력과 관심을 지속적으로 가질 예정임

2. 인력양성 계획 및 지원 방안

2.1 최근 1년간 대학원생 인력 확보 및 배출 실적

<표 2-1> 교육연구단 소속 학과(부) 참여대학원생 확보 및 배출 실적 (단위: 명)

대학원생 확보 및 배출 실적					
실적		석사	박사	석·박사 통합	계
확보 (재학생)	2020년 2학기	-	2	-	2
	2021년 1학기	15	3	1	19
	계	15	5	1	21
배출 (졸업생)	2020년 2학기	6	1		7
	2021년 1학기	2	1		3
	계	8	2		10

2.2 교육연구단의 우수 대학원생 확보 및 지원 계획

▶ 우수 대학원생 확보 노력

■ 본 교육단은 1차년도 기간 동안 대학본부의 국고 예산 대비 20% 현금매칭 등의 지원을 하였음

■ 교육연구단에 전담 행정인력을 1명 임용하여 행정인력을 지원하였음

■ 대학원 과목을 학부생이 사전에 이수할 수 있도록 하여 해당 학생이 석사과정이나 박사과정 진학 시 이수학기를 단축할 수 있는 수업 연한 단축 제도를 시행하고 있음

■ 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 동아리를 지속적으로 운영하고 있음

■ 본교 정보보안암호수학과 학생들을 대상으로 한 공모전을 개최하여 대학원에 관한 관심을 높였으며, 이는 향후 대학원에 입학할 경우 수행할 연구에 대한 밑거름 역할을 할 것으로 기대함

■ 학부 우수 졸업 예정자 중에서 학사·석사 연계 과정 입학생을 선발함으로써 본교 출신 우수 학부생이 학부 졸업과 동시에 대학원에 입학해 석사과정을 이수할 수 있도록 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' (연구 조교 A: 수업료의 100 %, 연구조교 B: 수업료의 70 %) 등 다양한 장학금 지원을 통해, 인재 확보, 연구 기회, 교육환경 제공에 기여함

■ 교육연구단의 원활한 연구수행을 위하여 2014년 10월 신축한 산학협력관에 교육연구단장 또는 사업 참여교수의 요청에 따라 현재 산학협력관 203-1호(96㎡), 301호(40㎡), 306호(48㎡)를 연구공간으로 배정하여 지원하고 있음

■ 본교 학사과정에서 대학원 교과목을 6학점 이상 수강하여 소정의 학점을 취득한 석사과 정 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

■ 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 요구하는 과학 인재로 성장할 기회를 제공함

■ 최신 연구정보를 획득하고 국제적 연구 감각을 익힐 수 있도록 창의적이고 도전적인 우수 대학원생을 선발하여, 공동연구 협력을 맺은 해외 연구소 및 대학에 장기연수를 보내고 있음

■ 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

■ 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 지원하고 있음

▶ 교육연구단의 우수 신진연구인력 확보 및 지원

■ 우수 신진연구인력인 박사후 과정생 및 계약교수를 적극적으로 유치하고, 연차에 따라서 2-3명을 단계적으

로 채용하여 산학협력 친화와 사업단의 연구 능력을 함양하고 있음

■ 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 제공하고 있음

2.3 참여대학원생의 취(창)업의 질적 우수성

<표 2-2> 2021.2월 졸업한 교육연구단 소속 학과(부) 참여대학원생 취(창)업률 실적 (단위: 명,%)

구 분		졸업 및 취(창)업현황 (단위: 명, %)						취(창)업률(%) (D/C)×100
		졸업자 (G)	비취업자(B)			취(창)업대상자 (C=G-B)	취(창)업자 (D)	
			진학자		입대자			
			국내	국외				
2021년 2월 졸업자	석사	7	2	-	-	5	4	83.33%
	박사	1			-	1	1	

▶ 오진혁 학생은 다양한 IoT 환경에서의 암호학적 보안 설계 및 기술 개발 연구를 기반으로 펜타시큐리티시스템에 취업하여 정보보안 국책 사업을 수행하고 있음

▶ 박호중 학생은 암호학적 난수발생기의 잡음원 분포와 암호학적 난수발생기의 안전성 평가 방법 연구를 기반으로 KT연구개발센터에 연구원으로 취업하여 암호 분야에 관한 연구를 이어나가고 있음

▶ 성효은 학생은 딥러닝을 활용한 블록암호분석 및 GPU기반 양자내성암호 NTRU 고속구현을 기반으로 근사동형암호 원천기술과 특허를 보유하고 있는 차세대 암호 기술 기업인 크립토랩에 취업하였음

▶ 박한별 학생은 바이오 전자서명 및 인증과 핀테크 보안 시스템 기업인 시큐센에 취업하여 부채널 분석에 안전한 바이오 인증 시스템 설계 업무를 진행하고 있음

▶ 임한섭 학생은 IoT 보안 및 데이터 보안 시스템 기업인 펜타시큐리티에 취업하여 IoT 보안 시스템 설계 업무를 진행하고 있음

3. 참여대학원생 연구실적의 우수성

① 참여대학원생 저명학술지 논문의 우수성

▶ 자체평가 대상 기간 내 국제 저널 16편, 국내 저널 9편 논문 등재의 성과를 냄

▶ 국제저널

■ 참여학생 김예원은 “Accelerated implementation for testing IID assumption of NIST SP 800-90B using GPU” 논문을 통해 기존 1시간 이상 시간이 소요되던 엔트로피 추정 및 검증 프로세스에 대해 GPU를 이용하여 병렬 고속화 방안을 제안함. 제안된 프로그램은 NIST에서 제공하는 프로그램보다 약 3~25배 빠른 성능을 제공하는 것으로 효율적인 난수발생기 분석이 가능함을 제시하시함

■ 참여학생 김일주는 “Single-Trace Attacks on Message Encoding in Lattice-Based KEMs” 논문을 통해 최근 이슈화되고 있는 후양자 암호 중 격자 기반을 대상으로 신규 부채널 공격 기법을 제안함

■ 참여학생 임성혁은 “Improved Differential Fault Attack on LEA by Algebraic Representation of Modular Addition” 논문을 통해 경량 블록 암호 LEA에 대한 신규 오류 주입 공격 기법을 제안함

■ 참여학생 델핀라즈는 수중 VLC 특성을 반영한 수중 VLC 핸드오버 메커니즘의 요구사항과 기본 설계를 수행하고, UHSDM에 하드-핸드오버 메커니즘을 구현함. 다양한 수중환경에서 수행된 하드-핸드오버 시험 결과를 바탕으로 수중에서 이동하는 일반 개체[사람, AUV] 대상의 고속수중통신 핸드오버의 Feasibility를 확인하였으며, 소프트웨어-핸드오버를 설계/구현하기 위한 계획 등을 기술함

■ 참여학생 김기윤은 “Forensic analysis of instant messaging apps: Decrypting Wickr and private text

messaging data", "A study on the decryption methods of telegram X and BBM-Enterprise databases in mobile and PC" 논문들을 통해 암호화된 인스턴트 메신저 데이터베이스를 복호화 하고 사용자 입력 패스워드의 복구방안을 제안함. 이를 통해 디지털 포렌식 수사 관점에서 추가적인 데이터 수집이 가능함을 제시함

- 참여학생 이세훈은 "Magniber v2 Ransomware Decryption: Exploiting the Vulnerability of a Self-Developed Pseudo Random Number Generator" 논문을 통해 악성코드 Magniber 랜섬웨어의 난수 생성기 취약점을 밝혀내고 이를 기반으로 암호화된 데이터의 복호화 방안을 제안함
- 참여학생 김소람은 "Smart Home Forensics—Data Analysis of IoT Devices" 논문을 통해 스마트 홈 디바이스의 데이터를 분석하고 이를 기반으로 디지털 포렌식 수사에 활용 가능한 데이터를 제시함
- 참여학생 송진교는 "Efficient Implementation of a Crypto Library Using Web Assembly" 논문을 통해 웹 환경에서 사용되는 WebAssembly를 통해 다양한 암호 알고리즘(CHAM, HMAC, ECDH)을 최적 설계를 제안함. 이를 통해 기존 JavaScript 보다 더 빠른 속도를 제공하는 웹 환경 암호 라이브러리를 제시함
- 참여학생 안상우는 "Efficient Implementation of ARX-based Block Ciphers on 8-bit AVR Microcontrollers" 논문을 통해 Low-end Processor로 널리 활용되는 8-bit AVR 환경에서 ARX기반 블록암호(LEA, HIGHT, CHAM)의 CTR 모드를 최적화함.
- 참여학생 안상우는 "Parallel Implementations of ARX-based Block Ciphers on Graphic Processing Units" 논문을 통해 GPU 환경에서 ARX기반 블록암호 (LEA, HIGHT, CHAM)의 최적화 구현을 제안함. GPU는 IoT 환경에서 서버로 널리 활용되고 있으므로, 본 논문의 기술은 향후 GPU 환경에서 블록암호의 최적화 구현 기반을 제공할 것으로 기대됨
- 참여학생 안상우는 "Efficient Parallel Implementations of LWE-based Post-Quantum Cryptosystems on Graphics Processing Units" 논문을 통해 GPU 환경에서 격자기반 양자내성암호를 최적화를 수행하였음. 격자기반 암호는 NIST PQC Round 3의 대부분의 후보자이기 때문에, 본 연구결과는 미래 환경인 양자컴퓨팅 환경에서 GPU를 통한 다양한 격자기반 암호의 최적화에 기여할 것으로 기대됨
- 참여학생 송진교는 "Secure and Fast Implementation of ARX-Based Block Ciphers Using ASIMD Instructions in ARMv8 Platforms" 논문을 통해 ARMv8 환경에서 경량암호 (Revised CHAM, HIGHT)에 대한 최적화 및 오류공격 대응 구현을 제안함. ASIMD 명령어를 활용하여 Revised CHAM, HIGHT 암호에 대해 ARMv8 환경에서 다수의 암호화를 동시에 처리하는 병렬 구현과 이전 오류공격 대응 방안에 대해 더욱 최적 설계된 대응 구현 방안을 제시함
- 참여학생 안상우는 "Designing a CHAM Block Cipher on Low-End Microcontrollers for Internet of Things" 논문을 통해 경량암호 CHAM을 Low-End Processor에서 널리 활용되는 8-bit AVR 환경에서 최적 구현 방안을 제안 하였으며 CHAM-CTR모드에 대한 최적화 방안을 제안하였음
- 참여학생 박보선은 "Efficient Implementation of NIST LWC ESTATE Algorithm using OpenCL and Web Assembly for Secure Communication in Edge Computing Environment" 논문을 통해 웹 환경에서 OpenCL을 활용하여 대량의 데이터를 암호화 하는 방안을 제안함.
- 참여학생 송진교는 "Efficient Parallel Implementation of CTR mode of ARX-based Block ciphers on ARMv8 Microcontrollers" 논문을 통해 ARMv8 환경에서 경량암호의 CTR모드 최적화 구현방안을 제안하였음. 본 결과는 ARMv8 환경에서 경량암호의 CTR모드 최적화에 대한 첫 연구임
- 참여학생 김영범은 "Chaining optimization methodology a new sha-3 implementation on low-end microcontrollers" 논문을 통해 AVR 환경에서 SHA-3의 최적화를 수행하였으며 가장 빠른 SHA-3 성능을 달성 하였음. 현재 모든 PQC 알고리즘이 SHA-3를 사용하므로 본 연구결과는 앞으로 활발하게 사용될 것으로 기대됨

▶ 국내저널

- 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
- 참여학생 권수진은 “블록암호 DES의 신경망 기반 평문 복구 공격에 대한 재고찰” 논문을 통해 2012년에 제안된 신경망 기반 DES 복구가 실제로는 어렵다는 사실을 제시함. 동일한 조건에서 공격을 재연하고 결과를 비교함으로써 기존 논문의 해석이 과도하게 낙관적으로 작성되었음을 밝혔으며 암호키 없이 암호문만으로 DES의 평문 복구는 어려움을 제시함
- 참여학생 허욱은 “OBD 스캐너 애플리케이션 INFOCAR 데이터 분석을 통한 차량 포렌식 기법” 논문을 통해 차량 제어 시스템의 데이터 획득 방안을 제시함 애플리케이션의 문의하기 기능에서 추출되는 로그 정보를 활용하여 루트 영역에 존재하는 데이터를 획득하고, 이를 통해 차량 제어 시스템의 정보를 획득하여 디지털 포렌식 수사 관점에서 유용한 데이터를 제안함
- 참여학생 안상우는 “CHES 2020을 중심으로 살펴본 SW/HW 암호 분석 및 구현기술 연구 동향” 논문을 통해 세계적으로 저명한 학회인 CHES 2020에서의 암호 분석 및 구현기술 동향을 분석 하고 향후 연구 전망을 제시함
- 참여학생 송진교는 “GPU를 활용한 고속 소프트웨어 암호모듈 설계 및 구현” 논문을 통해 국내 S/W기반 암호 모듈의 대용량 데이터의 처리에 대한 한계점을 이야기하고 해결방안을 제시함. GPU를 활용한 고속화된 S/W 암호모듈을 제시하고 GPU를 추가적으로 활용함에 따라 발생하는 KCMVP의 보안요구사항의 변동점과 만족사항을 제시함
- 참여학생 송진교는 “NIST PQC Round 3 격자 기반 암호의 부채널 대응 기법 동향 분석” 논문을 통해 NIST PQC Round 3 후보자들의 부채널 공격 및 대응방안에 관한 최신 연구 동향을 정리함. 이를 통해 양자컴퓨팅 환경에 안전한 PQC 일지라도 여전히 부채널 취약점이 존재함을 밝혔으며 따라서 부채널 대응방안 적용이 필요함을 밝힘
- 참여학생 송진교는 “ARM/NEON 프로세서를 활용한 NIST PQC SABER에서 Toom-Cook 알고리즘 최적화 구현 연구” 논문을 통해 ARMv8 환경에서 NIST PQC SABER의 핵심연산인 Toom-Cook 알고리즘의 최적화 구현 방안을 제시함. 평가, 보간에서 모두 ARMv8 환경에 최적화된 설계방안을 제안하였으며, ARM/NEON 코어를 동시에 활용하는 Interleaving 구현 방안을 제시함
- 참여학생 김영범은 “32-bit RISC-V 프로세서에서 국산 블록암호 성능 벤치마킹” 논문을 통해 RISC-V환경에서의 국산 블록암호를 구현하고 성능 벤치마킹 결과를 최초로 제공함

▶ 본 교육 연구단은 상기 내용과 같이 국제 저널 16편, 국내 저널 9편의 논문 등재 실적을 달성하였음. 향후에도 적극적이고 다양한 지원을 통해 우수 인력양성 및 역량 향상에 도움을 줄 예정임

② 참여대학원생 학술대회 대표실적의 우수성

▶ 자체평가 대상 기간 내 국제 학회 10편, 국내 학회 26편의 논문 발표의 성과를 냄

▶ 국제 학회

- 참여학생 권수진은 “Analysis of public-key cryptography using a 3-regular graph with a perfect dominating set” 논문을 통해 NP-complete 문제에 의존하는 Perfect dominating set을 가지는 3-regular 그

래프를 이용한 공개키 암호학 개념의 보안 및 성능 분석을 수행함. 보안 매개변수의 실제 범위를 제안하여 Perfect dominating set을 가진 그래프 기반 공개키 암호를 화이트박스 암호화 인코딩 기법으로 사용할 수 있는 방향성을 제시하였으며, 결과 Best Paper에 선정됨

■ 참여학생 임형신은 “An Efficient Structural Analysis of SAS and its Application to White-Box Cryptography” 논문을 통해 서로 다른 크기를 가지는 비선형 함수 S(substitution)와 큰 입출력 크기를 가지는 경우에 대해서 아핀 함수 A(affine)와 결합된 S_1AS_2 구조에 대해 구조 분석 방법을 제시함

■ 참여학생 임한섭은 2020 ACM International Conference on Intelligent Computing and Its Emerging Applications 국제 학술대회에 ‘Fault Injection Method for Hardware-implemented AES without Artificial Triggering’ 논문을 발표함. 본 논문에서는 인위적인 트리거가 없는 환경에서 하드웨어로 구현된 AES를 대상으로 오류 주입 공격을 수행함

■ 참여학생 김일주는 2020 ACM International Conference on Intelligent Computing and Its Emerging Applications 국제 학술대회에 ‘Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-based Profiling’ 논문을 발표함. 본 논문에서는 NIST의 후양자 암호 공모의 3라운드 후보인 Dilithium을 대상으로 머신러닝을 활용한 부채널 공격 기법을 제안함

■ 참여학생 박한별은 2020 ACM International Conference on Intelligent Computing and Its Emerging Applications 국제 학술대회에 ‘Machine Learning-Based Profiling Attack Method in RSA Prime Multiplication’ 논문을 발표함. 본 논문에서는 공개키 암호 알고리즘 RSA를 대상으로 머신러닝 기반의 부채널 공격 기법을 제안함

■ 참여학생 염선호는 극한지 센서네트워크 기반 분석 연구의 효율을 높이기 위한 ‘극한지 센서데이터 원격회수 시스템’과 ‘극한지 빅데이터 구축’의 개념과 공통요구사항을 제안한 논문을 국제학술대회에서 발표함

■ 참여학생 김한기는 ICISC 2020에서 “PIPO: A Lightweight Block Cipher with Efficient Higher-Order Masking Software Implementations” 논문을 발표함. 본 논문에서는 부채널 마스킹을 적용한 환경 및 적용하지 않은 환경 모두에서 효율적인 블록암호를 제안함

■ 참여학생 김영범은 World Conference on Information Security Applications (WISA 2021) 국제 학술대회에서 “Parallel Implementation of PIPO Block Cipher on 32-bit RISC-V Processor” 논문을 발표함. 일반적으로 병렬 유닛을 제공하지 않는 RISC-V에서는 오버플로가 발생할 수 있는 연산들에 대해서는 병렬 구현이 쉽지 않음. 본 논문에서는 이러한 32-bit RISC-V 프로세서에서 PIPO 블록암호의 병렬 구현 방안을 제시함

■ 참여학생 송진교 학생은 World Conference on Information Security Applications (WISA 2021) 국제 학술대회에서 “High-Speed Software of Karatsuba Muliplication for SABER Round 3 on ARMv8-A Series” 논문을 발표함. 본 논문은 ARMv8-A 환경에서 SABER Round 3의 핵심 연산인 Karatsuba 곱셈에 대한 최적 구현 방안을 제안하였으며 결과 ARMv8-A Series 환경에서 SABER Round 3의 빠른 처리가 가능함을 제시함

■ 참여학생 안상우는 World Conference on Information Security Applications (WISA 2021) 국제 학술대회에서 “XTS-AES Parallel Optimization Implementation Technique for Fast FDE” 논문을 발표하였음. 본 논문은 FDE (Full Disk Encryption)에서 대표적으로 사용되는 XTS-AES 방식을 GPU환경에 효율적인 구현 방안을 제안하였음. 그리고 이 결과가 SIMD, NEON 병렬환경에 쉽게 확장하여 사용 가능함을 제시함

▶ 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

- 참여학생 정서우는 “Lua 스크립트 기반 5G AKA wireshark 플러그인 제작” 논문을 통해 5G AKA 데이터 분석을 용이하게 하기 위해 Lua 스크립트를 기반으로 널리 사용되고 있는 분석 도구인 wireshark 상에서의 5G AKA 플러그인을 제작하고, 그에 따른 과정 및 결과를 제시함. 표준에서 요구하는 데이터 형식에 맞춰 정형화된 플러그인을 사용한다면, 다양한 언어로 구현된 플랫폼 혹은 다양한 장비에서 프로토콜을 분석할 때 데이터를 따로 분류하는 과정을 생략할 수 있어 분석 시간을 줄일 수 있고, 보다 용이하게 분석할 수 있음을 제시함
- 참여학생 한주홍은 “모의 공격을 통한 MAVLink 프로토콜 취약점 분석” 논문을 통해 드론 환경에서 주로 사용되는 MAVLink 프로토콜의 버전별 데이터 보안 취약점을 분석하고 그에 대한 모의 공격을 수행해 분석한 취약점들에 대해 증명함. 이를 통해 드론 환경에서 요구되는 보안 기능들에 대해 정리하였으며, 해당 연구 내용은 향후 안전한 드론 통신 프로토콜 제작 시 기초가 될 것으로 기대됨
- 참여학생 정서우는 “CSFC 내 MSC 솔루션 보안 요구사항 비교분석” 논문을 통해 CSFC 프로그램 내 MSC(Multi-Site Connectivity) 솔루션의 보안 요구사항을 분석하고, 이를 통해 정보보호 제품을 포함한 솔루션 도입 시 전반에서 확인해야 할 요구사항을 통해 국내 보안적합성 검증제도의 추가적인 보안 요구사항을 제안함
- 참여학생 이세윤은 “UAS 보안인증 시험을 위한 보안 요구사항” 논문을 통해 UAS 보안인증 시험의 필요성과 UAS 보안인증 시험 내 시험 항목과 보안 요구사항을 제시함. UAS 보안인증 시험이 도입될 경우, 드론 보안 사고를 사전에 방지할 수 있는 초석이 될 것으로 기대됨
- 참여학생 김태완은 “클라우드 컴퓨팅 서비스 보안 인증제도 개선사항” 논문을 통해 클라우드 컴퓨팅에 도입될 동형암호에 대해 분석하고, 현재 클라우드 컴퓨팅 보안 인증제도에 동형암호에 대한 보안 통제 항목을 포함시켜 클라우드 컴퓨팅 발전을 위한 방법을 제시함
- 참여학생 전창열은 “이진 Goppa 부호 구현에 관한 연구” 논문을 통해 SAGE 프로그램을 이용한 Goppa 부호의 생성, 인코딩, 디코딩과정의 구현을 제시함. 이후 Classic McEliece에서 제안한 파라미터를 이용하여 각 연산 시간을 측정하고, 연산 시간에 영향을 주는 파라미터를 분석함
- 참여학생 황아리는 VL, IR 기반 수중통신에서 버블이 통신 감쇄에 미치는 영향을 분석하는 시뮬레이션을 수행함
- 참여학생 신수민은 “디지털 포렌식 관점에서 협업 및 화상회의 애플리케이션 분석” 논문을 통해 협업 및 화상회의 애플리케이션을 분석 및 발표하였다. 코로나19 시대에 사용량이 증가하고 있는 협업 및 화상회의 애플리케이션을 분석하고, 디지털 포렌식 관점에서 유용한 데이터를 식별함
- 참여학생 최용철은 “사진 및 동영상/은닉 암호화 특정 애플리케이션 분석” 논문을 통해 데이터를 은닉 및 암호화 하는 안티포렌식 애플리케이션을 분석하고, 데이터 암호화 취약점을 발표함. 이를 통해 특정 애플리케이션을 통해 은닉 및 암호화된 데이터를 디지털 포렌식 수사관점에서 사용방법을 제안함
- 참여학생 박종현은 “확장된 RNBP 알고리즘” 논문을 통해 기존에 제시된 RNBP 알고리즘의 성능 향상 방안을 제안하였음. 해당 결과를 통해 기존에 알려진 Pyjamask의 MDS코드 최적화 구현을 더욱 최적화함
- 참여학생 안상우는 2020 정보보호학회 동계학술대회에서 “GPU 환경에서의 효율적인 Number Theoretic Transform 최적화 구현” 논문을 통해 GPU의 Threads를 효율적으로 스케줄링하여 격자기반 암호의 핵심연산인 NTT 곱셈에 대한 최적화 방안을 제안함
- 참여학생 송진교는 2020 정보보호학회 동계학술대회에서 “NEON을 활용한 NIST 양자암호 Saber에서 다항식 곱셈기반 Toom-Cook 알고리즘 최적화 연구” 논문을 통해 NEON 엔진을 활용하여 연산 부하가 큰 Toom-Cook 알고리즘의 최적화 방안을 제안함
- 참여학생 송진교는 2020 정보보호학회 동계학술대회에서 “RISC-V 환경에서 Curve25519의 Reduction 연산

최적화 연구” 논문을 통해 RISC-V 환경에서 Curve25519의 Reduction 연산을 최적화 하기 위해 효율적으로 Carry를 핸들링하는 방안을 제안함

- ■ 참여학생 송진교는 2020년 정보보호학회 동계학술대회에서 “ARM Cortex-M4 환경에서 SIMD 명령어를 이용한 CHAM-64/128 최적화 연구” 논문을 통해 ARM Cortex-M4 환경에서 지원하는 SIMD 명령어를 활용하여 2개의 CHAM 암호화를 동시에 수행하는 병렬 구현 방안을 제안함
- ■ 참여학생 안상우는 2021 한국컴퓨터종합학술대회에서 “격자기반 양자내성암호에서 RST를 이용한 기각 샘플링 병렬 최적화” 논문을 통해 양자내성암호에서 샘플링 수행 시 많이 사용되는 Rejection Sampling 방안을 최적화하였으며, GPU 환경에서의 최적화 구현방안을 제안함
- ■ 참여학생 송진교는 2021 한국컴퓨터종합학술대회에서 “타원곡선 암호의 최적화 구현, 부채널 대응기법 동향 분석 및 벤치마킹” 논문을 통해 타원곡선 암호의 최적화 구현 및 부채널 대응 기법에 대한 최신 동향 분석을 제공하였으며, 최적화 관점에서는 wNAF, Comb, 부채널 대응기법 관점에서는 DPA, SPA 관점으로 최신 동향 및 구현 방안을 제안함
- ■ 참여학생 최호진은 2021 한국컴퓨터종합학술대회에서 “GPU 환경에서의 NIST PQC 3-round Lattice 및 Symmetric 기반 전자서명 최적화 구현 동향” 논문을 통해 NIST PQC Round 3 격자기반 암호의 GPU 환경에서 최신 구현 동향 분석한 결과를 제시함
- ■ 참여학생 김영범은 2021 한국컴퓨터종합학술대회에서 “Metamorphic Testing기반 암호알고리즘 구현 정확성 검증 기술 동향 분석” 논문을 통해 기존 CAVP 검증방법의 한계점을 대체할 수 있는 Metamorphic Testing 기법에 대한 연구가 최근 활발히 진행되고을 통해 최신 연구 동향을 제시함
- ■ 참여학생 박보선은 2021 한국컴퓨터종합학술대회에서 “Web Assembly를 이용한 국산 블록 암호 알고리즘 벤치마킹” 논문을 통해 웹 환경에서 JavaScript보다 빠른 속도를 제공하는 Web Assembly를 활용하여 국산 블록 암호 알고리즘 (ARIA, LEA, HIGHT)에 대한 벤치마킹 결과를 제시함
- ■ 참여학생 안상우는 2021 정보보호학회 하계학술대회에서 “중간값 참조 테이블을 활용한 CPU-GPU 하이브리드 AES-XTS 최적화 기법” 논문을 통해 CPU-GPU를 동시에 활용하여 AES-XTS에 대해 중간값 테이블을 활용한 최적화 방안을 제안함
- ■ 참여학생 송진교는 2021 정보보호학회 하계학술대회에서 “ARMv8-A Series에서 Crystal-Dilithium Round 3의 NTT 곱셈 병렬 구현” 논문을 통해 ARMv8-A Series 환경에서 Crystals-Dilithium의 핵심 연산인 NTT 곱셈에 대해 NEON 엔진을 활용한 병렬 구현 방안을 제안함
- ■ 참여학생 최호진은 2021 정보보호학회 하계학술대회에서 “GPU 환경에서 SHA-3(512) 병렬 최적 구현” 논문을 통해 GPU 환경에서 효율적인 Threads 스케쥴링을 통한 SHA-3(512)에 대한 최적화 구현 방안을 제안함
- ■ 참여학생 김영범은 2021 정보보호학회 하계학술대회에서 “8-bit AVR 환경에서 PIPO 최적 구현” 논문을 통해 메모리 접근 시간을 최소화할 수 있는 PIPO 최적 구현 방안을 제안함
- ■ 참여학생 박보선은 2021 정보보호학회 하계학술대회에서 “OpenCL, OpenMP 병렬처리를 사용한 PIPO 알고리즘 구현” 논문을 통해 최대 다수의 암호화를 동시에 처리할 수 있도록 OpenCL, OpenMP에 최적화된 PIPO 알고리즘의 병렬 구현 방안을 제안함

▶ 본 교육 연구단은 상기 내용과 같이 국제 학회 10편, 국내 학회 26편의 논문 발표 실적을 달성하였음. 향후에도 적극적이고 다양한 지원을 통해 우수 인력양성 및 역량 향상에 도움을 줄 예정임

③ 참여대학원생 특허, 기술이전, 창업 실적의 우수성

▶ 특허

■ 비행체에서의 잡음원 도출 장치 및 방법

✓ 난수 생성 기능은 암호기능에서 가장 핵심적인 기능이며 entropy가 충분한 잡음원을 바탕으로 생성되어야 함. 하지만, 드론과 같은 비행체는 임베디드 장비를 활용해 구성되며, 이러한 환경에서는 잡음원 수집에 어려움이 존재함. 본 특허에서는 해당 환경에서의 원활한 잡음원 수집 방법에 대한 방법에 관해 기술함

■ 5G SIDF 암호처리장치 및 그 방법

✓ 5G 시스템에서는 새롭게 SUPI와 SUCI를 새롭게 도입하였으며, 5G 홈 네트워크에서는 암호화된 SUCI의 복호화를 SIDF를 통해 수행됨. 해당 특허는 이러한 SIDF에서 5G 시스템에서 목표하고 있는 단말 수를 커버하면서도 가용성을 보장할 방법에 관해 기술함

■ 독립성 측정을 이용한 엔트로피 관리 장치 및 방법, 이를 이용한 난수 생성 장치

✓ 난수발생기의 엔트로피 풀 관리 방법은 구현 환경에 따라 설계되었거나 모듈러(modulo) 연산 등을 이용하여 편향성을 제거하는 방식으로 설계되어야함. 안전한 시드를 생성하기 위해서 독립성과 편향성을 조정할 수 있는 엔트로피 풀 관리 장치가 필요함. 본 특허 에서는 독립성 지표를 이용하여 편향성과 독립성 정도를 동시에 관리할 수 있는 난수발생기 발명에 관해 기술함

■ NTRU LPRime 암호에 대한 부채널 분석 장치 및 방법

✓ 후양자 암호 알고리즘 NTRU LPRime에 대한 신규 부채널 기법을 기술함

■ 종단간 암호화가 적용된 파일에 대한 복호화 장치 및 방법

✓ 종단간 암호화가 적용된 파일은 중간 서버에 존재하는 데이터만으로는 평문의 획득이 불가능함. 따라서 단말 사이에 존재하는 주요 키가 필요하며, 본 특허에서는 특정 애플리케이션의 단말단의 정보 수집을 통해 종단간 암호화가 적용된 데이터를 복호화 하는 방법에 관해 기술함

▶ 기술이전

■ 양자난수 기반 UAV용 LTE 암호장비 개발 기술

✓ 양자엔트로피 및 DRBG를 활용하는 양자난수를 적용하여 드론 등의 UAV의 안전한 데이터 전송이 가능한 통신 및 암호장비 개발을 위한 기술임

■ KMULIB v2.1 Windows용 KCMVP 검증필암호모듈

✓ Windows 환경을 위한 KMULiB v2.1 검증필암호모듈이며, 해당 기업에 암호모듈과 함께, 활용방법을 이전하였음

■ 하이브리드 수중무선통신 장치 및 그 통신 방법

✓ 다중매체 채널을 통해 다양한 운영 조건의 수중통신 요구사항을 충족하는 기술임

▶ 본 교육 연구단은 상기 내용과 같이 특허 5건, 기술이전 1건의 실적을 달성 할 수 있도록 지원하였음. 향후에도 적극적이고 다양한 지원을 통해 우수 인력양성 및 역량 향상에 도움을 줄 예정임

4. 신진연구인력 현황 및 실적

▶ 연구교수 윤승환의 연구 활동

- ■ 암호모듈 및 보안제품의 평가/인증 방법론에 관한 연구
- ■ 양자난수발생기 기반 6G 이동통신 보안 플랫폼에 관한 연구
- ■ 무선 통신 환경에서 기기와 망 사이의 상호 인증을 위한 경량화된 기기 식별과 인증 및 키 일치에 관한 연구
  - ✓ IoT 환경에서 저사양 기기를 사용하는 보안 서비스를 위하여 기기-망 구간의 경량화된 기기 식별과 인증 및 키 일치 기술을 적용하는 방법에 대한 강연 및 실습 자문
- ■ 산업제어시스템에서 암호의 이해와 활용 현황(2021.4.6.), 경기과학고등학교
  - ✓ 산업시스템에 암호 기술을 적용하기 위한 연구내용 및 활용 현황에 대한 강연
- ■ FPGA를 활용한 스트림 암호 구현(2021.07.19.), 국민대학교
  - ✓ 양자난수 발생기에서 발생한 엔트로피와 FPGA를 활용한 스트림암호 모듈 개발 방법에 대한 강연 및 실습 자문

▶ 연구교수 이재훈은 이동통신 및 IoT 기술을 활용한 융합보안과 국가기반시설 및 공공기관 보안 기술, 양자암호 기술 융합 및 양자난수를 활용한 응용 서비스 연구를 수행하고 있음

5. 참여교수의 교육역량 대표실적

▶ 인재 양성을 위한 노력

- ■ 동계 방학 학부생 인턴십을 통해 학부생이 프로젝트를 경험할 수 있는 기회 제공. 이를 통해 암호 분야에 대한 관심을 가질 수 있도록 노력 하였으며, 결과 2021년 대학원에 진학하여 전문성을 가진 인재가 될 수 있도록 하였음
- ■ 코로나19로 다양한 학부 행사가 취소되는 도중 학문적 흥미를 잃지 않도록 동아리 차원의 암호분석 공모전을 개최하도록 도와주었으며, 결과 1~4학년의 다양한 학부생들이 흥미롭게 공모전에 참여할 수 있게 하였음.
- ■ 교과과정 개편을 통해 안전한 초 연결사회를 위한 문제해결을 위한 강의를 개설, 기존 강의를 개선하였음. ‘정보보호프로토콜’과 ‘증명가능안전성론’ 등 다양한 교육 내용으로 강의노트를 개선하며 문제해결형 정보보안 교육연구단의 비전과 목표에 적합한 교육을 추가하였음
- ■ ‘보안구현개발방법론’, ‘암호소프트웨어구현’ 등 다양한 교육을 개선함으로서 KCMVP에대한 이해를 끌어내고 다양한 플랫폼에서의 최적화 구현을 통해 암호 알고리즘의 고속 구현의 필요성과 설계 기술에 대한 지식을 심어줄 수 있도록 하였음
- ■ 대학원 수준의 수업을 체험해볼 수 있는 다양한 교내 동아리 (부채널 분석, 난수성 분석, 디지털 포렌식 등)을 지속적으로 운영함으로써 인재 양성에 힘쓰고 있음
- ■ 이론 교육의 이해도 향상을 위해 기존 선 이론, 후 실습 교육을 대체하는 선 실습, 후 이론 수업을 개설하였음. 4학년~대학원 수업에 1학년들이 참여할 기회를 제공하고 멘토-멘티를 활용하여 실습 수업을 따라갈 수 있게 보조 하고 있음. 이 수업을 통해 향후 이론 수업이 어떠한 곳에 활용되는지를 명확히 하고 있으며, 더 나은 이론 수업 이해도를 제공 할 것으로 기대됨
- ■ 수중에서 고성능 수중통신 기술을 실현하기 위한 핵심 요소기술 ‘UHSDM, S-DTN(Seamless Delay Tolerant Network), 채널 모델, 채널 선택 메커니즘, 핸드오버 메커니즘’의 기술 개발 및 논문지도를 위한 교육 일정을 수립, 갈야니(수료), 델핀라즈(수료), 염선호, 황아리 연구원의 연구력 향상을 위한 세미나, 외부 도메인 전문가를 초빙 등을 진행 하였음
- ■ UHSDM(S-DTN 탑재) 시작품 2건 제작, 국내학술대회 논문 3건 발표, 국제학술대회 논문 1건 발표하였음

▶ 강연

- 5G+ 6G를 향한 양자보안과 KCMVP 암호 발전 동향(2021.05.17.), 한양대
  - ✓ 5G 및 6G 이동통신망과 양자보안의 발전 동향에 대한 강연
- 5G+ 기반 CPS를 위한 KCMVP 암호와 Quantum 암호의 도입 전략(2021.05.21.), CPS 보안 워크숍
  - ✓ 5G 이동통신망 기반의 CPS 환경을 위한 양자암호의 도입을 위한 전략에 대한 강연
- QRNG 기반 암호모듈 활용 방안(2021.07.21.), 국가보안기술연구소
  - ✓ 양자난수발생기 연구내용 및 KCMVP 검증을 위한 시험방안에 대한 강연
- 드론에서의 경량 암호(2021.07.29.), 세종대
  - ✓ 드론 환경을 위한 DIM 등의 식별모듈과 양자암호의 연구 동향에 대한 강연
- IoT 보안 디바이스 개발 고려 사항 및 기술 소개(2021.08.16.), 한양대
  - ✓ IoT 암호 및 정보보안을 위한 양자암호의 발전 동향에 대한 강연
- Code-based Cryptography (2020.11.12.), NSHC
  - ✓ 부호기반 암호의 동향과 안전성 분석 방법인 정보집합디코딩에 대한 강연
- Collision Search and its Applications (2021.1.26.), 고려대
  - ✓ 충돌쌍을 찾는 방법과 충돌쌍의 활용에 대한 강연

▶ Code-based Cryptography (2021.7.19.), 한성대

- ✓ 부호기반 암호의 동향과 McEliece 암호에 대한 강연

▶ 워크숍

- 제3회 부채널 분석 워크숍(2020.10.29.~2020.10.30.)
- 부채널 분석 워크숍을 주관하여 개최함
- 부채널 공격 대응이 용이한 경량암호 PIPO 개발 및 응용(2021.05.20.), CPS 보안 워크숍
- 부채널 공격 대응기법 설계가 용이한 경량암호 PIPO 개발에 대한 강연

6. 교육의 국제화 전략

① 교육 프로그램의 국제화 현황 및 계획

▶ 본 교육연구단은 국제적 경쟁력을 갖춘 정보보안 전문인력 양성을 위해 국제학회 참석 및 논문 발표를 독려하고 있음

- 해당 기간 국제 저널 23건, 국제 학회 11건의 논문을 발표하였음
- 해당 기간 국제 특허 등록 1건을 완료하였음
- 이옥연 교수팀은 ㈜이와이엘, 플로리다 주립대학교 FICS와 국제 공동연구를 수행하였음
- 이옥연 교수팀의 참여학생 장찬국, 위한샘, 김현기는 국내 2개 대학(국민대학교, 순천향대학교), 해외 1개 대학(Georgia State University)의 2개 연구실로 총 3개 대학이 참여하는 국제 공동연구를 수행하고 있음

② 참여대학원생 국제공동연구 현황과 계획

▶ 이옥연 교수팀의 참여학생 장찬국, 위한샘, 김현기는 글로벌 고급 인재 양성을 목표로 하는 국제 공동연구 '5G와 클라우드 융합환경에서의 안전한 UTM 서비스를 위한 보안기술 연구 및 인력 양성' 을 수행함

▶ 본 공동연구는 국내 2개 대학(국민대학교, 순천향대학교), 해외 1개 대학(Georgia State University)의 2개 연구실로 총 3개 대학이 참여함

▶ 참여학생 장찬국, 위한샘, 김현기는 21년 8월 1일부터 22년 4월 30일까지 미국 Georgia State University에서 협업을 위한 파견 근무를 수행 중임

▶ 본 연구의 결과물은 관련 해외 학술대회와 논문지에 투고할 것이며 연구 중 발생한 다양한 연구결과는 연구종료 후에도 참여 기관과 지속해서 공유하고 차후 관련 분야에 진출하는 국내 연구진 혹은 기업에 공개하여 국내 기술력 향상에 이바지할 것으로 보임

▶ 본 공동연구는 파견인력에 대한 지원만이 아니라 국내에 체류하는 미파견인력에 대한 지원 및 연구 프로세스의 최적화 및 각 기관의 유기적인 협업을 수행할 수 있도록 설계됨

▶ 귀국 후 미파견 참여연구원들에게 파견 기간 중 습득한 해외 연구 경험을 공유하여 미파견연구원들에 대한 간접 경험을 통해 다양한 상승효과를 기대할 수 있음

Ⅲ 연구역량 영역

□ 연구역량 대표 우수성과 (자체평가 대상 기간 2020.9.1.~2021.8.31.)

▶ 자체평가 대상 기간 내 국제 저널 23편, 국내 저널 17편, 국제 학회 8편, 국내 학회 39편의 논문 발표, 수상 11건, 특허 13건, 연구비 수주 56건 등의 성과를 냄

▶ 국제 저널

- "Privacy Preservation in Edge Consumer Electronics by Combining Anomaly Detection with Dynamic Attribute-Based Re-Encryption", Eunmok Yang, Velmurugan Subbiah Parvathy, P.pandi Selvi, K.shankar, Changho Seo;Gyanendra Prasad Joshi, Okyeon Yi, MDPI Mathematics (SCIE, IF=1.747)
- "A methodology for the decryption of encrypted smartphone backup data on android platform: A case study on the latest samsung smartphone backup system", Myungseo Park, Okyeon Yi, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, IF=1.660)
- "Single-Trace Attacks on Message Encoding in Lattice-Based KEMs", Bo-Yeon Sim, Jihoon Kwon, Joohee Lee, Il-Ju Kim, Tae-Ho Lee, Jaeseung Han, Hyojin Yoon, Jihoon Cho, Dong-Guk Han, IEEE Access (SCIE, IF-3.367)
- "Improved Differential Fault Attack on LEA by Algebraic Representation of Modular Addition", Seonghyuck Lim, Jonghyeok Lee, Dong-Guk Han, IEEE Access((SCIE, IF-3.367)
- "Efficient Implementation of a Crypto Library Using Web Assembly", Bosun Park, JinGyo Song, Seog Chung Seo (Corresponding), MDPI Electronics (SCIE, IF=2.412)
- "Efficient Implementation of ARX-based Block Ciphers on 8-bit AVR Microcontrollers", YoungBeom Kim, Hyeokdong Kwon, SangWoo An, Hwajeong Seo, Seog Chung Seo(Corresponding), MDPI Mathematics (SCIE, IF=1.747)
- "Parallel Implementations of ARX-based Block Ciphers on Graphic Processing Units", SangWoo An, YoungBeom Kim, Hyeokdong Kwon, Hwajeong Seo, Seog Chung Seo(Corresponding), MDPI Mathematics (SCIE, IF=1.747)
- "Faster Data Forwarding in Content-Centric Network via Overlaid Packet Authentication Architecture", Taek-Young Youn, Joongheon Kim, David Mohaisen, and SeogChung Seo(Corresponding), MDPI

Sustainability (SSCI, IF= 2.798)

- “Efficient Parallel Implementations of LWE-based Post-Quantum Cryptosystems on Graphics Processing Units”, SangWoo An, Seog Chung Seo(Corresponding), MDPI Mathematics (SCIE, IF=1.747)
- “Secure and Fast Implementation of ARX-Based Block Ciphers Using ASIMD Instructions in ARMv8 Platforms“, JinGyo Song, Seo Chung Seo(Corresponding), IEEE ACCESS (SCIE, IF=3.745)
- “Designing a CHAM Block Cipher on Low-End Microcontrollers for Internet of Things“, Hyeokdong Kwon, SangWoo An, YoungBeom Kim, Hyunji Kim, Seung Ju Choi, Kyoungbae Jang, Jaehoon Park, Hyunjun Kim, Seog Chung Seo, Hwajeong Seo, MDPI Electronics (SCIE, IF=2.412)
- “High-Speed Implementation of PRESENT on AVR Microcontroller “, Hyeokdong Kwon, YoungBeom Kim, Seog Chung Seo, Hwajeong Seo, MDPI Mathematics (SCIE, IF=1.747)
- “Efficient Implementation of AES and CTR_DRBG on 8-bit AVR-based Sensor Nodes“ by YoungBeom Kim and Seog Chung Seo (Corresponding), IEEE ACCESS (SCIE, IF=3.745)
- “Efficient Implementation of NIST LWC ESTATE Algorithm using OpenCL and Web Assembly for Secure Communication in Edge Computing Environment“, BoSun Park and Seog Chung Seo(Corresponding), MDPI Sensors (SCIE, IF=3.275)
- “Efficient Parallel Implementation of CTR mode of ARX-based Block ciphers on ARMv8 Microcontrollers“, JinGyo Song and Seog Chung Seo(Corresponding), MDPI Applied Sciences (SCIE, IF=2.474)
- “Chaining optimization methodology: A New SHA-3 Implementation on Low-End Microcontrollers“, YoungBeom Kim, Taek-Young Youn, and SeogChung Seo(Corresponding), MDPI Sustainability (SSCI, IF= 2.576)
- “SIKE on GPU: Accelerating Supersingular Isogeny-based Key Encapsulation Mechanism on Graphic Processing Units”, Seog Chung Seo, IEEE ACCESS (SCIE, IF=3.367)
- “Generating Cryptographic S-Boxes Using the Reinforcement Learning“, Giyoon Kim, Hangi Kim, Yeachan Heo, Yongjin Jeon, Jongsung Kim, IEEE ACCESS. (SCIE, I.F=3.745)
- “Forensic analysis of instant messaging apps: Decrypting Wickr and private text messaging data.“, Giyoon Kim, Soram Kim, Myungseo Park, Younjai Park, Insoo Lee, and Jongsung Kim, Forensic Science International: Digital Investigation 37 (2021): 301138. (SCIE, IF=1.66)
- “Research on Note-Taking Apps with Security Features.“, Myungseo Park, Soram Kim, and Jongsung Kim, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications Vol.11(4),(2020):63-76 (SCOPUS)
- “Magniber v2 Ransomware Decryption: Exploiting the Vulnerability of a Self-Developed Pseudo Random Number Generator.“, Sehoon Lee, Myungseo Park, and Jongsung Kim, Electronics Vol.10(1), (2020): 16. (SCIE, IF=2.412)
- “Smart Home Forensics—Data Analysis of IoT Devices“, Soram Kim, Myungseo Park, Sehoon Lee, Jongsung Kim, Electronics, Vol.9(8), (2020): 1215. (SCIE, IF=2.412)
- “A study on the decryption methods of telegram X and BBM-Enterprise databases in mobile and PC“, Giyoon Kim, Myungseo Park, Sehoon Lee, Younjai Park, Insoo Lee, Jongsung Kim , Forensic Science International: Digital Investigation Vol.35 (2020): 300998. (SCIE, IF=1.66)

▶ 국내 저널

- “양자 엔트로피 기반 난수 발생기를 이용한 드론 제어 데이터 보안 연구”, 김태완, 이세윤, 정서우, 위한샘, 이옥연, 정보보호학회논문지 2021년 4월 호

■ “5G+ 초연결 환경을 위한 암호기술 연구”, 장찬국, 김현기, 윤승환, 이옥연, 정보보호학회지 2020년 12월 호

■ “GPU를 이용한 LWE 기반 양자 내성 암호의 병렬화 및 성능 분석”, 김예원, 염용진, 강주성, 한국통신학회논문지, Vol.45, No.12, pp.2,183-2,192, 2020

■ “CHES 2020을 중심으로 살펴본 SW/HW 암호 분석 및 구현 기술 연구 동향”, 안상우, 송진교, 박보선, 서석충, 정보보호학회지 2020년 12월 호

■ “GPU를 활용한 고속 소프트웨어 암호모듈 설계 및 구현”, 송진교, 안상우, 서석충, 정보보호학회논문지(KCI) 2020년 12월 호

■ “차분 퍼징을 이용한 국내 공개 암호소스코드 안전성 검증”, 윤형준, 서석충, 정보보호학회논문지(KCI) 2020년 12월 호

■ “NIST PQC Round 3 격자 기반 암호의 부채널 대응 기법 동향 분석”, 송진교, 김영범, 곽유진, 서석충, 정보보호학회지 2021년 2월 호

■ “ARM/NEON 프로세서를 활용한 NIST PQC SABER에서 Toom-Cook 알고리즘 최적화 구현 연구”, 송진교, 김영범, 서석충, 정보보호논문지(KCI) 2021 6월 호

■ “32-bit RISC-V 프로세서에서 국산 블록 암호 성능 밴치마킹”, 곽유진, 김영범, 서석충, 정보보호논문지(KCI) 2021 6월 호

■ “블록암호 RECTANGLE에 대한 DLCT를 이용한 차분-선형 공격“, 조세희, 백승준, 김종성, 정보보호학회논문지, 31권, 2호, pp. 123-132, 2021.

■ “OBD 스캐너 애플리케이션 INFOCAR 데이터 분석을 통한 차량 포렌식 기법“, 허욱, 김기윤, 김종성, 디지털포렌식연구, 15권 2호, pp. 137-147, 2021.

■ “협업 툴 아티팩트 분석 및 삭제된 데이터 복구 연구“, 신수민, 최용철, 김소람, 김종성, 디지털포렌식연구, 15권 2호, pp. 235-259, 2021.

■ “키 재사용 공격을 통한 RAGNAR LOCKER 랜섬웨어 감염 파일 복호화 및 활용 방안 연구“, 강수진, 이세훈, 김소람, 김대운, 김기문, 김종성, 정보보호학회논문지, 31권 2호, pp. 221-231, 2021.

■ “샤오미 스마트 홈 아티팩트 분석 및 활용방안 연구“, 강수진, 신수민, 김소람, 김기윤, 김종성, 디지털포렌식연구, 15권 1호, pp. 54-67, 2021.

■ “Windows에서의 Wire 크리덴셜 획득 및 아티팩트 분석“, 신수민, 김소람, 윤병철, 김종성, 정보보호학회논문지, 31권 1호, pp. 61-71, 2021.

■ “5ss5c와 Immuni 랜섬웨어의 암호화 프로세스 분석 및 복구방안 연구“, 신수민, 김소람, 윤병철, 허욱, 김대운, 김기문 김종성, 디지털콘텐츠학회논문지, 21권 10호 pp. 1895-1903, 2020

■ “안드로이드 악성코드 탐지를 위한 머신러닝 기술 활용 동향 및 권한정보를 활용한 악성코드 탐지“, 김기윤, 김소람, 전용진, 김종성, 디지털포렌식연구, 14권 3호, pp. 316-326, 2020.

▶ 국제 학회

■ “Optimization of PBKDF2-HMAC-SHA256 and PBKDF2-HMAC-LSH256 in CPU Environments”, HoJin Choi, Seog Chung Seo, 21st World Conference on Information Security Applications (WISA 2020)

■ “An Efficient Implementation of AES on 8-bit AVR-based Sensor Node”, YoungBeom Kim, Seog Chung Seo, 21st World Conference on Information Security Applications (WISA 2020)

■ “Efficient Implementation of SHA-3 Hash Function on 8-bit AVR-based Sensor Nodes”, YoungBeom Kim, HoJin Choi, Seog Chung Seo, the 23rd Annual International Conference on Information Security and Cryptology (ICISC 2020)

■ “Efficient Data Delivery in Content-Centric Network with Stronger Privacy of Publisher”, Taek-Young Youn, Joongheon Kim, and Seog Chung Seo, The 35th International Conference on Information

Networking (ICOIN 2021)

- “PIPO: A Lightweight Block Cipher with Efficient Higher-Order Masking Software Implementations”, Hangi Kim, Yongjin Jeon, Giyoon Kim, Jongsung Kim, Bo Yeon Sim, Dong Guk Han, Hwajeong Seo, Seonggyeom Kim, Seokhie Hong, Jaechul Sung, Deukjo Hong (ICISC 2020)
- “Parallel Implementation of PIPO Block Cipher on 32-bit RISC-V Processor”, Yujin Kwak, YounngBeom Kim, Seog Chung Seo, 22st World Conference on Information Security Applications (WISA 2021)
- “High-Speed Software of Karatsuba Multiplication for SABER Round 3 on ARMv8-A Series”, JinGyo Song, YounngBeom Kim, Seog Chung Seo, 22st World Conference on Information Security Applications (WISA 2021)
- “XTS-AES Parallel Optimization Implementation Technique for Fast FDE”, SangWoo An and Seog Chung Seo, 22st World Conference on Information Security Applications (WISA 2021)

▶ 국내 학회

- “5G-AKA 및 SMC의 RAN 취약점 분석”, 김태완, 김현기, 이옥연, 2021 한국정보보호학회 하계학술대회
- “6G 보안을 위한 5G 코어 오픈소스 프로젝트 분석”, 이세윤, 위한샘, 윤승환, 이옥연, 2021 한국정보보호학회 하계학술대회
- “Lua 스크립트 기반 5G AKA wireshark 플러그인 제작”, 정서우, 장찬국, 이옥연, 2021 한국정보보호학회 하계학술대회
- “IoT 보안 인증 제도 기반 홈 IoT 기기 애플리케이션의 취약점 분석 및 대응책 제시”, 윤혜진, 김은주, 최지원, 위한샘, 이옥연, 2021 한국정보보호학회 하계학술대회
- “모의 공격을 통한 MAVLink 프로토콜 취약점 분석”, 한주홍, 위한샘, 이옥연, 2020 한국정보보호학회 동계학술대회
- “CSFC 내 MSC 솔루션 보안요구사항 비교분석”, 정서우, 오진혁, 장찬국, 이옥연, 2020 한국정보보호학회 동계학술대회
- “UAS 보안인증 시험을 위한 보안 요구사항”, 이세윤, 장찬국, 이옥연, 2020 한국정보보호학회 동계학술대회
- “클라우드 컴퓨팅 서비스 보안 인증제도 개선사항”, 김태완, 김현기, 장찬국, 이옥연, 2020 한국정보보호학회 동계학술대회
- “GPU 환경에서의 효율적인 Number Theoretic Transform 최적화 구현”, 안상우, 서석충, 2020 정보보호학회 동계학술대회
- “NEON을 활용한 NIST 양자암호 Saber에서 다항식 곱셈기반 Toom-Cook 알고리즘 최적화 연구”, 송진교, 김영범, 서석충, 2020 정보보호학회 동계학술대회
- “GPU 환경에서의 SHA-3 최적화 구현 동향”, 최호진, 서석충, 2020 정보보호학회 동계학술대회
- “RISC-V 환경에서 Curve25519의 Reduction 연산 최적화 연구”, 김영범, 송진교, 서석충, 2020 정보보호학회 동계학술대회
- “32-bit RISC-V 환경에서 LEA 최적화 연구”, 곽유진, 김영범, 서석충, 2020 정보보호학회 동계학술대회
- “OpenCL을 사용한 NIST LWC 2 라운드 후보 ESTATE 병렬연산 최적구현”, 박보선, 서석충, 2020 정보보호학회 동계학술대회
- “중복데이터를 이용한 16-bit MSP430 환경에서의 HIGHT 알고리즘 오류공격 대응 연구” , 고의석, 박보선, 서석충, 2020 정보보호학회 동계학술대회
- “ARM Cortex-M4 환경에서 SIMD 명령어를 이용한 CHAM-64/128 최적화 연구”, 이정민, 송진교, 서석충, 2020 정보보호학회 동계학술대회
- “격자기반 양자내성암호에서 RST를 이용한 기각 샘플링 병렬 최적화”, 안상우, 서석충, 2021 한국컴퓨

터종합학술대회

- “타원곡선 암호의 최적화 구현, 부채널 대응기법 동향 분석 및 벤치마킹”, 송진교, 서석충, 2021 한국컴퓨터종합학술대회
- “GPU 환경에서의 NIST PQC 3-round Lattice 및 Symmetric 기반 전자서명 최적화 구현 동향”, 최호진, 서석충, 2021 한국컴퓨터종합학술대회
- “Metamorphic Testing기반 암호알고리즘 구현 정확성 검증 기술 동향 분석”, 김영범, 서석충, 2021 한국컴퓨터종합학술대회
- “Web Assembly를 이용한 국산 블록 암호 알고리즘 벤치마킹”, 박보선, 서석충, 2021 한국컴퓨터종합학술대회
- “32-bit RISC-V 프로세서에서 블록 암호 최적화 구현 동향”, 곽유진, 서석충, 2021 한국컴퓨터종합학술대회
- “중간값 참조 테이블을 활용한 CPU-GPU 하이브리드 AES-XTS 최적화 기법”, 안상우, 서석충, 2021 정보보호학회 하계학술대회
- “ARMv8-A Series에서 Crystal-Dilithium Round 3의 NTT 곱셈 병렬 구현”, 송진교, 김영범, 서석충, 2021 정보보호학회 하계학술대회
- “GPU 환경에서의 SHA-3(512) 병렬 최적 구현”, 최호진, 서석충, 2021 정보보호학회 하계학술대회
- “8-bit AVR 환경에서 PIPO 최적 구현”, 김영범, 서석충, 2021 정보보호학회 하계학술대회
- “OpenCL, OpenMP 병렬처리를 사용한 PIPO 알고리즘 구현”, 박보선, 서석충, 2021 정보보호학회 하계학술대회
- “32-bit 프로세서 ARM Cortex-M4에서의 PIPO 최적화 구현”, 곽유진, 서석충, 2021 정보보호학회 하계학술대회
- “확장된 RNBP 알고리즘“, 박종현, 전용진, 김종성, 정보보호학회 하계 학술대회, 2021.
- “축소 라운드 GIFT의 향상된 차분 선형 특성“, 백승준, 김한기, 김종성, 정보보호학회 하계 학술대회, 2021.
- “NIST 경량암호 공모사업 후보 알고리즘 HyENA의 안전성 분석 동향“, 김주헌, 김시은, 박종현, 백승준, 김종성, 한국정보보호학회 동계 학술대회, 2020.
- “NIST 경량암호 공모사업 후보 알고리즘 COMET의 안전성 분석 동향“, 조세희, 백승준, 김종성, 한국정보보호학회 동계 학술대회, 2020.
- “ARIA에 대한 Shifting Retracing 부메랑 공격”, 백승준, 박종현, 김종성, 한국정보보호학회 동계 학술대회, 2020.
- “디지털 포렌식 관점에서 협업 및 화상회의 애플리케이션 분석“, 신수민, 김소람, 강수진, 김종성, 한국디지털포렌식학회 하계 학술대회, 2021.
- “사진 및 동영상/은닉 암호화 특정 애플리케이션 분석“, 최용철, 김기윤, 김종성, 정보보호학회 하계 학술대회, 2021.
- “윈도우 환경에서 Pinngle 및 미스리 메신저 아티팩트 분석“, 박귀은, 김수빈, 김현재, 이민정, 옥정수, 신수민, 김종성, 정보보호학회 하계 학술대회, 2021.
- “2020년 및 2021년 국내・외 랜섬웨어 대응 정책 동향“, 강수진, 김수빈, 이민정, 김소람, 김종성, 정보보호학회 하계 학술대회, 2021.
- “Ragnar Locker 랜섬웨어 데이터 복호화 방안 연구”, 강수진, 이세훈, 김소람, 김종성, 정보보호학회 동계 학술대회, 2020.
- “디지털 포렌식 관점에서의 샤오미 스마트 홈 아티팩트 분석”, 강수진, 신수민, 김소람, 김기윤, 김종성, 한국디지털포렌식학회 동계 학술대회, 2020.

▶ 수상

- 2021 한국정보보호학회 하계학술대회 우수논문상
- 2020 국가암호 공모전 최우수상 1건, 장려상 1건, 특별상 2건 수상
- 2021 한국컴퓨터 종합학술대회 우수발표논문상 (KCC 2021)
- 2020 한국정보보호학회 동계학술대회 한국전자통신연구원 원장상 수상
- 2020 한국디지털포렌식학회 동계학술대회 디지털포렌식학회 학회장상 수상
- 2020 부채널 분석 경진대회 학회장상 수상
- 2020 국가암호공모전 특별상 수상
- 2020 디지털 포렌식 챌린지 Tech Contest 입상 (2위)

▶ 특허

- 비행체에서의 잡음원 도출 장치 및 방법
- 5G SIDF 암호처리장치 및 그 방법
- DUSS 지원 가능한 양자난수 엔트로피 암호화용 코드 발급 장치 및 방법
- 구명용 비상신호 발신장치 및 방법
- 독립성 측정을 이용한 엔트로피 관리 장치 및 방법, 이를 이용한 난수 생성 장치
- 수중 사물 인터넷의 온톨로지 기반 통신 매체 선택 방법 및 이를 수행하는 수중 통신 장치
- 무선 통신 기기 및 이의 동작 방법’(‘21.01), ‘수중 네트워크 관리 시스템 및 그의 동작 방법
- TUM-IoT에서의 심리스 서비스 기반 경로 설정 기법
- 수중 네트워크 관리 시스템
- 수중 네트워크 관리 시스템 및 그의 동작 방법
- 종단간 암호화가 적용된 파일에 대한 복호화 장치 및 방법
- 캐시 파일을 이용한 삭제 메시지 복구 장치 및 방법
- 부채널 공격 대응이 용이한 128비트 경량 블록 암호화 방법 및 이를 이용한 장치

▶ 기술이전

- 양자난수 기반 UAV용 LTE암호장비 개발 기술
- KMULIB v2.1 Windows용 KCMVP 검증필암호모듈
- 하이브리드 수중무선통신 장치 및 그 통신 방법

▶ 연구비 수주 실적

- 자체평가 대상 기간 총 56건의 연구를 수행하였으며, 총연구비 8,220,366,437원, 수입금액 5,666,481,468원을 달성하였음

▶ 연구비 수주실적 표(자체평가 대상 기간 2020.9.1.~2021.8.31.)

총 56건			합계	8,220366,437	5,666,481,468
연번	과제번호	연구과제명	기간	총연구비	수입금액
1	A2021-0304	5G와 클라우드 융합환경에서의 안전한 UTM 서비스를 위한 보안기술 연구 및 인력 양성	2021-05-01~ 2022-04-30	260,000,000	260,000,000
2	A2021-0058	CCTV 암호화 영상 및 프로토콜 취약점 분석	2021-03-01~ 2021-08-31	30,000,000	30,000,000
3	A2021-0004	한전 KCMVP 암호모듈 재검증을 위한 소스코드 검증 및 표준문서 작성	2021-01-04~ 2022-01-03	187,000,000	130,900,000

4	A2021-0059	5G+ 기반 6G 이동통신 정보보안 기술 연구(1/2)	2021-01-01~ 2021-12-31	339,000,000	339,000,000
5	A2021-0053	베타 난수칩을 적용한 IoT 보안통신 활용 기술 개발(1/1)	2021-01-01~ 2021-12-31	40,000,000	40,000,000
6	G2021-0001	UAV용 양자난수 기반 암호모듈 상용화 자문 용역	2021-01-01~ 2021-06-30	22,000,000	22,000,000
7	A2020-0318	DW-01 위성통신 인프라 상에서의 스크램블링 및 보안 규격 분석	2020-06-22~ 2020-11-30	28,000,000	14,000,000
8	A2020-0021	(MC31) 의사난수 생성기술 및 암호 알고리즘 식별기술 연구(4/4)	2020-01-01~ 2020-11-30	97,232,798	51,180,709
9	A2019-0515	군SW형 암호를 탑재한 드론 전투실험	2019-12-16~ 2020-12-31	188,035,000	56,410,500
10	A2021-0349	양자컴퓨팅 환경에 대비한 분산자원 플랫폼 관리용 암호 기술 연구(1/3)	2021-05-24~ 2022-02-23	67,500,000	67,500,000
11	S2021-0280	DRAM Security 기술 연구 클러스트 산학	2021-07-01~ 2024-06-30	264,000,000	44,000,000
12	A2021-0268	고신뢰 온-디바이스 딥러닝 가속기 설계를 위한물리채널 기반 취약점 검증 및 대응기술 개발	2021-04-01~ 2021-12-31	114,000,000	114,000,000
13	A2021-0054	무선 은닉채널 위험성 검증 연구(1/2)	2021-01-01~ 2021-12-31	80,000,000	80,000,000
14	A2021-0055	(ICT 전문연구실) SCR-Friendly 대칭키 암호 및 응용 모드 개발(2/2)	2021-01-01~ 2021-12-31	300,000,000	300,000,000
15	S2021-0026	양자내성암호 대상 부채널 내성암호 연구	2021-02-15~ 2021-12-14	110,000,000	44,000,000
16	A2020-0478	딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발(2차년도)	2020-12-01~ 2021-11-30	100,000,000	74,704,504
17	A2021-0210	격자 기반 양자 내성 PKE/KEM 알고리즘의 안전한 구현기술 연구	2021-04-01~ 2021-10-31	45,000,000	31,500,000
18	A2021-0211	스마트폰 외부 통신 인터페이스를 활용한 기기정보 식별기술 연구	2021-04-01~ 2021-10-31	60,000,000	42,000,000
19	A2020-0027	(ICT 기초연구실) SCR-Friendly 대칭키 암호 및 응용 모드 개발(4차년도)	2020-01-01~ 2020-12-31	305,000,000	60,000,000
20	S2020-0009	PQC대상 부채널내성암호 기술연구	2020-02-01~ 2020-11-30	110,000,000	33,000,000
21	A2019-0503	딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발(1차년도)	2019-12-01~ 2020-11-30	100,000,000	99,956,226
22	A2020-0020	(MC24) 비침입·준침입 공격 및 분석기법 연구(4/4)	2020-01-01~ 2020-11-30	151,196,818	79,585,905
23	A2020-0270	IoT용 초경량 암호 부채널 분석 검증 기술 동향	2020-06-01~ 2020-10-31	46,900,000	23,450,000
24	A2021-0227	암호 알고리즘 표준화 현황 및 전환 프로세스 분석	2021-04-16~ 2021-10-31	50,000,000	35,000,000
25	A2020-0283	QKD 비광학적 구성요소 안전성 검증 모델 연구	2020-06-01~ 2020-11-15	50,000,000	15,000,000
26	A2020-0253	신경망을 이용한 난수성 및 블록암호	2020-05-07~	60,000,000	18,000,000

		안전성 분석 기법 연구	2020-12-06		
27	A2021-0213	모바일 기반(안드로이드) 안티포렌식 소프트웨어 정보은닉 방식 연구	2021-04-01~ 2021-10-31	70,000,000	49,000,000
28	A2021-0214	디지털포렌식 도구의 증거 수집 및 분석 신뢰성 검증 연구	2021-04-01~ 2021-10-31	50,000,000	35,000,000
29	A2021-0187	랜섬웨어 동향 및 암호기능 상세분석 추진	2021-03-23~ 2021-11-30	85,500,000	68,400,000
30	A2021-0093	IoT 환경에 적용 가능한 디지털 포렌식 분석 연구(3/3)	2021-03-01~ 2022-02-28	50,000,000	50,000,000
31	A2020-0262	모바일DB 및 PC기반 안티포렌식앱 분석 기법 연구	2020-06-01~ 2020-11-27	174,500,000	52,350,000
32	A2020-0194	랜섬웨어 암호기능 및 복구가능성 분석	2020-03-31~ 2020-11-30	85,500,000	17,100,000
33	A2020-0022	(MC33) 블록암호/해쉬함수 분석기술 연구 및 분석도구 개발(4/4)	2020-01-01~ 2020-11-30	116,119,821	61,122,326
34	A2021-0356	부호기반 암호의 안전성 및 효율성에 관한 연구(1/3)	2021-06-01~ 2022-02-28	58,864,000	58,864,000
35	A2021-0225	NIST PQC 공모 코드 기반 암호의 안전성에 관한 연구	2021-04-16~ 2021-10-31	60,000,000	42,000,000
36	A2021-0269	국가공공 정보시스템 안전성 및 활용성 제고를 위한 차세대 암호체계 개발	2021-04-01~ 2021-12-31	160,000,000	160,000,000
37	A2021-0267	GPU/ASIC 기반 암호알고리즘 고속화 설계 및 구현 기술개발	2021-04-01~ 2021-12-31	285,000,000	285,000,000
38	A2021-0270	상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구	2021-04-01~ 2021-12-31	100,000,000	100,000,000
39	A2021-0212	Metamorphic Testing 기반 암호 알고리즘 구현 취약점 검증기술 연구	2021-04-01~ 2021-10-31	60,000,000	42,000,000
40	S2021-0036	암호모듈검증시험(K-CMVP) 인증 용역	2021-03-02~ 2021-11-30	50,000,000	15,000,000
41	A2021-0098	양자컴퓨팅환경에서 안전한 보안통신을 위한 포스트 양자암호 키설정방법 최적화 구현기술 연구(3/3)	2021-03-01~ 2022-02-28	50,000,000	50,000,000
42	A2021-0263	수중 SNS 포스팅을 지원하는 다이버 데이터 심리스 커뮤니케이션 개발(1/2)	2021-04-16~ 2021-12-31	90,000,000	19,225,280
43	A2021-0260	극한지 관측 정보 네트워크 구조 설계/검증(1/5)	2021-04-01~ 2021-12-31	120,000,000	34,976,090
44	A2021-0322	해상통신 네트워크 연동기술 설계 (1/5)	2021-04-01~ 2021-12-31	40,000,000	3,779,825
45	A2021-0012	Flying BS 기반 극지 생물 바이오로거 데이터 원격 회수 기술 개발(2/3)	2021-01-01~ 2021-12-31	82,500,000	82,500,000
46	A2021-0078	IoT 기반 수중 네트워크 연동 서비스 플랫폼 기술 표준개발(3차년도)	2021-01-01~ 2021-12-31	115,000,000	71,950,318
47	A2021-0010	지상망을 고려한 수중망 인터페이스 설계(10/10)	2021-01-01~ 2022-07-31	50,000,000	21,490,997
48	A2021-0009	분산형 수중 관측 제어망 개발(7/7)	2021-01-01~ 2021-12-31	80,000,000	28,946,325
49	A2020-0426	Flying BS 기반 극지 생물 바이오로	2020-08-01~	35,000,000	35,000,000

		거 데이터 원격 회수 기술 개발(1/3)	2020-12-31		
50	A2020-0117	IoT 기반 수중 네트워크 연동 서비스 플랫폼 기술 표준개발(2차년도)	2020-01-01~ 2020-12-31	101,700,000	32,238,986
51	A2020-0068	분산형 수중 관측 제어망 개발(6/7)	2020-01-01~ 2020-12-31	90,000,000	52,418,595
52	A2020-0165	지상망을 고려한 수중망 인터페이스 설계(9/10)	2020-01-01~ 2020-12-31	50,000,000	42,112,882
53	S2020-0002	딥러닝 기반 부분 가림 영상 복원 기술 개발	2020-01-02~ 2021-06-30	110,000,000	55,000,000
54	A2021-0107	모듈형 스마트 패션 플랫폼 연구센터(2/2-3단계)	2021-03-01~ 2022-02-28	2,000,000,000	1,400,000,000
55	A2021-0142	단안 영상 기반 사용자 중심 3차원 인터랙션을 위한 경량 비전 기술 연구(1/3)	2021-03-01~ 2022-02-28	95,818,000	95,818,000
56	A2021-0076	AI 기반 선도적 실전문제해결 연구인재 양성(1/2)	2021-01-01~ 2021-12-31	500,000,000	500,000,000

1. 참여교수 연구역량

1.1 연구비 수주 실적

<표 3-1> 최근 1년간(2020.9.1.-2021.8.31.) 참여교수 1인당 정부, 산업체, 해외기관 등 연구비 수주 실적

항 목	수주액(천원)		
	3년간(2017.1.1.-2019.12.31.) 실적 (선정평가 보고서 작성내용)	최근 1년간(2020.9.1.~2021.8.31.) 실적	비고
정부 연구비 수주 총 입금액	9,858,736	5,666,481	약 1.7배
산업체(국내) 연구비 수주 총 입금액	763,070	250,450	약 1배
해외기관 연구비 수주 총 (환산) 입금액	0	0	
1인당 총 연구비 수주액	1,062,180	566,648	약 1.6배
참여교수 수	10	10	

1.2 연구업적물

① 참여교수 연구업적물의 우수성 (자체평가 대상 기간 2020.9.1.~2021.8.31.)

▶ 국제 저널

■ Accelerated implementation for testing IID assumption of NIST SP 800-90B using GPU

✓ 병렬 엔트로피 추정 프로그램을 개발하여 기존 NIST에서 공개한 도구대비 3~25배 빠른 엔트로피 추정을 가능하도록 하였음

■ Single-Trace Attacks on Message Encoding in Lattice-Based KEMs
  ✓ 후양자 암호 중 격자 기반을 대상으로 신규 부채널 공격 기법을 제안하였음
■ Improved Differential Fault Attack on LEA by Algebraic Representation of Modular Addition
  ✓ 경량 블록 암호 LEA에 대한 신규 오류 주입 공격 기법을 제안하였음
■ Non-Profiled Side-Channel Attack Based on Deep Learning Using Picture Trace
  ✓ 부채널 파형을 1차원 수열 데이터가 아닌 2차원의 그림 데이터로 보고 이를 이용한 신규 부채널 공격 기법을 제안하였음

▶ 국내 학회
■ 확장 이진 유한체 제곱근 연산의 최적 구현 기법에 관한 연구
  ✓ C언어와 테이블 참조를 활용한 지수승 연산의 고속화를 진행하였음
■ Horner's Method와 Chien Search의 효율성 측정에 관한 연구
  ✓ BCH부호에서 오류벡터는 오류벡터의 해밍무게, 위치정보를 복구를 위한 다항식 근 계산 방법을 비교, 계산복잡도를 파악하고 SAGE를 통해 구현하여 성능 비교를 진행하였음

▶ 특허
■ "수중 사물 인터넷의 온톨로지 기반 통신 매체 선택 방법 및 이를 수행하는 수중 통신 장치" ('20.12)
■ "무선 통신 기기 및 이의 동작 방법" ('21.01)
■ "수중 네트워크 관리 시스템 및 그의 동작 방" ' ('21.01)
■ "TUM-IoT에서의 심리스 서비스 기반 경로 설정 기법" ('21.02)
■ "수중 네트워크 관리 시스템" ('21.02)
■ "수중 네트워크 관리 시스템 및 그의 동작 방법" ('21.02) 등 6건 특허 출허
■ 다중매체 채널을 통해 다양한 운영조건의 수중통신 요구사항을 충족하는 기술인 '하이브리드 수중무선통신 장치 및 그 통신 방법' 국내 등록특허의 기술 실시권 부여('21.05)

② 교육연구단의 학문적 수월성을 대표하는 연구업적물 (자체평가 대상 기간 2020.9.1.-2021.8.31.)

연번	대표연구업적물 설명
1	▶ 퓨시아 운영체제 및 지르콘 커널의 난수발생기에 대한 안전성 분석 연구 [김예원, 염용진, 강주성, "퓨시아 운영체제 및 지르콘 커널의 난수발생기에 대한 안전성 분석 연구", 한국통신학회 논문지, Vol.31, No.2, pp.145-156, 2021.] 퓨시아(Fuchsia)는 구글이 개발하고 있는 지르콘(Zircon)이라는 마이크로 커널(microkernel)을 기반으로 하는 운영체제이며, 일반환경과 경량환경에서 사용될 수 있다. 난수발생기의 취약성은 운영체제의 안전성에 영향을 미치므로, 퓨시아 및 지르콘에서 사용하는 난수발생기에 대한 안전성 분석이 필요하다. 본 연구실에서는 퓨시아 및 지르콘의 난수발생기에 대한 구조와 사용하는 엔트로피 소스를 분석하였다. 또한, 퓨시아 및 지르콘의 난수발생기 의 유일한 입력이 될 가능성이 큰 지터 엔트로피 소스에 대한 엔트로피를 추정하고, 지터 엔트로피 소스에 대한 전수조사 방법과 전수조사량을 제시하였다. 본 연구의 결과는 다양한 환경에서 동작하는 퓨시아 및 지르콘 난수발생기에 대한 공격 가능성을 보여주며, 지터 엔트로피 소스를 사용하는 여러 운영체제의 난수발생기에 대한 안전성을 분석하는 데 활용될 것으로 기대한다.
2	▶ 암호학적 난수발생기 잡음원의 분포 변화 탐지법 [박호중, 권수진, 염용진, 강주성, "암호학적 난수발생기 잡음원의 분포 변화 탐지법", 한국통신학회논문지, Vol.46, No.7, pp.1,208-1,218, 2021.]

	암호학적으로 안전한 난수는 암호시스템에 필수적으로 사용된다. 암호학적으로 안전한 난수발생기의 안전성은 난수성의 원천이라 할 수 있는 잡음원의 엔트로피에 근본적으로 의존하며, 대표적인 엔트로피 추정법으로는 미국 NIST의 SP 800-90B가 널리 알려져 있다. 하지만 NIST의 엔트로피 추정법은 기본적으로 잡음원의 분포가 변하지 않음을 가정하고 설계를 하였기 때문에 SP 800-90B에는 잡음원의 분포 변화를 확인하는 방법이 명시되어 있지 않다. 본 연구실에서는 잡음원의 분포 변화를 탐지할 수 있는 방법을 제시하였다. 제시하는 방법은 잡음원의 통계적 특성이 IID인 경우와 마르코프 특성을 가지는 Non-IID인 경우를 포함하고 있다. 또한, 여러 시뮬레이션을 통해 제안한 분포 변화 탐지법의 유효성을 실험적으로 확인하였다. 본 연구실에서 제시한 방법은 잡음원의 분포가 기존 설계에서 변했는지 확인하는 잡음원의 정류성 검사로 활용될 것으로 기대한다.
3	▶ 다중 사용자 환경에서 효과적인 키 교환을 위한 GPU 기반의 NTRU 고속구현 [성효은, 김예원, 염용진, 강주성, “다중 사용자 환경에서 효과적인 키 교환을 위한 GPU 기반의 NTRU 고속구현”, 한국통신학회논문지, Vol.31, No.3, pp.481-496, 2021.] GPU를 이용하여 격자 기반 양자내성암호인 NTRU를 병렬 고속화하는 방법을 제시하였고, 병렬화된 NTRU를 활용하여 TLS 상에서 서버와 다수의 사용자가 세션키(session key)를 공유하는 키 교환(key exchange) 시나리오를 제시하였다. 향후 NIST가 양자내성암호를 표준화하여 다수의 사용자 환경에서 서버가 대량의 데이터를 처리해야 할 때, 본 연구실에서 제시한 방법을 활용하여 효과적인 키 교환을 실행 가능할 것으로 기대한다.
4	▶ Improved Differential Fault Attack on LEA by Algebraic Representation of Modular Addition [Seonghyuck Lim, Jonghyeok Lee, Dong-Guk Han, IEEE Access 8 (2020): 212794-212802.] IoT 장비의 발전과 사용량 증가에 따라 경량암호의 안전성에 대한 평가는 필수적이다. LEA는 국산 경량 블록암호로 국제 경량 블록암호 표준이다. 기존 LEA에 대한 차분오류공격 기법은 단일 비트 반전 오류 기반으로 강한 공격자 가정에 기반한다. 하지만 본 연구에서는 모듈로 덧셈에 대한 그뢰브너 기저 기반의 대수적 표현을 통해 랜덤 워드 오류 기반의 완화된 공격자 가정에서 효율적인 차분 오류 공격이 가능함을 보여준다. 따라서 LEA 운용에 있어 오류주입 대응기법 적용의 필요성을 시사하며, 본 기술이 LEA 오류주입 안전성 검증에 기여할 것으로 기대한다.
5	▶ Single-Trace Attacks on Message Encoding in Lattice-Based KEMs [Bo-Yeon Sim, Jihoon Kwon, Joohee Lee, Il-Ju Kim, Tae-Ho Lee, Jaeseung Han, Hyojin Yoon, Jihoon Cho, Dong-Guk Han, IEEE Access 8 (2020): 212794-212802] 양자 내성 암호(PQC)는 미래에 필수적으로 사용될 암호로 고려되고 있다. 특히 표준화 공모를 진행 중인 NIST에서는 현재 15개의 암호 알고리즘을 대상으로 Round 3를 진행 중이다. 거의 대부분의 암호 알고리즘들이 메시지의 올바른 암복호화를 위하여 메시지 인코딩이라는 기술을 사용하는데 그 과정에서 부채널 취약점이 발생한다. 본 연구실에서는 다양한 PQC 후보들의 메시지 인코딩 연산의 부채널 분석을 통해 비밀 메시지를 복구하여 암호 통신에 사용되는 세션키를 획득하는 방법을 제시했다. 본 연구는 단일 파형으로도 분석이 가능한 매우 강력한 공격으로써 이후 PQC의 부채널 분석 대응기법 설계 방향에 크게 활용될 것으로 기대한다.
6	▶ Secure and Fast Implementation of ARX-Based Block Ciphers Using ASIMD Instructions in ARMv8 Platforms [JinGyo Song, Seo Chung Seo, IEEE Access 8 (2020): 193138-193153.] 현재 모바일 및 태블릿 환경에서 널리 사용될 뿐만 아니라, 자율주행 및 컴퓨터의 핵심 Core로

	발전하고 있는 ARMv8-A Series에서 경량암호 (HIGHT, Revised CHAM)의 최적 구현 및 오류공격 대응 구현 방법을 제안하였다. NEON 엔진을 활용하여 제안하는 병렬 구현을 통해 다수의 암호화를 동시에 수행하였다. 특히, 임베디드 환경에서 오류공격은 DFA 공격으로 실질적인 부채널 공격 중 하나로 발전하고 있다. 이전 오류공격 대응 구현에서 연산 부하가 큰 연산에 대해 이를 더욱 최적 구현할 방안을 제시하여, 오류공격 대응책의 연산 부하를 효과적으로 감소시켰다. 본 연구결과는 ARMv8-A Series에서 최초의 경량암호(HIGHT, Revised CHAM)에 대한 고속 구현 결과이며, 제안된 방법이 기존 대안을 능가하여 우수한 연구결과를 제공하였다.
7	▶ Efficient Parallel Implementations of LWE-based Post-Quantum Cryptosystems on Graphics Processing Units [SangWoo An, Seog Chung Seo, Mathematics 8.10 (2020): 1781.] 현재 양자 알고리즘에도 안전한 양자내성암호 기술을 표준화하고 있는 NIST 공모전 Round 2 후보로 선정된 KEM 알고리즘인 FrodoKEM과 NewHope의 구성 함수에 대한 병렬 최적화 구현 기법을 제안한다. FrodoKEM의 주요 연산 방식인 다항식 기반 연산을 GPU 스레드를 활용하여 병렬적으로 협력 연산하는 기법을 소개하며, NewHope의 경우 NTT 기반 연산을 고속화할 수 있는 구현 방향성을 제시하였다. 구현 결과, 기존 CPU 환경에서의 연산 대비 훌륭한 성능 향상을 확인할 수 있었다. 기존에 격자기반 양자내성암호에 대한 GPU 환경 상에서의 연구가 미진하였기에 제안된 최적화 구현 기법은 큰 의미가 있으며, 본 연구결과는 향후 타 격자기반 양자내성암호나 양자내성암호 기반 전자서명 알고리즘에도 활용될 수 있다.
8	▶ Efficient Implementation of AES and CTR_DRBG on 8-bit AVR-based Sensor Nodes [Kim, Youngbeom, and Seog Chung Seo, IEEE Access 9 (2021): 30496-30510.] 임베디드 디바이스 기반의 센서노드중 가장 널리 사용되는 AVR환경에서 국제표준 알고리즘인 AES의 새로운 최적화 구현을 제안한다. AES의 세가지 연산인 SubBytes, ShiftRows, MixColumns을 하나로 합쳐 구현하며 column-wise 접근방안을 통해 메모리 엑세스를 최대로 줄였다. 이를 통해 2019년에 제안된 AES최적화 구현인 FACE-LIGHT와 달리 테이블생성비용이 필요 없으며 모든 블록암호 운용모드에 적용할 수 있다. 본연구결과는 AVR환경에서 가장빠른 AES구현을 달성하였고, 향후 양자내성암호의 난수생성과정에서 AES를 기반한 난수발생기에 효과적으로 사용될 수 있다.
9	▶ Forensic analysis of instant messaging apps: Decrypting Wickr and private text messaging data [Giyoon Kim, Soram Kim, Myungseo Park, Younjai Park, Insoo Lee, and Jongsung Kim, Forensic Science International: Digital Investigation 37 (2021): 301138] ▶ A study on the decryption methods of telegram X and BBM-Enterprise databases in mobile and PC [Giyoon Kim, Myungseo Park, Sehoon Lee, Younjai Park, Insoo Lee, Jongsung Kim , Forensic Science International: Digital Investigation Vol.35 (2020): 300998] 다양한 개인정보를 저장하고 있는 인스턴트 메신저는 디지털 포렌식 수사관점에서 주요 분석대상이다. 하지만, 많은 메신저가 개인정보 보호를 위해 보안기능을 적용하고 있다. 보안기능은 사용 방법에 따라 디지털 포렌식 수사관점에서 안티포렌식으로 작동할 수 있다. 보안 메신저로 알려진 다양한 메신저들은 강력한 암호시스템을 구축하여 개인정보를 보호하고 있다. 이로인해 용의자의 데이터역시 확보하기 어려운 실정이다. 따라서 이러한 보안 메신저에 대한 분석은 중요하다. 본 논문들 에서는 보안메신저로 알려진 Wickr, Private Text Messaging, Telegram X, BBM-Enterprise의 데이터 암호화 스킴을 분석하고 데이터 복호화 방안 및 주요 키의 복구가능성을 논의하였다.

③ 참여교수 특허, 기술이전, 창업 실적의 우수성 (자체평가 대상 기간 2020.9.1.~2021.8.31.)

▶ 국외 특허

■ Apparatus and Method for Inspecting Side Channels of Combined Smartcard (EP3232375B1)

✓ 콤비형 스마트카에 대한 부채널 분석 방법을 개발한 특허임

▶ 국내 특허

■ DUSS 지원 가능한 양자난수 엔트로피 암호화용 코드 발급 장치 및 방법

✓ 안전한 DRBG 기반의 난수를 생성하기 위한 알파 또는 베타선원 기반의 양자 엔트로피를 적용하는 방법에 대한 특허임

■ 구명용 비상신호 발신장치 및 방법

✓ 무선통신을 사용하여 해상, 산악지역 등에서 발생가능한 인명사고 예방을 위해 통신과 보안과 식별이 가능한 구명장치의 방법에 대한 특허임

■ 경량 엔트로피 관리 장치 및 방법

✓ 덧셈 연산 과정에서 발생하는 캐리 정보를 이용하여 엔트로피 풀의 통계적 난수성을 향상할 수 있고 경량 환경에도 쉽게 적용할 수 있는 엔트로피 관리장치를 발명에 대한 특허임

■ 경량 블록 암호화에 대한 고차 부채널 공격에 대응하는 방법 및 이를 이용한 장치

■ 경량 블록 암호화에 대한 1차 부채널 공격에 대응하는 방법 및 이를 이용한 장치

■ NTRU LPRime 암호에 대한 부채널 분석 장치 및 방법

■ 부채널 공격 대응이 용이한 128비트 경량 블록 암호화 방법 및 이를 이용한 장치

■ 수중 사물 인터넷의 온톨로지 기반 통신 매체 선택 방법 및 이를 수행하는 수중 통신 장치

■ 무선 통신 기기 및 이의 동작 방법

■ 수중 네트워크 관리 시스템 및 그의 동작 방법

■ TUM-IoT에서의 심리스 서비스 기반 경로 설정 기법

■ 수중 네트워크 관리 시스템

■ 수중 네트워크 관리 시스템 및 그의 동작 방법

■ 종단간 암호화가 적용된 파일에 대한 복호화 장치 및 방법

■ 캐시 파일을 이용한 삭제 메시지 복구 장치 및 방법

■ 부채널 공격 대응이 용이한 128비트 경량 블록 암호화 방법 및 이를 이용한 장치

▶ 기술이전

■ 양자난수 기반 UAV용 LTE 암호장비 개발 기술

✓ 양자엔트로피 및 DRBG를 활용하는 양자난수를 적용하여 드론 등의 UAV의 안전한 데이터 전송이 가능한 통신 및 암호장비 개발을 위한 기술임

■ KMULIB v2.1 Windows용 KCMVP 검증필암호모듈

✓ Windows 환경을 위한 KMULiB v2.1 검증필암호모듈이며, 해당 기업에 암호모듈과 함께, 활용방법을 이전하였음

■ 하이브리드 수중무선통신 장치 및 그 통신 방법

✓ 다중매체 채널을 통해 다양한 운영조건의 수중통신 요구사항을 충족하는 기술인 ‘하이브리드 수중무선통신 장치 및 그 통신 방법’ 국내 등록특허의 기술 실시권 부여에 참여하였으며 기술이전 완료 기업의 사업화, 제품화를 위한 대상 기술의 고도화 후속 연구 수행 중임

2. 산업・사회에 대한 기여도

▶ 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

▶ 박수현 교수는 국제 공적 표준 SDO(Standard Development Organization) 수중통신, 해양통신, 디지털트윈 분야 ISO/IEC JTC 1/SC 41 WG7이 신설됨(21.06), 박수현 교수는 지난 10년간 ISO/IEC JTC 1/SC 41에서 '수중통신' 기술 국제 공적 표준화 위원으로 활동하며 UWASN(Underwater Acoustic Sensor Network) 기술의 표준 제정에 기여한 노력과 수중, 해상 도메인 통신기술 기반의 도메인 발전방향을 예측, 제안함에 따라 세계 여러 표준 위원들의 합의를 통해 이번 신설 그룹 Convenor로 선정됨. 이에 가까운 미래 '위성 인터넷, 해양플랜트 고도화/다변화, 저탄소 대체에너지 발전(power generation), 해양물류 시스템 무인화/고도화 등'의 연구/빅데이터/비즈니스 활성화가 예상되는 '수중, 해상' 도메인의 초연결 기술 표준화 주제를 한국이 선점하고자 '수중 망관리 프로토콜(U-NMS), 수중 사물인터넷, 해상 사물인터넷, 수중-해상-지상 연동형 사물인터넷, 수중-해상-지상 복합 도메인 Digital Twin'이 포함된 WG 7 로드맵을 21.06~08까지 개발하고 현재 기업/기관이 참여하는 한국 표준그룹의 검토를 진행하고 있음. WG7은 기존 해상 SDO 'ITU, IMO 등'과 이해관계가 없는 최신 Trend를 추구함에 따라 로드맵 확정 전 수중/해양 통신 기반 보안기술도 고려할 계획임

▶ 강주성, 염용진 교수는 난수발생기의 잡음원 분포, 엔트로피 추정법, 안전성 분석, 경량환경에서의 적용 등의 연구를 진행하여 자체 평가기간 동안 특허 등록 2건, 국제 논문지 1편, 국내 논문지 2편, 국내 학술대회 4편의 성과를 냄. 정보보안시스템에서 난수발생기는 암호키와 보안 매개변수, 암호 프로토콜에서 사용하는 각종 파라미터 등의 생성 시에 반드시 사용되어야 하는 핵심 요소임. 안전하지 않은 난수발생기의 사용이나 잘못된 사용 때문에 암호시스템과 암호 프로토콜의 취약점이 발견된 사례가 빈번하게 보고되고 있음. 따라서 암호학적 난수발생기의 안전성은 입력되는 잡음원의 엔트로피에 의존하기 때문에 사용되는 잡음원에 대한 엔트로피를 최대한 정확하게 추정할 수 있는 기술은 필수적으로 필요함. 그러므로 본 연구 결과들은 안전한 난수발생기 사용에 대한 토대를 마련하여 난수발생기의 취약성으로 발생할 수 있는 산업・사회적 피해를 최소화하는데 이바지할 수 있을 것으로 기대됨

▶ NIST는 양자 컴퓨팅 시대에도 안전성을 보장받을 수 있는 양자내성암호에 대한 표준화 공모사업 진행 중이며, 2022년에 표준화 초안을 준비하고 있음. 후보로 등록된 알고리즘은 대부분은 기존에 사용하는 암호 알고리즘과 연산 측면에서 상이한 구조를 가짐. 암호 알고리즘이 산업계에서 활용되기 위해서는 안전성뿐만 아니라 계산 효율성도 보장되어야 함. 강주성, 염용진 교수는 GPU를 이용한 양자내성암호 고속구현기법 제안과 성능분석에 관한 연구를 진행하여 자체 평가기간 동안 국내 논문지 2편의 성과를 냄. 본 연구 결과는 향후 국가/공공기관뿐만 아니라 산업계에서 NIST의 표준화된 양자내성암호 도입 시, 고속구현 기술에 관한 기반연구로 활용될 것으로 기됨

▶ 강주성, 염용진 교수는 산업체 에잇바이트가 주관하는 사업에서 연구과제명 '양자내성암호가 적용된 비대면 금융거래 암호화 기술 개발' 로 공동연구를 진행하고 있음. PQC 기반 보안 프로토콜 설계 및 구축과 양자내성암호 알고리즘 분석 및 암호키 보호 기술 메커니즘 연구를 진행하고 있음. 2021년 8월 1일 ~ 2022년 7월 31일 동안 총 5,000만 원의 연구비 수주를 달성함. 다가오는 포스트 퀀텀 시대에 기존 공개키암호와 양자내성암호가 결합된 하이브리드 방식의 인증/암호화 제품을 선보임으로써 새로운 시장의 활로를 개척해나가는 계기가 될 것으로 기대됨

▶ 한동국 교수는 전자신문의 기사 "쇼핑몰서 산 RFID 카드 복제기에 아파트 도어락 뚫렸다" 에서 과학기술을 이용한 범죄 문제를 다룸. 현재 다방면에서 사용되는 저가 RFID가 복제 가능성에 취약함에도 저렴하다는 이유로 여전히 사용되고 있음을 지적함. 이처럼 부채널 분석에 취약하지만 경제적인 이유로 실생활에 널리 사용

되는 제품에 대한 안전성을 지적하여 향후 예견되는 산업·사회적 피해를 사전에 예방할 수 있을 것으로 기대됨

▶ 김동찬 교수는 부호기반 암호에대한 안전성 분석을 지속적으로 진행하고 있음. 현재 NIST가 진행 중인 양자내성암호 공모전은 현재 최종라운드 심사를 진행하고 있음. 공모전의 KEM 분야에는 격자기반암호와 부호기반암호가 최종후보에 왔으나 부호기반암호는 현재까지 안전성에 대한 증명이 완전하게 이루어진 것이 아니므로 다양한 시도를 통해 안전성에 대한 연구가 진행 중임. 따라서 부호기반암호의 안전성 판단을 위해서는 현재까지 진행된 다양한 안전성 분석 기법에 대한 연구와 그에 따른 안전성의 확인이 필요함. 그러므로 현재 연구중인 분야는 앞으로 다양한 부호기반암호의 안전성 판단에 기반이 될 것으로 기대됨

▶ 서석충 교수는 암호 알고리즘의 고속 설계 및 부채널 분석 대응 구현시의 성능 부하 최소화 연구로 결과를 도출하고 있음. 수학적으로 안전한 암호 알고리즘이라도 부채널 공격에는 취약하므로, 구현 상에서는 반드시 부채널 공격을 대응할 수 있는 대응책이 적용되어야함. 하지만 이러한 부채널 대응책은 성능 부하를 발생시키며, 이는 전체적인 성능 저하를 발생시킴. 따라서 암호 알고리즘의 고속 설계뿐만 아니라, 부채널 분석 대응 구현을 적용하고 이에 대한 성능 부하를 최소화는 필수적이며, 이러한 최적화를 통해 안전하고 고속화된 보안을 구성할 수 있을 것으로 기대됨

▶ 격자기반 암호에서 가장 성능 부하가 큰 부분은 다항식 곱셈임. 서석충 교수는 다항식 곱셈에 대한 성능 부하를 최소화하기 위해, 다수의 연구를 수행하여 결과를 도출하고 있음. 양자컴퓨터에서 Shor 알고리즘을 적용하면 기존 공개키 암호의 안전성 (인수분해, 이산로그)이 다항시간내에 풀리게 됨. 이로인해 NIST에서는 양자 컴퓨팅 환경에 안전한 양자내성 암호 공모사업을 진행 중임. 특히 격자기반 암호는 양자내성 암호 중 가장 유망한 후보이며, 격자기반 암호에서 가장 성능 부하가 큰 부분은 다항식 곱셈임. 그러므로 진행중인 연구들은 향후 양자 컴퓨터가 사용화 되었을때에도 안전한 암호 알고리즘 사용에 도움을 줄 것으로 기대됨

▶ 서석충 교수는 국가보안기술연구소와 활발하게 교류하며, Metamorphic Testing 방법을 통한 국내 알고리즘의 검증 방법과 적용하기 위한 프레임 워크를 설계하고 적용하고 있음. 암호모듈 검증제도인 CMVP에서 CAVP 구현적합성 검사의 취약점이 발견된 다수의 경우가 존재하므로, 이러한 취약점을 보완하기 위해 Metamorphic Testing를 통한 검증대상 암호알고리즘의 연구가 활발히 진행 중에 있음. 결과적으로 Metamophic Testing 방법을 통해 기존 KISA의 소스코드에서 취약점을 발견하는 결과를 성취하였음

▶ 김종성 교수는 디지털 포렌식 수사 관점에서 안티포렌식 대응 기법을 연구하고 도구화 하는 연구를 진행하고 있음. 자체 평가 기간 동안 지금까지 분석되지 않은 애플리케이션을 70 여종 분석 하였으며 이러한 결과를 기반으로 국제 논문지 4편, 국내 논문지 2편, 국내 학술대회 2편의 성과를 내었으며 이 외 논문들을 심사 받고 있음. 이 외에도 안전한 초연결사회를 위해 다양한 랜섬웨어 10종, 은닉 및 암호화 애플리케이션 4종을 추가로 분석하였음. 암호 프로세스를 분석하고 그 결과를 기반으로 원본 데이터의 획득 방안을 연구하였으며, 다양한 결과들을 통해 디지털 포렌식 수사에 도움을 줄 수 있을것으로 기대됨

3. 참여교수의 연구의 국제화 현황

① 국제적 학술활동 참여 실적 및 현황

▶ 한동국 교수는 The 23rd Annual International Conference on information Security and Cryptology (ICISC) 국제 학술대회의 Program committee로 활동함

▶ 한동국 교수는 Cryptographic Hardware and Embedded Systems (CHES) 국제 학술대회의 Program committee로 활동하함

▶ 한동국 교수는 The 24th Annual International Conference on information Security and Cryptology (ICISC) 국제 학술대회의 Program committee로 활동함

② 국제 공동연구 실적

<표 3-6> 최근 1년간 국제 공동연구 실적

연번	공동연구 참여자		상대국/소속기관	국제 공동연구 실적	DOI 번호/ISBN 등 관련 인터넷 link 주소
	교육연구단 참여교수	국외 공동연구자			
1	한동국	Dirmanto Jap, Shivam Bhasin	Singaport / Nanyang Technological University	3.367의 IF를 갖는 IEEE Access에 'Non-Profiled Side-Channel Attack Based on Deep Learning Using Picture Trace' 논문을 게재하함. 본 논문은 부채널 파형을 1차원 수열 데이터가 아닌 2차원의 그림 데이터로 보고 이를 이용한 신규 부채널 공격 기법을 제안함	10.1109/ACCESS.2021.3055833
2	이옥연	David Kim	United States of America / Georgia State University	국민대, 순천향대, 조지아 주립대학 간 화상으로 비대면 연합 세미나를 진행하여 최신 보안기술을 교류하였음	www.youtube.com/watch?v=9ELAb-ORn28

③ 외국 대학 및 연구기관과의 연구자 교류 실적 및 계획

▶ IoT 장비 펌웨어 보안성 검증 및 기술 개발

■ 이옥연 교수팀은 ㈜이와이엘, 플로리다 주립대학교 FICS와 국제 공동연구 'IoT 장비 펌웨어 보안성 검증 및 기술 개발' 을 2108년 6월 1일부터 2020년 12월 31일까지 수행함

■ 본 연구는 IoT 장비의 펌웨어 보안성 검증 기술개발을 위해 펌웨어, 하드웨어, 통신채널, 서비스와 같은 서로 다른 4개의 계층에서 새로운 IoT 보안성 검증 프레임워크의 개발 및 보안성 검증을 수행하고 보안 IoT ASIC 칩을 개발하여 취약점 검증 개념을 증명함

▶ 이옥연 교수팀은 국제 공동연구 '5G와 클라우드 융합환경에서의 안전한 UTM 서비스를 위한 보안기술 연구 및 인력 양성' 을 통해 22년 4월까지 5G 융합환경에서의 보안과 관련된 4편 이상의 SCI급 논문 출판 예정임

■ 참여연구원 장찬국은 UTM UAV 단말과 5G 엣지 클라우드 응용 서버 간 End-to-End 보안 연구 및 UTM UAV 단말과 5G 엣지 클라우드 응용 서버에서의 보안 가용성에 관해 연구 중이며 해당 주제로 SCI 급 논문 1편 이상 작성 예정임

■ 참여연구원 김현기는 UTM 내 UAV의 보안 파라미터용 데이터를 딥러닝 기반으로 생성하는 방법과 딥러닝 기반 UTM 내에서 사용하는 보안 파라미터용 데이터 탐지 연구를 진행하고 있으며 해당 연구주제로 SCI 급 논문 1편 이상 작성 예정임

■ 참여연구원 위한샘은 UTM 5G MEC 환경에서 UAV용 기기 인증서 기반 인증 시스템에 관한 연구와 UAV 중요 정보 관리를 위한 블랙박스 설계에 대해 연구를 진행하고 있으며 해당 연구주제로 SCI 급 논문 1편 이상 작성 예정임

Ⅳ 4단계 BK21 교육연구단(팀) 관련 언론보도 리스트

교육연구단(팀)명	안전한 초연결사회를 위한 문제해결형 정보보안 교육연구단
교육연구단(팀)장명	이 옥 연 교수

연번	구분	언론사명 /수상기관 등	보도일자/ 수상일자 등	제목/ 수상명 등	관련 URL
		주요내용 (200자이내)			
1	성과	연합뉴스 외 7건	20.10.15-11.20	인천항만공사, '제1회 인천국제해양포럼' 기획위원회 출범 外	http://www.newsway.co.kr/news/view?tp=1&ud=2020072215395486612 https://www.yna.co.kr/view/AKR20201015078300065?input=1195m http://dongascience.donga.com/news.php?idx=32551 https://www.yna.co.kr/view/AKR20201103078000065?input=1195m http://www.busan.com/view/busan/view.php?code=2020111019422716949 http://www.viva100.com/main/view.php?key=20201110010002800 http://www.joongboo.com/news/articleView.html?idxno=363455155 https://www.yna.co.kr/view/AKR20201116142800065?input=1195m http://www.obsnews.co.kr/news/articleView.html?idxno=1241628
		인천항만공사(IPA, 사장 최준욱)는 해양수산부와 인천시가 공동 주최하고 인천항만공사, 연합뉴스가 주관해 오는 11월 19일~20일 일정으로 개최 예정인 '제1회 인천국제해양포럼(IIOF 2020)' 기획위원회가 22일 출범했다.			
2	성과	연합뉴스 외 22건	21.06.06-07	해양/수중IoT국제표준화 준비그룹 의장에 박수현 교수	https://www.yna.co.kr/view/AKR20210606014000017 http://www.busan.com/view/busan/view.php?code=2021060609332941494 https://mobile.newsis.com/view.html?ar_id=NISX20210606_0001466360 http://it.chosun.com/site/data/html_dir/2021/06/06/2021060600195.html https://www.digitaltoday.co.kr/news/articleView.html?idxno=404617 https://news.mt.co.kr/mtview.php?no=2021060610032389495 https://www.aitimes.kr/news/articleView.html?idxno=21241 https://www.koit.co.kr/news/articleView.html?idxno=85388 https://www.dongascience.com/news.php?idx=47070 https://www.edaily.co.kr/news/read?newsId=01489126629079096&mediaCodeNo=257 https://www.metroseoul.co.kr/articl

					e/20210606500093 http://m.ddaily.co.kr/m/m_article/?no=215592 http://www.inews24.com/view/1373558 https://www.datanet.co.kr/news/articleView.html?idxno=160318 https://www.etnews.com/20210606000031 https://www.itbiznews.com/news/articleView.html?idxno=39316 https://cm.asiae.co.kr/ampview.htm?no=2021060614070295094 https://www.asiaa.co.kr/news/articleView.html?idxno=41623 https://www.newstomato.com/ReadNews.aspx?no=1049649 https://www.hankyung.com/it/article/2021060691181 https://www.asiatime.co.kr/article/20210606500094?1=1 https://www.hellodd.com/news/articleView.html?idxno=93007 https://www.sedaily.com/NewsView/22NJ5QUO3X/GK0509 http://www.dt.co.kr/contents.html?article_no=2021060702102119807001
		과학기술정보통신부 국립전파연구원은 'ISO/IEC JTC1/SC41' 국제표준화 회의에서 해양/수중 사물인터넷(IoT) 분야 작업반을 신설했다고 6일 밝혔다. 작업반 의장으로는 박수현 국민대 교수가 선임됐다.			
3	수상	스마트경제 외 3건	20.11.27	국민대 학생들, 2020 암호분석경진대회 대상 수상	http://www.dailysmart.co.kr/news/articleView.html?idxno=36471 https://www.dhnews.co.kr/news/articleView.html?idxno=132396 http://www.veritas-a.com/news/articleView.html?idxno=347247 https://news.unn.net/news/articleView.html?idxno=500476
		2020년 국방암호기술특화센터에서 주최하고 777사령부에서 후원하여 열린 암호분석 경진대회에서 대상인 국방부장관상을 수상하였다.			