붙임 1

4단계 BK21사업 자체평가보고서(양식)
_산업 · 사회 문제 해결 분야 교육연구단

※ 해당양식은 자체평가보고서 참고용이며 반드시 따를 필요는 없으나, 사업기본계획 및 공고문에 따라 자체평가보고서는 교육연구단의 필수 지표, 영역별 계획대비 성과 등의 내용을 반드 시 포함해야 함

『4단계 BK21사업』 혁신인재양성사업(산업·사회 문제 해결 분야) 교육연구단 자체평가보고서

접수번호	-								
신청분야	산업 · 사회 문제 해결분야				단위	전국			
학술연구분야 분류코드	구분	관련분야		관련분야		관련분야			
		중분류	소분류	중분류	소분류	중분류	소분류		
	분류명	컴퓨터학	정보보호	수학	응용수학	전자/정보통신공학	정보통신		
	비중(%)	50%		30%		20%			
교육연구단명	국문) 안전한 초연결사회를 위한 문제해결형 정보보안 교육연구단								
	영문) Institute of Information Security Education for Secure Hyperconnected Society								
교육연구단장	소 속	국민대학교 금융정보보안학과							
	직 위	교수							
	성명 국문	이옥연		전화	[redacted]				
				팩스	[redacted]				
	성명 영문	Yi, Okyeon		이동전화	[redacted]				
				E-mail	[redacted]				
연차별 총 사업비 (백만원)	구분	1차년도 ('20.9~'21.2)	2차년도 ('21.3~'22.2)	3차년도 ('22.3~'23.2)	4차년도 ('23.3~'24.2)	5차년도 ('24.3~'25.2)	6차년도 ('25.3~'26.2)	7차년도 ('26.3~'27.2)	8차년도 ('27.3~'28.2)
	국고지원금	258,720	517,440	517,440	517,440	517,440	517,440	517,440	258,720
총 사업기간	2020.9.1.-2027.8.31.(84개월)								
자체평가 대상기간	2021.9.1.-2022.8.31.(12개월)								

본인은 관련 규정에 따라, 『4단계 BK21사업』 관련 법령, 귀 재단과의 협약에 따라 다음과 같이 자체평가보고서 및 자체평가결과보고서를 제출합니다.

2022년 9월 28일

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) 기간에 수립된 정보보안 교육체계를 지속적으로 유지 및 개선하여 정보보안을 선도하는 전문가 양성에 힘쓰고 있음
■ 2단계(2022~2024) 기간에서의 목표를 정보보안 협력체계 강화로 선정하여, 이를 위해 산업계 전문가를 초청한 교육과정을 개설하였으며, 대외 협력을 위한 재학생의 인턴파견을 진행함
■ 자체평가 대상 기간(2021.9.1.~2022.8.31.)동안 국내 금융보안원과 MicroChip社의 전문가를 초청하여 학부 및 대학원 수업을 개설하여 금융권에서 활용되는 최신 보안 기술과 임베디드 장비에 대한 교육과정 운영중
■ 국제공동연구를 위해 박사과정 3명의 미국 Georgia State University에서 협업을 위한 파견 근무를 수행하였음
■ 교육연구단의 참여교수들은 교과과정 외에도 운영하는 랩을 통해 통신 보안, 디바이스 보안, 암호기술, AI 응용 분야에 다양한 기관 및 업체와의 협력 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">▶ 연구소, 산업계의 전문가와 함께하는 교육과정 및 정보보안 실무과정을 운영하여 대외협력체계 강화하고 우수 인재 양성에 힘쓰고 있음
■ 참여교수인 이옥연, 유일선, 박수현 교수는 통신 분야의 5G / 6G와 수중통신 환경의 정보보안 구현, 초연결 통신환경을 위한 정보보안 서비스 신뢰성 확보를 위한 교육을 추진함
✓ 참여교수 이옥연 교수는 국내 2개 대학(국민대학교, 순천향대학교), 해외 1개(Georgia State University) 대학이 참여하는 국제 공동연구를 수행하였음
✓ 참여교수 유일선 교수는 오세아니아 최정상급 명문대 보안관련 연구센터 혹은 연구실(웰런공 대학교 Institute of Cybersecurity and Cryptology)과 협력의향서를 체결하여 대외협력을 강화함
■ 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 추진함
✓ 참여교수 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
✓ 참여교수 서석충 교수는 정보보안 실무과정 및 대외협력체계 강화를 위해 여러 산업계 전문가를 초빙하여 특강 및 토론을 진행하는 산업체 세미나 과목을 개설하고 있음
■ 참여교수인 강주성, 염용진, 김동찬 교수는 안전한 양자내성암호의 개발 및 안전성 검</td></tr>
</table>

	증, 안전하고 효율적인 구현을 통한 보안제품의 개발기술 확보 및 보안 표준기술 이해를 위한 교육을 추진함 ✓ 참여교수 염용진 교수는 국제 표준화기구(ISO/IEC), 미국 국가표준기술연구원(NIST), IETF(Internet Engineering Task Force)에서의 보안기술 표준 및 관련 실무과정을 이해할 수 있도록 보안기술표준분석및구현 과목을 개설하고 융합교육을 실현함 ■ 참여교수인 최은미, 윤상민 교수는 데이터마이닝, 분산지능화 시스템, 인공지능 기술, 빅데이터 분석 및 적대적 공격 / 방어 시스템 개발기술 확보를 위한 교육을 추진함 ✓ 실제 사회에 활용되는 데이터를 기반으로 스스로 학습하고 이해할 수 있는 다양한 인공지능 모델을 개발함과 동시에 시스템에 적용할 수 있는 역량을 갖추도록 함 ▶ 교육과정 편찬 추진 외에도 우수 인재 양성을 위해 보안강연 및 워크숍 등을 진행하고 있음 ■ PQC 대전환시대 국내 기술 경쟁력 확보 전략 (2021.10.05.), 양자보안워크숍 ■ 부채널 분석 최신기술 동향 (2021.12.23.), 국립전파연구원 ■ 경량암호 및 양자내성암호 동향 소개(2021.10.25.), 삼성전자 무선사업부 ■ 외 9건의 강연 및 2건의 워크숍 진행 ▶ 선정평가 당시 본 연구단에서 제안한 연구 역량 향상을 위한 대학원생 지원을 계획하였음 ■ 결과 자체 평가 기간 내에 국제 저널 23건, 국내 저널 17건, 국제 학회 11건, 국내 학회 40건, 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 38건, 산업체 3건 총 41건의 연구를 진행하였음 ■ 총 41건의 연구를 통해 64.8억에 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 18건의 특허를 등록한 상태이며 23건이 출원된 상태임 ▶ 연구 결과를 기반으로 11건의 기술이전을 시행하였으며 다양한 매체를 통해 산업·사회에 대한 기여하였음 ▶ 총 6개의 보안관련 연구센터 혹은 연구실과 국제 공동연구 및 협력의향서를 체결하였으며, 국제 공동연구 및 연구자 교류를 위한 파견근무를 진행함으로써 연구역량의 확대를 진행하고 있음
달성 성과 요약	▶ 세부목표 달성을 위해 연구소, 산업계의 전문가 초청하여 교육과정을 개설하고 국내·외 보안관련 연구센터 혹은 연구실과 협력하여 해외 인턴파견, 협력의향서 체결 등 대외협력 강화함 ▶ 현재 금융보안원, MicroChip社의 전문가를 초청하여 융합 강좌를 개설하고 정보보안 관련 실무교육을 수행함 ▶ 박사과정 3명이 미국 Georgia State University 파견되어 국제공동연구를 수행함 ▶ 다양한 융합교육 및 랩별 심화 연구를 통해 다양한 연구성과를 내었음 ▶ 자체평가 대상 기간(2021.9.1.~2022.8.31.)동안 국제 저널 23건, 국내 저널 17건, 국제 학회 11건, 국내 학회 40건, 특허 등록 18건, 특허 출원 23건, 기술이전 11건, 연구비 수주 41건, 국내외 수상 13건, 강연 12건, 워크숍 2건의 실적을 달성하였음 ▶ 해당 기간 동안 석사 19명, 박사 8명을 확보하였으며, 석사 졸업생 7명, 박사 졸업생 3명을 배출하였음 ▶ 정보보안 분야에서 다양한 국내·외 대외 협력 연구를 수행하고 있는 유일선 교수를 신규 임용하여 대외협력체계를 강화함

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

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

✓ 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 신청학과 소속 전체 교수 및 참여연구진

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

신청학과(부)	기준 학기	전체교수 수			참여교수 수		
		전임	겸임	계	전임	겸임	계
금융정보보안학과	2021년 2학기	10	2	12	10	-	10
	2022년 1학기	11	2	13	11	-	11

<표 1-2> 최근 1년간 교육연구단 대학원 학과(부) 소속 전임/겸임 교수 변동 내역

연번	성명	변동 학기	전출/전입	변동 사유	비고
1	유일선	2022년 1학기	전입	신규 임용	

<표 1-3> 교육연구단 참여교수 지도학생 현황 (단위: 명, %)

신청학과(부)	기준 학기	대학원생 수											
		석사			박사			석·박사 통합			계		
		전체	참여	참여비율(%)	전체	참여	참여비율(%)	전체	참여	참여비율(%)	전체	참여	참여비율(%)
금융정보보안학과	2021년 2학기	25	24	96%	24	11	45.8%	3	3	100%	52	38	73%
	2022년 1학기	27	26	96.3%	25	10	40%	3	3	100%	55	39	70.9%
참여교수 대 참여학생 비율		1 : 3.8											

▶ 본 교육연구단 대학원은 22년 1학기 전임 교원 1명을 추가 임용하여 총 11명의 교수진이 되었음
▶ 본 교육연구단 대학원은 21년 2학기 석사 23명, 박사 17명, 석·박사 통합 3명 재학 중이었으며, 전체 참여비율 73%를 달성하였음
▶ 본 교육연구단 대학원은 22년 1학기 석사 27명, 박사 15명, 석·박사 통합 3명 재학 중이었으며, 전체 참여비율 70.9%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(2021.9.1.~2022.8.31.)동안 신청서에 작성된 37개의 교과 구성 중 9개 교과를 운영하였으며, 이는 전체 교과 구성 중 약 25%를 달성한 것임

✓ 전 년도 평가 대상 기간(2020.91.~2021.8.31.)동안 에는 11개 교과를 운영하였으며, 이 중 2가지 교과만 올해와 중복됨

■ 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

■ 계획된 우수 신임교원을 충원하기 위해 노력하였으며, 1명의 신규 전임 교원을 유치하는 성과를 내었음

■ 자체평가 기간 내에 국제 저널 23건, 국내 저널 17건, 국제 학회 11건, 국내 학회 40건, 수상 13건을 달성하였음

■ 자체평가 기간 내에 정부 38건, 산업체 3건 총 31건의 연구를 진행하였음

■ 자체평가 기간 내에 선정평가 보고서 작성대비 약 1.3배의 연구를 수주하는 성과를 내었음

▶ 코로나19(COVID-19)로 인해 국제적 교류는 미진하였으나, 작년 대비 산학협력은 확대할 수 있게 되었음

■ 국제적 교류가 미진하기는 하였으나, 신규 교원 충원을 통해 작년보다 확대에는 성공하였음

II 교육역량 영역

□ 교육역량 대표 우수성과

▶ 자체평가 대상 기간 내 국제 저널 23편, 국내 저널 17편, 국제 학회 11편, 국내 학회 40편의 논문 발표, 수상 13건, 특허 (등록 18건/출원 23건) 등의 성과를 냄

▶ 국제 저널

- “Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-Based Profiling”, JeaSeung Han, TaeHo Lee, JiHoon Kwon, JooHee Lee, Il-Ju Kim, JiHoon Cho, Dong-Guk Han, and Bo-Yeon Sim, IEEE ACCESS. (SCIE, I.F=3.367)
- “Profiling Attack against RSA Key Generation Based on a Euclidean Algorithm”, Sadiel de la Fe, Han-Byeol Park, Bo-Yeon Sim, Dong-Guk Han, and Carles Ferrer, MDPI Information. (SCOPUS)
- “Improved Correlation Power Analysis on Bitslice Block Ciphers”, JeaSeung Han, Yeon-Jae Kim, Soo-Jin Kim, Bo-Yeon Sim, and Dong-Guk Han, IEEE ACCESS. (SCIE, I.F=3.367)
- “Deep-Learning-Based Side-Channel Analysis of Block Cipher PIPO With Bitslice Implementation”, Ji-Eun Woo, Jaeseung Han, and Dong-Guk Han, IEEE ACCESS. (SCIE, I.F=3.367)
- “Single-Byte Error-Based Practical Differential Fault Attack on Bit-Sliced Lightweight Block Cipher PIPO”, Seonghuuck Lim, Jaeseung Han, and Dong-Guk Han, IEEE ACCESS. (SCIE, I.F=3.367)
- “Experimental evaluation of differential fault attack on lightweight block cipher PIPO”, Seonghuuck Lim, and Dong-Guk Han, IET Information Security. (SCIE, I.F=1.371)
- “Novel Shuffling Countermeasure for Advanced Encryption Standard (AES) against Profiled Attack in Mobile Multimedia Services”, JongHyeok Lee, Jiyoon Kim, and Dong-Guk Han, Wireless Communications and Mobile Computing. (SCIE, I.F=2.146)
- “Secure and Optimal Secret Sharing Scheme for Color Images”, K.Shankar, David Taniar, Eunmok Yang, Okyeon Yi, Mathematics (SCIE, IF = 2.84)
- “Convolution Neural Network-Based Sensitive Security Parameter Identification and Analysis”, Hyunki Kim, Donghyun Kim, Okyeon Yi, Hindawi WCMC (SCIE, IF = 2.146)
- “Analysis of Radioactive Decay Based Entropy Generator in the IoT Environments“, Taewan Kim, Seyoon Lee, Seunghwan Yun, Jongbum Kim, Okyeon Yi, 2022 한국정보보호학회 WISA
- “Telecommunication for Quantum Computer”, Seyoon Lee, Taewan Kim, Changuk Jang, Okyeon Yi, 2022 한국정보보호학회 WISA (포스터)
- “Fast Implementation of SHA-3 in GPU Environment”, Hojin Choi and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “High-Speed Fault Attack Resistant Implementation of PIPO Block Cipher on ARM Cortex-A”, JinGyo Song, YoungBeom Kim and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “CRYSTALS-Dilithium on ARMv8”, YoungBeom Kim, JinGyo Song and Seog Chung Seo, Security and Communication Networks (SCIE, IF = 1.791)
- “Designing a New XTS-AES Parallel Optimization Implementation Technique for Fast File Encryption”, SangWoo An and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “Efficient Implementation of AES-CTR and AES-ECB on GPUs with Applications for High-speed FrodoKEM and Exhaustive Key Search”, Wai-Kong Lee, HwaJeong Seo, Seog Chung Seo, and Seong

Oun Hwang, IEEE Transactions on Circuits and System II: Express Briefs (SCIE, IF = 3.292)

- “Accelerating Falcon on ARMv8”, YoungBeom Kim, JinGyo Song and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “Efficient Parallel Implementations of PIPO Block Cipher on CPU and GPU”, Hojin Choi and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “Parallel Implementation of CRYSTALS-Dilithium for Effective Signing and Verification in Autonomous Driving Environment”, Seog Chung Seo, and SangWoo An, ICT Express (SCIE, IF = 4.754)
- “Optimized Implementation of PIPO Block Cipher on 32-bit ARM and RISC-V Processors”, YoungBeom Kim and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things”, Delphin Raj Kesari Mary, Eunbi Ko, Seung-Geun Kim, Sun-Ho Yum, Soo-Young Shin, Soo-Hyun Park, Sensors (SCI, I.F 3.576)
- “A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application”, Hangi Kim, Yongjin Jeon, Giyoon Kim, Jongsung Kim, Boyeon Sim, Dongguk Han, Hwajeong Seo, Seonggyeom Kim, Seokhie Hong, Jaechul Sung, Deukjo Hong, IEEE ACCESS (SCIE, I.F 3.745)
- “Differential uniformity and linearity of S-boxes by multiplicative complexity”, Yongjin Jeon, Seungjun Baek, Hangi Kim, Giyoon Kim, Jongsung Kim, Cryptography and Communication (SCIE, I.F 1.73)
- “Speeding Up LAT: Generating a Linear Approximation Table Using a Bitsliced Implementation”, Giyoon Kim, Yongjin Jeon, Jongsung Kim, IEEE ACCESS (SCIE, I.F 3.745)
- “Quantum cryptanalysis of the full AES-256-based Davies-Meyer, Hirose and MJH hash functions”, Seungjun Baek, Sehee Cho, Jongsung Kim, Quantum Information Processing (SCIE, I.F 2.349)
- “A Study on Data Acquisition based on the Huawei Smartphone Backup Protocol”, Myungseo Park, Sehoon Lee, Okyeon Yi, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, I.F 2.395)
- “A Reused Key Attack on an Encrypted Mobile App Database: Case Study on KakaoTalk and ProtonMail”, Uk Hur, Myungseo Park, Jongsung Kim, Journal of Information Security and Applications (SCIE, I.F 3.872)
- “Forensic analysis of note and journal applications”, Sumin Shin, Giyoon Kim, Soram Kim, JongsungKim, Forensic Science International: Digital Investigation (SCIE, I.F 2.395)
- “Methods for recovering deleted data from the Realm database: Case study on Minitalk and Xabber”, Soram Kim, Giyoon Kim, Sumin Shin, Byungchul Youn, Jian Song, Insoo Lee, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, I.F 2.395)
- “Methods for decrypting the data encrypted by the latest Samsung smartphone backup programs in Windows and macOS” Soojin Kang, Giyoon Kim, Myungseo Park, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, I.F 2.395)
- “A study on LG content lock and data acquisition from apps based on content lock function”, Giyoon Kim, Myungseo Park, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, I.F 2.395)
- “Improved See-In-The-Middle Attacks on AES”, Jonghyun Park, Hangi Kim, Jongsung Kim, ICISC 2021, LNCS 13218, pp. 271-279, Springer, 2022.
- “A Study on the New Saturnin S-box with Improved Implementation Efficiency“, Hangi Kim, Jongsung Kim, Platform Technology Letters
- “Quantum cryptanalysis of the full AES-256-based Davies-Meyer, Hirose and MJH hash functions“,

Seungjun Baek, Sehee Cho, Jongsung Kim, Quantum Information Processing (I.F 2.349)

- "Speeding Up LAT: Generating a Linear Approximation Table Using a Bitsliced Implementation", Giyoon Kim, Yongjin Jeon, Jongsung Kim, IEEE ACCESS (I.F 3.745), Vol 10
- "Differential uniformity and linearity of S-boxes by multiplicative complexity", Yongjin Jeon, Seungjun Baek, Hangi Kim, Giyoon Kim, Jongsung Kim, Cryptography and Communication (I.F 1.73)
- "Optimizing High-Speed Mobile Networks with Smart Collaborative Theory", Fei Song, Letian Li, Ilsun You, Shui Yu, Hongke Zhang, IEEE ACCESS (SCIE, IF=3.476)
- "A Secrecy Transmission Protocol with Energy Harvesting for Federated Learning", Ping Xie, Fan Li, Ilsun You, Ling Xing, Honghai Wu, Huahong Ma, MDPI Sensors (SCIE, IF=4.35)
- "Federated intelligence of anomaly detection agent in IoTMD-enabled Diabetes Management Control System", Philip Virgil Astillo, Daniel Gerbi Duguma, Hoonyong Park, Jiyoon Kim, bonam Kim, IlsunYou, Future Generation Computer Systems. (SCIE, IF=7.187)
- "Session Management for Security Systems in 5G Standalone Network", Seongmin Park, Sungmoon Kwon, Youngkwon Park, Dowon Kim, Ilsun You, IEEE ACCESS (SCIE, IF=3.476)

▶ 국내 저널

- "극한지 환경에서 무인기를 이용한 MQTT 기반 극한지 생물용 바이오로거 데이터 원격 회수 시스템 구현", 이정국, 염선호, 이진영, 황아리, 채지윤, 임지영, 임용곤, 최유성, 박수현, 전자공학회논문지 2022년 8월호
- "Gohr의 Speck32/64 신경 망 구분자에 대한 분석과 Simon32/64에의 응용", 성효은, 유현도, 염용진, 강주성, 정보보호학회논문지 2022년 4월 호
- "블록암호 PRESENT에 대한 향상된 SITM 공격", 박종현, 김한기, 김종성, 정보보호학회논문지, 32권, 2호
- "양자 컴퓨팅 환경에서의 해시함수 충돌쌍 공격 동향", 백승준, 조세희, 김종성, 정보보호학회지 2022년 2월 호
- "Vault 앱의 데이터 암호화 알고리즘 및 은닉 알고리즘 분석", 최용철, 김기윤, 김종성, 디지털포렌식연구, 15권 4호, 2021
- "양자 컴퓨팅 환경에서의 Ascon-Hash에 대한 Free-Start 충돌 공격", 조세희, 백승준, 김종성, 정보보호학회논문지, 32권, 4호
- "GIFT-128에 대한 SITM 공격: NIST 경량암호 최종 후보 GIFT-COFB 적용 방안 연구", 박종현, 김한기, 김종성, 정보보호학회논문지, 32권, 4호
- "AND 연산자 축적을 통한 경량 S-boxes 생성 방법", 전용진, 김종성, 정보보호학회논문지, 32권, 3호
- "안드로이드 환경에서의 지도 애플리케이션 아티팩트 분석 및 복호화 방안 연구", 박귀은, 강수진, 김종성, 디지털포렌식연구, 16권 2호
- "안드로이드 기반 클라우드 스토리지 앱 크리덴셜 활용 및 아티팩트 분석", 최용철, 김기윤, 김종성, 디지털포렌식연구, 16권 2호

▶ 국제 학회

- "Deep Learning-based Side-Channel Analysis on PIPO", Ji-Eun Woo, Jaeseung Han, Yeon-Jae Kim, Hye-Won Mun, SeongHyuck Lim, Tae-Ho Lee, Seong-Hyun An, Soo-Jin Kim, and Dong-Guk Han, The 24th Annual International Conference on Information Security and Cryptology (ICISC 2021)
- "Differential Fault Attack on Lightweight Block Chiper PIPO", SeongHyuck Lim, Jaeseung Han, Tae-Ho Lee, and Dong-Guk Han, The 24th Annual International Conference on Information Security and

Cryptology (ICISC 2021)

- “Illegal Photo Shoot Detection Method Using Operating Frequency of Smartphone Camera”, Seong-Hyun An, Ji-Woo, Lee, and Dong-Guk Han, The 23th World Conference on Information Security Applications (WISA 2022)
- “Analysis of 5G AKA vulnerabilities through 5G Simulator”, SeoWoo Jung, Seunghwan Yun, Okyeon Yi, IEEE Region 10 Symp, 2022 ICFICE
- “Efficient parallel implementation methods of LSH-512 utilizing SIMD AVX-512”, Hojin Choi and Seog Chung Seo, The 23rd World Conference on Information Security Applications (WISA 2022 Poster Section)
- “MFT: Metamorphic Fuzz Testing for Efficient Correctness Validation of Cryptographic Implementation”, HyungJoon Yoon, YoungBeom Kim, Yongryeol Choi and Seog Chung Seo, The 23rd World Conference on Information Security Applications (WISA 2022 Poster Section)
- “Metamorphic Testing on NIST LWC Finalists”, Yongryeol Choi, YoungBeom Kim and Seog Chung Seo, The 23rd World Conference on Information Security Applications (WISA 2022 Poster Section)
- “MUD for Infusion Pumps: An Attempt to Reduce Network-based Attacks”, Daniel Gerbi Duguma, Gunwoo Kim, Bonam Kim, Ilsun You, The 23st World Conference on Information Security Applications (WISA 2022)

▶ 국내 학회

- “효율적인 교차 디바이스 부채널 분석을 위한 프로파일링 디바이스 선택 방법”, 안성현, 임성혁, 이종혁, 한동국, 2021 한국군사과학기술학회 종합학술대회
- “경량암호 PIPO에 대한 신경망 및 라벨 설정에 따른 프로파일링 부채널 분석”, 김수진, 우지은, 김연재, 안성현, 문혜원, 한동국, 2021 한국정보보호학회 동계학술대회
- “딥러닝 기반 비프로파일링 이차 부채널 분석 성능 향상 기법에 관한 연구”, 임성혁, 문혜원, 한동국, 2021 한국정보보호학회 동계학술대회
- “딥러닝을 활용한 스마트폰 카메라 불법 촬영 탐지 방안”, 안성현, 이현호, 우지은, 김연재, 한동국, 2021 한국정보보호학회 동계학술대회
- “AES CTR 모드에 대한 향상된 전력분석 기법”, 한재승, 한동국, 2022 한국정보보호학회 하계학술대회
- “ARIA 암호 알고리즘에의 전력 글리치 다중 오류 주입 공격”, 이종혁, 임성혁, 문혜원, 한동국, 2022 한국정보보호학회 하계학술대회
- “NIST PQC Round 3 격자 기반 PKE KEM의 소프트웨어 하드웨어 구현에 대한 부채널 분석 동향”, 김수진, 한동국, 2022 한국정보보호학회 하계학술대회
- “글로벌 IT 보안 기업 CENSUS 사 Masked AES software library에 대한 잔여 1차 부채널 취약점 분석”, 김연재, 한동국, 2022 한국정보보호학회 하계학술대회
- “이종 디바이스 환경에서의 비지도 도메인 적응을 이용한 신규 프로파일링 부채널 분석”, 우지은, 한동국, 2022 한국정보보호학회 하계학술대회
- “장치의 열 방출량을 이용한 오류 주입 공격 성공률 향상 방안 연구”, 문혜원, 지재덕, 한동국, 2022 한국정보보호학회 하계학술대회
- “TCP 통신 환경 암호장비에 대한 최적화 요소 분석”, 한주홍, 이옥연, 2021 한국정보보호학회 동계학술대회
- “서버에서의 양자내성암호 기반 통합 암호 체계 제안”, 이세윤, 김태완, 이옥연, 2021 한국정보보호학회 동계학술대회
- “안드로이드 애플리케이션 인증방식의 취약점 분석 및 동향”, 윤혜진, 이옥연, 2021 한국정보보호학회 동계학술대회

- “난수발생기에 따른 UDM 인증 벡터 생성 속도 분석”, 김태완, 이옥연, 2021 한국정보보호학회 동계학술대회
- “양자 암호모듈 기반 드론 식별 및 정보 제공 기술 구현에 대한 연구”, 정서우, 윤승환, 이옥연, 2021 한국정보보호학회 동계학술대회
- “BB84 프로토콜 분석 및 양자 키 분배 표준화 동향”, 김형엽, 이옥연, 2021 한국정보보호학회 동계학술대회
- “UTM 내 드론에서 사용 가능한 보안 파라미터 딥러닝 기반 탐지”, 김현기, 김태완, 이옥연, 2022 한국인터넷정보학회 춘계학술발표대회
- “검증필 암호모듈 기반 드론 식별 체계 연구“, 김태완, 이세윤, 윤승환, 이옥연, 2022 한국정보보호호학회 하계학술대회
- “상용 드론의 군 도입을 위한 검증필 암호모듈 상호호환 운용 환경 요구사항”, 정서우, 김현기, 이옥연, 2022 한국정보보호호학회 하계학술대회
- “드론 비행 데이터 저장 방법에 대한 연구”, 김형엽, 김태완, 이재훈, 이옥연, 2022 한국정보보호호학회 하계학술대회
- “오프라인 환경의 디바이스에 인증을 위한 AHS 프로토콜 제안“, 윤혜진, 장찬국, 이재훈, 이옥연, 2022 한국정보보호학회 하계학술대회
- “한국형 UTM 내부 양자 보안 아키텍처 설계”, 이세윤, 김태완, 위한샘, 이옥연, 2022 한국정보보호학회 하계학술대회
- “ARM Cortex-A 환경에서 Falcon Round 3의 FFT 곱셈 최적화 연구”, 송진교, 김영범, 서석충, 2021 한국정보보호학회 동계학술대회
- “키 유도함수에 대한 Metamorphic Testing 설계”, 김영범, 송진교, 서석충, 2021 한국정보보호학회 동계학술대회
- “GPU 환경에서의 16-bit 자료형을 활용한 PIPO 암호 알고리즘 최적화 방안”, 최호진, 서석충, 2021 한국정보보호학회 동계학술대회
- “CUDA GPU 환경에서의 Falcon Fast Fourier Sampling 연산을 위한 이중 재귀함수의 반복문 대체 기법”, 안상우, 서석충, 2021 한국정보보호학회 동계학술대회
- “블록체인의 구조적 문제 및 암호학적 취약점에 대한 동향 조사”, 김동천, 김영범, 서석충, 2021 한국정보보호학회 하계학술대회
- “PQC-DSA 기반 블록체인 기술 동향 조사”, 김동천, 서석충, 2022 한국통신학회 동계종합학술발표회
- “자율주행환경에서 PQC 적용분석을 위한 V2Verifier 분석 및 확장”, 김영범, 서석충, 2022 한국통신학회 동계종합학술발표회
- “CPU 환경에서 최신 경량 암호 GIFT-COFB의 최적화 및 속도 개선과 구현”, 최용렬, 김영범, 서석충, 2022 한국통신학회 동계종합학술발표회
- “CPU 환경에서의 AVX-512를 활용한 블록 암호 알고리즘 PIPO 벤치마킹”, 최호진, 서석충, 2022 한국통신학회 동계종합학술발표회
- “NVIDIA GPU 환경에서 효율적인 병렬 작업 수행을 위한 더미 연산 구현 기법”, 안상우, 서석충, 2022 한국통신학회 동계종합학술발표회
- “SIMD AVX-512를 활용한 LEA 병렬 구현 방안”, 최호진, 서석충, 2022 한국정보보호학회 하계학술대회
- “PQC 마이그레이션을 위한 고려사항 분석 및 최신연구 동향 조사”, 강혜리, 김영범, 서석충, 2022 한국정보보호학회 하계학술대회
- “격자기반 다항식 곱셈 최적화 구현 동향”, 김영범, 서석충, 2022 한국정보보호학회 하계학술대회
- “IoT 환경을 위한 경량암호 최적화 동향 분석”, 최용렬, 김영범, 서석충, 2022 한국정보보호학회 하계학술대회

■ “자동차 OTA(Over The Air) 업데이트 보안 동향 분석”, 신동현, 김영범, 서석충, 2022 한국정보보호학회 하계학술대회
■ “Patterson 디코딩 기반 Classic McEliece 키 복호 연산에 관한 연구”, 전창열, 김동찬, 2022 한국통신학회 동계학술대회
■ “유한체 상에서의 기약다항식 생성에 관한 연구”, 전창열, 최장혁, 김동찬, 2022 한국통신학회 동계학술대회
■ “유한체의 랜덤 순서 집합 생성 기법에 관한 연구”, 이제원, 전창열, 최장혁, 김동찬, 2022 한국통신학회 동계학술대회
■ “다항식 몫환 F_p[X]/<X^n-1>의 이산 푸리에 변환 기반 곱셈에 관한 연구”, 최장혁, 전창열, 김동찬, 2022 한국통신학회 동계학술대회
■ “유클리드 호제법과 이진 최대공약수 알고리듬을 이용한 최대공약수 고속 계산에 관한 연구”,김영효, 김민지, 이제원, 전창열, 김동찬, 2022 하계 통신학회 종합학술발표회
■ “다항식 몫환 F_p[X]〈X^n+1〉의 NTT 기반 곱셈 연산에 관한 연구”, 이제원, 김민지, 김영효, 전창열, 김동찬, 2022 하계 통신학회 종합학술발표회
■ “경량 암호 CHAM을 사용한 암호학적 난수발생기 GPU 병렬 구현”, 유현도, 강주성, 염용진, 2021 한국통신학회 추계종합 학술발표회
■ “MODBUS 프로토콜의 양자내성암호(PQC) 적용 방안에 관한 연구”, 김원일, 강주성, 염용진, 2021 한국통신학회 추계종합 학술발표회
■ “이미지 센서 기반 난수발생기의 잡음원에 적용 가능한 헬스테스트 설계”, 유현도, 강주성, 염용진, 2021 한국통신학회 동계종합 학술발표회
■ “그래프 기반 PDF 암호시스템 개선 방법에 관한 연구”, 류지은, 강주성, 염용진, 2021 한국통신학회 동계종합 학술발표회
■ “블록암호 SIMECK에 대한 양자회로 설계 및 구현”, 노준영, 백승준, 박종현, 조세희, 김종성, 정보보호학회 동계 학술대회
■ “NIST 경량 해시함수 Ascon-Hash의 양자 충돌쌍 공격을 위한 MILP 모델 개발”, 조세희, 백승준, 김종성, 2022 한국인터넷정보학회 춘계학술발표대회
■ “GIFT-COFB 위조 공격”, 박종현, 김기윤, 김종성, 2022 한국인터넷정보학회 춘계학술발표대회
■ “DPAPI 기반 크리덴셜 위조를 통한 클라우드 데이터 획득 : Cisco Webex 및 Zoom에 대한 사례연구”, 허욱, 김기윤, 김종성, 2022 한국인터넷정보학회 춘계학술발표대회
■ “TMAP 애플리케이션의 사용자 위치 데이터 분석”, 박귀은, 강수진, 김종성, 2022 한국인터넷정보학회 춘계학술발표대회
■ “특정 환경을 위해 설계된 해시함수 및 블록암호 동향”, 조수정, 권주아, 서재원, 이수현, 임효은, 조세희, 박종현, 김종성, 한국정보보호학회 하계 학술대회
■ “S-box 확장구조 효율성 분석“, 전용진, 김종성, 한국인터넷정보학회 춘계학술발표대회
■ “디지털 포렌식 관점에서의 인공지능 활용 동향“, 이용진, 방수경, 박귀은, 김종성, 정보보호학회 하계 학술대회
■ “SNS 애플리케이션의 디지털 포렌식 동향“, 박세준, 원채은, 이민정, 김종성, 정보보호학회 하계 학술대회
■ “iOS 및 Android Vault 앱 암호화 알고리즘 분석 및 패스워드 복구 방안“, 최용철, 김기윤, 김종성, 디지털포렌식 하계 학술대회
■ “이음 5G에서 허위기지국 탐지 정확도를 향상하기 위한 연합 학습 시스템 연구”, 박훈용, 손대현, 김건우, 유일선, 2022 한국정보보호학회 하계학술대회(CISC-S’22)
■ “IoV 네트워크에서의 BAN 논리를 이용한 정형화 검증”, 오종민, 손대현, 김보남, 유일선, 2022 한국정보

보호학회 하계학술대회(CISC-S’22)

- “블록체인 기반의 스마트 HACCP 구축 사례 연구”, 김건우, 임아정, 김보남, 유일선, 2022 한국정보보호학회 하계학술대회(CISC-S’22)
- “5G 네트워크상에서 Braeken이 제안한 대칭키 기반의 5G-AKA 인증 프로토콜 BAN Logic 정형화 검증”, 손대현, 박훈용, 김보남, 유일선, 2022 한국융합보안학회 하계학술대회
- ” 웨어러블 디바이스 클라우드 프로토콜에서의 정형화 검증 “, 오종민, 김지윤, 김보남, 유일선, 2022 한국융합보안학회 하계학술대회
- ” 5G NSA 네트워크에서의 블록체인 기술 기반 키 관리를 위한 Lee-Ma 보안 프로토콜 취약점 분석 “, 김건우, 임아정, 김보남, 유일선, 한국융합보안학회 하계학술대회

▶ 수상

- 과학기술정보통신부장관 표창장
- 대한전자공학회 공로상
- 2021 국가암호 공모전 대상 1건, 우수상 1건, 장려상 1건, 특별상 1건 수상
- 2021 국가암호 경진대회 대상 1건, 최우수상 1건, 우수상 2건 수상
- 2021 한국정보보호학회 국제논문상
- 2021 한국정보보호학회 동계학술대회 우수논문상 1건, 정보보호학회장상 1건, 행정안전부 장관상 1건 수상
- 2021 한국디지털포렌식학회 KDS 챌린지 장려상
- 2021 한국통신학회 추계학술대회 우수논문상
- 2021 사이버 안보 논문 공모전 장려상
- 2021 국가 암호기술 전문인력 양성과정 우수상
- 2021 경량 PIPO 대칭키 암호 고속구현, SCA, 활용사례 경진대회 국가보안기술연구소 소장상
- 2022 한국인터넷정보학회 춘계학술발표대회 우수논문상
- 2022 한국통신학회 동계학술대회 우수논문상
- 2022 우수신진연구자 한국인터넷진흥원 원장상 수상
- 2022 한국멀티미디어학회 춘계학술대회 우수논문상
- 2022 한국정보보호학회 하계학술대회 정보보호학회장상
- 2022 한국정보보호학회 하계학술대회 행정안전부 장관상 수상
- 2022 WISA Best Poster Award 수상
- 2022 WISA Best Student Paper Award 수상
- 2022 HACK@SEC 2022 Winners 2nd 수상
- 2022 한국융합보안학회 하계학술대회 우수논문상

▶ 참여교수 교육대표실적

- 보안 강연
  - ✓ PQC 대전환시대 국내 기술 경쟁력 확보 전략 (2021.10.05.) 양자보안워크숍
  - ✓ 컴파일러 최적화 옵션은 부채널 분석에 아군인가? 적군인가? (2021.10.28.) 부채널정보분석 워크숍
  - ✓ PQC 전환 준비 – 인력양성 및 시험 평가 (2021.11.09.) KISA
  - ✓ 부채널 분석 최신기술 동향 (2021.12.23.) 국립전파연구원
  - ✓ IC 칩 해킹 및 복제 가능 시나리오 교육 (2022.01.21.) KISA
  - ✓ 부채널 분석 방지 기술 특강 (2022.05.18.) 국방과학연구소
  - ✓ 양자내성암호 최적화 구현 동향 소개(2021.10.14.), 한국암호포럼

✓ 경량암호 및 양자내성암호 동향 소개(2021.10.25.), 삼성전자 무선사업부
✓ 정보보호 전문가를 위한 암호교육(2022.03.23. ~ 2022.03.25.), 한국암호포럼
✓ 암호모듈검증 KCMVP 전문교육 온라인 과정 (2022.05.03.~2022.05.04.) 한국인터넷진흥원
✓ Key note: "IIMB-Lite: Lightweight Misbehavior Detection Approach for Insulin Infusion System", Ilsun You, Philip Virgil Astillo, ACM on ASIA Public-Key Cryptography
✓ 독립형 5G 인증과 보안 기술(2022.06.07.), 국민대

■ 워크숍
✓ 제 4회 부채널정보분석 워크숍 (2021.10.28.~2021.10.29.)
• 부채널정보분석 워크숍을 주관하여 개최함
✓ 제 5회 5G보안 워크숍 (2022.7.7.~2022.7.8.)
• 5G보안워크숍을 주관하여 개최함

▶ 국내특허
■ 차분 오류 공격 방법 및 장치 (등록)
■ 블록암호에 대한 상관전력 분석 방법 및 장치 (등록)
■ LAC에 대한 부채널 분석 장치 및 방법 (등록)
■ 오류 주입 공격 시스템 (등록)
■ 오류 주입 공격 장치 및 방법 (등록)
■ 전자서명 알고리즘의 부채널 분석 방법 및 그 장치 (등록)
■ 양자보안 통신장치 통합형 영상 감시 시스템 및 방법 (등록)
■ 양자보안 통신장치 통합형 지능형 교통신호 제어 시스템 및 방법 (등록)
■ 양자보안 통신장치 통합형 수배전반 보안 시스템 및 방법 (등록)
■ 양자보안 통신장치 통합형 PLC/HMI 제어 시스템 및 방법 (등록)
■ 양자보안 통신장치 통합형 자율이동체 이동기록 시스템 및 방법 (등록)
■ 양자보안 통신장치 통합형 자율이동체 식별 시스템 및 방법 (등록)
■ 비행체에서의 잡음원 도출 장치 및 방법 (등록 결정)
■ 양자 엔트로피 기반 일회용 양자 비밀번호 생성 장치 및 방법(출원)
■ 안티-인버전 함수를 이용한 화이트박스 암호 인코딩 장치 및 방법 (등록)
■ 미디어 파일에 대한 안티 포렌식 해제 장치 및 방법 (등록)
✓ 미디어 파일 은닉 기능에 대한 은닉 해제 방법에 대한 연구임
■ 경량 블록암호 PIPO에 대한 단일 바이트 오류 기반 신규 차분 오류 공격 (출원)
■ 경량 블록암호 PIPO에 대한 신규 딥러닝 기반 프로파일링 및 비프로파일링 부채널 분석 (출원)
■ 소프트웨어 동작 감지 창치 및 방법 (출원)
■ SHA-3 처리를 위한 그래픽 처리 장치 및 방법 (출원)
■ 기각 시퀀스 테이블을 이용한 기각 샘플링 병렬 최적화 장치, 방법 및 그 방법을 이용한 전자서명 및 암호화 연산 방법 (출원)
■ XTS 최적화를 위한 병렬 처리 장치 및 방법 (출원)
■ 이미지 센서 기반 난수발생기 헬스 테스트 장치 및 방법 (출원)
■ 일방향 함수를 이용한 암호 운영모드 기반의 화이트박스 암호화 방법 및 장치 (출원)
■ DLBN이 3 이상인 조건을 만족하는 확장 에스박스 및 이를 이용한 비트 연산 방법 (출원)
✓ DLBN이 3 이상인 조건을 만족하는 확장구조와 이를통한 확장 S-box를 개발한 특허임
■ FTS 색인데이터 기반의 삭제 채팅 메시지 복구 장치 및 방법 (출원)
✓ SQLite FTS 데이터베이스의 색인 데이터를 활용하여 삭제된 메시지를 복구하는 특허임

▶ 기술이전
- ■ 무인이동체 보안을 위한 암호장비의 설계 기술
- ■ 검증필암호모듈 KMULiB v2.1 기술
- ■ 화이트박스 암호화 기술
- ■ LEA 블록암호의 화이트박스 암호 구현 장치 및 방법외 특허 1건 통상실시권 이전

▶ 소프트웨어 등록
- ■ UHSDM(유에이치에스디엠)용 수중 가시광선 및 적외선 무선 통신 송신 출력 제어 프로그램 등록

▶ 국제 표준
- ■ SO/IEC JTC 1/SC 41 국제표준 총회에서 신설된 “해양/수중 IoT 및 디지털 트윈 어플리케이션” 작업반(WG; Working Group)인 WG 7 의장
  - ✓ 2021년 11월 제10차 SC41 국제표준 총회에서 WG 7 의장으로서 회의를 주도함
  - ✓ 2022년 2월 ‘WG 7 1st Open Workshop’ 개최
  - ✓ 2022년 4월 ‘SC41 Webinar on IoT and Digital Twin Standardization’에서 ‘Maritime IoT and Digital Twin’ 발표
  - ✓ 2022년 5월 제11차 SC41 국제표준 총회에서 WG 7 의장으로서 회의를 주도함

▶ 국내 표준
- ■ 과기정통부가 발간하는 ‘ICT 표준전략맵’ 작성에 참여하여 수중통신 기술의 국내외 표준화 전략 방향을 제시
  - ✓ 2021년 12월 ICT 표준화전략맵 Ver. 2022 발간

1. 교육과정 구성 및 운영

1.1 교육과정 구성 및 운영 현황과 계획

▶ 대학원 교육과정 구성 및 학사관리 운영계획
- ■ 공개키암호분석이론, 디지털포렌식개론, 무선보안특강, 보안구현개발방법론, 증명가능안전성론, 난수성분석론, 디지털포렌식특수연구, 보안기술표준분석및구현, 암호모듈평가및검증 과목을 개설해 운영하였으며, 이는 신청서 대비 약 25%의 실적 달성임
  - ✓ 해당 교과들은 다양한 교과 개설을 위해 작년 30% 실적과 최대한 겹치지 않도록 개설한 결과임
  - ✓ 4단계 BK21사업 이후 계획대비 교과 개설 실적은 50%를 달성하였음
- ■ 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·응용 분야로 교과목을 나누어 공통기초 과정부터 실용과정까지 단계별로 체계화된 교과과정을 구성함
- 현재 암호알고리즘, 해시함수와데이터인증, 정보보호프로토콜, 부채널공격대응론, 대칭키암호분석, 비즈니스정보통신, 이동통신보안, 증명가능안정성론, 융합보안특강, 보안기술표준분석및구현, 공개키암호분석이론, 디지털포렌식개론, 무선보안특강, 보안구현개발방법론, 난수성분석론, 디지털포렌식특수연구, 암호모듈평가및검증 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 18건, 특허 출원 23건, 기술이전 11건, 연구비 수주 41건, 국내외 수상 13건, 강연 12건, 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, 유일선 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, 정보보호프로토콜 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 기기 등의 디지털 기기에 대한 기본적인 이해를 위해 OS, 메모리, 저장공간 등의 전반적인 컴퓨터 이

론을 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(2021.9.1.~2022.8.31.)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

■ 기반이론 분야

✓ 김종성 교수는 디지털포렌식개론과목 개설을 통해 안티포렌식 기술에 대한 이해와 안티포렌식 기술을 우회하기 위한 안티안티포렌식 기술을 교육하고 실사례를 분석함으로써 원리를 교육함

✓ 서석충 교수는 보안구현개발방법론과목 개설을 통해 국가 및 공공기관에서 중요정보의 보호를 위해 사용되는 암호모듈의 시험 및 설계방법에 대해 학습하고, 암호모듈 검증제도(CMVP)의 정책적, 제도적 이해를 바탕으로 암호모듈의 시험요소(구현 정확성, 안전성 시험 등)에 대해 교육함

✓ 유일선 교수는 정보보호프로토콜과목 개설을 통해 정보보호 프로토콜의 기본 개념과 정형화를 검증하고 정보보호 프로토콜의 사례연구를 통해 정보보호 프로토콜의 핵심을 교육함

■ 핵심역량 분야

✓ 김동찬 교수는 공개키암호분석이론과목 개설을 통해 인수분해와 이산대수문제의 해를 찾는 알고리듬, 양자 연산을 이용한 암호 공격 기법, 주요 양자내성 암호 알고리즘과 공개키암호의 구조를 분석하고 안전성을 분석 방법을 교육함

✓ 이옥연 교수는 무선보안특강과목 개설을 통해 4G, 5G, 6G, TVWS, WiFi, 위성통신 등의 다양한 무선통신 기술을 학습하고, 각각의 통신에서 사용되는 정보보안 구조를 학습함으로써 관련된 암호 알고리즘과 정보보안 지식을 교육함

✓ 김종성 교수는 디지털포렌식특수연구과목 개설을 통해 최신 디지털포렌식 기술 동향을 학습하고, 크리덴셜 정보 활용 등 다양한 기법을 활용한 데이터 획득 방법을 교육함

■ 심화응용 분야

✓ 강주성 교수는 증명가능안전성론과목 개설을 통해 Shannon's Perfect Secrecy, 엔트로피, 블록암호의 의사난수성, 블록암호 운영모드의 안전성 분석, 해쉬함수의 안전성 분석, MAC의 안전성 등을 교육함

✓ 이옥연 교수는 암호모듈평가및검증과목 개설을 통해 CMVP에 대한 정책적, 제도적 이해를 바탕으로 암호모듈의 평가, 검증을 위한 기준과 관련된 기술에 대한 이해와 적용방법을 학습하고, 각 검증기준에 대한 취지의 이해와 함께 평가기술의 적용방법을 교육함

✓ 강주성 교수는 난수성분석론과목 개설을 통해 정보보안 프로토콜 및 암호 알고리즘에 필수적으로 사용되는 난수발생기의 설계와 안전성 평가, 분석 방법을 교육함

■ 산업·융합 분야

✓ 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 설계할수있는 능력을 배양함

▶ 향후 추진계획

■ 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

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)	2021년 2학기	4	5	-	9
	2022년 1학기	15	3	-	18
	계	19	8	-	27

배출 (졸업생)	2021년 2학기	7	1		8
	2022년 1학기	-	2		2
	계	7	3		10

2.2 교육연구단의 우수 대학원생 확보 및 지원 계획

▶ 우수 대학원생 확보 노력

- 본 교육단은 2차년도 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 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.

▶ 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
- 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 미래

가 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

▶ 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 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

■ 신설된 국민*미네르바 교육원을 통해 특성화 영역이나 연구집중학과의 교수진에 커리큘럼 설계를 자문하고, 첨단 융복합 연구주제와 관련된 강의를 하는 것으로 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

■ 상기 확보한 우수 신진연구인력을 활용하여 기 계획된 학부생 연구인턴십 과정 및 연구지도를 수행하였고, 다양한 우수 대학원생 유치에 성공하였음

2.3 대학원생 학술활동 지원 계획

▶ 대학원생 학술활동 지원 계획

■ 교육연구단의 원활한 연구수행을 위하여 2014년 10월 신축한 산학협력관에 교육연구단장 또는 사업 참여교수의 요청에 따라 현재 산학협력관 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

■ 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

■ 과제 교육비를 통해 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

■ 본 교육연구단은 전담 행정인력을 1명 채용할 수 있도록 지원하고 있으며, 산학협력단 내에 배정된 협약담당자, 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

2.4 참여대학원생의 취(창)업의 질적 우수성

<표 2-2> 2021년 8월 및 2022년 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 8월 졸업자	석사	3	-	-	-	3	3	100%
	박사	1			-	1	1	
2022년 2월 졸업자	석사	10	4	-	-	6	6	100%
	박사	3			-	3	3	

▶ 이태호 학생은 정보통신분야의 표준화 및 시험인증 기관인 한국정보통신기술협회(TTA)에 취업하여 정보통신망 연결기기에 대한 정보보호 인증 시험 업무를 진행하고 있다.

▶ 한주홍 학생은 글로벌 메신저 플랫폼 기업인 LINE Plus에 취업하여 LINE의 암호 기술 고도화와 함께 보안 시스템 설계, 개발, 컨설팅 업무를 진행하고 있음

▶ 송진교 학생은 IoT 환경에서의 차세대 양자내성암호 설계 및 최적화 구현 연구를 기반으로 LG U+에 취업하여 양자 보안 소프트웨어 및 통신 설계 구현 업무를 진행하고 있음

▶ 안상우 학생은 GPU 환경에서의 암호 알고리즘 구현 방안 및 최적화 구현 연구를 기반으로 한국정보통신기술협회(TTA)에 취업하여 정보보호제품 보안성 평가 업무를 진행하고 있음

▶ 캐서린 마리 델핀라즈 학생은 22년 02월 박사과정 졸업 후 동년 04월 국민대학교 산학협력관에 박사급 선임연구원으로 입사하여 수중 및 극지와 같은 특수 통신 네트워크의 보안에 대한 연구를 진행 중

▶ 무팔라 갈야니는 22년 02월 박사과정 졸업 후 동년 03월 ㈜비스토스에 소프트웨어 엔지니어로 입사하여 산부인과용 초음파 기기의 보안에 대한 업무를 수행 중

▶ 김예원 학생은 난수발생기의 안전성 분석 및 GPU의 암호학적 응용에 관한 연구를 기반으로 국방에 필요한 무기 및 국방과학기술에 대한 기술적 조사, 연구, 개발 및 시험 등을 담당하여 국방력 강화와 자주국방 완수에 기여하는 국방과학연구소에 취업하였음

▶ 권수진 학생은 그래프 기반 공개키 암호 프리미티브 및 양자내성암호로의 전환에 관한 연구를 기반으로 대표 금융기업 중 하나인 신한은행에 취업하였음

▶ 임형신 학생은 화이트박스 암호의 효율적인 안전성 분석 및 응용에 관한 연구를 기반으로 In-Car와 Out-Car 영역 전반의 소프트웨어와 인프라를 안정적, 효율적, 혁신적으로 지원하는 기업인 현대 오토에버에 취업하였음

▶ 박명서 학생은 스마트폰에서 생성되는 다양한 암호화된 데이터에 대한 복호화에 관한 연구를 진행하여 본 연구단의 연구교수를 거쳐 2022년 3월 강남대학교 ICT 융합공학부의 교수로 취임하였음.

▶ 이세훈 학생은 스마트폰을 포함한 디지털 기기에서 생성된 데이터의 추출 분석에 관한 연구를 진행하여 한국 원자력 연구원에서 드론 위협에 대응하고 있음.

▶

3. 참여대학원생 연구실적의 우수성

① 참여대학원생 저명학술지 논문의 우수성

▶ 자체평가 대상 기간 내 국제 저널 13편, 국내 저널 5편 논문 등재의 성과를 냄

▶ 국제 저널

■ 참여학생 한재승은 “Single-Trace Attack on NIST 3 Candidate Dilithium Using Machine Learning-Based Profiling” 논문을 통해 NIST 3라운드 후보인 격자 기반 암호 Crystals-Dilithium을 대상으로 단일 파형 분석이 가능한 딥러닝 기반 프로파일링 공격 기법을 제안함.

■ 참여학생 한재승은 “Improved Correlation Power Analysis on Bitslice Block Ciphers” 논문을 통해 비트슬라이스 암호의 상관전력분석 성능 향상을 위한 비트별 분석 성능을 예측 기법을 제안하고 이에 대한 이론적 근거를 제시함.

■ 참여학생 우지은 “Deep-Learning-Based Side-Channel Analysis of Block Cipher PIPO With Bitslice Implementation” 논문을 통해 PIPO 암호 알고리즘의 비트 슬라이스 구현에 대하여 딥러닝 기반 프로파일링 및 비프로파일링 부채널 분석 기법을 제안함.

■ 참여학생 임성혁은 “Experimental evaluation of differential fault attack on lightweight block cipher PIPO” 논문을 통해 블록 암호 PIPO를 대상으로 단일 비트 반전 오류 기반 차분 오류 공격 제안 및 EM-FI를 통해 실험적으로 증명함.

■ 참여학생 임성혁은 “Single-Byte Error-Based Practical Differential Fault Attack on Bit-Sliced Lightweight Block Cipher PIPO” 논문을 통해 블록 암호 PIPO를 대상으로 단일 바이트 오류 기반의 실질적인 차분 오류 공격 기법을 제안하고 실험적으로 증명함.

■ 참여학생 이종혁은 “Novel Shuffling Countermeasure for Advanced Encryption Standard (AES) against Profiled Attack in Mobile Multimedia Services” 논문을 통해 모바일 환경에서의 AES 프로파일링 공격에 대한 신규 셔플링 대응기법을 제안함.

■ 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

■ 참여 학생 최호진은 “Fast Implementation of SHA-3 in GPU Environment” 논문을 통해 SHA-3 알고리즘의 소프트웨어 환경 최적화 방안을 제안하였음. 기존의 SHA-3 해시함수는 소프트웨어 환경에서 느린 성능의 문제점을 파악하고, 내부 구조를 변경 및 GPU 병렬 고속화 방안을 통해 효과적인 SHA-3 병렬 연산 처리 방안을 기술하였음

■ 참여 학생 송진교는 “High-Speed Fault Attack Resistant Implementation of PIPO Block Cipher on ARM Cortex-A,” 논문을 통해 ARM Cortex-A 환경에서의 경량 블록 암호 PIPO 최적화 방안을 제안하였음. ARM Cortex-A 플랫폼의 레지스터 설계 방안, 경량 블록 암호 PIPO 최적화 구현 방안, 부채널 공격 대응방안 등을 제안하여 효과적인 PIPO 연산 처리 방안을 기술하였음

■ 참여 학생 김영범은 “CRYSTALS-Dilithium on ARMv8” 논문을 통해 ARMv8 환경에서의 차세대 양자내성 전자서명 알고리즘 Crystals-Dilithium 구현방안을 최초로 제안하였음. NTT 최신구현 기법들을 적용하고, 파이프라인 구조를 활용한 인터리빙 기법을 새롭게 제안함.

■ 참여 학생 안상우는 “Designing a New XTS-AES Parallel Optimization Implementation Technique for Fast File Encryption” 논문을 통해 GPU 환경에서의 파일 시스템 암호화 고속 병렬 방안을 제안하였음. 고속 병렬처리가 가능한 GPU 플랫폼은 서버 환경에서 주로 활용되며, 본 논문에서 제안한 고속 파일 시스템 병렬 암호화 방안은 서버 환경에서 효과적인 파일 암호화 방안으로 사용될 것으로 기대됨

■ 참여 학생 김영범은 “Accelerating Falcon on ARMv8” 논문을 통해 Falcon의 핵심연산인 FFT/NTT에 대한 최적화 구현기법을 제안함. Merging, Register Holding을 이용한 최적화 방안을 FFT/NTT의 구현물들에 모두 적용하여 성능을 가속화 함

■ 참여 학생 최호진은 “Efficient Parallel Implementations of PIPO Block Cipher on CPU and GPU” 논문을

통해 CPU/GPU 환경에서의 경량 블록 암호 알고리즘 PIPO에 대한 최적화 방안을 제안하였음. 연산 기기들의 환경적 특성을 고려하여 암호 알고리즘 연산에 대한 병렬 처리 방안을 제안하였음. 본 논문에서 제안한 최적화 방안은 서버 환경에서의 PIPO 암호 알고리즘 통신/연산에서 효과적인 연산 가속기 방안으로 사용될 수 있음

- 참여 학생 김영범은 “Optimized Implementation of PIPO Block Cipher on 32-bit ARM and RISC-V Processors” 논문을 통해 임베디드 기기에서의 경량 블록 암호 알고리즘 PIPO 에 대한 최적화 방안을 제안하였음. 임베디드 기기의 특성을 고려하여 메모리 및 레지스터 가용 방안을 설계하여 PIPO 암호 알고리즘 연산 가속 방안을 제안하였음. 본 논문에서 제안한 최적화 방안은 IoT 기기에서의 PIPO 암호 알고리즘 통신/연산에서 효과적인 방안으로 적용할 수 있음
- 기존 IoT의 기술을 발전, 응용시켜 해양학, 다이버 네트워크 모니터링, 심해 탐사 및 조기 경보 시스템 같은 응용 프로그램을 개발되고 있고 제한된 UIoT 환경에는 지상에서 활용되고 있는 암호 프로토콜 및 모듈을 직접 적용할 수 없기 때문에 UIoT 환경에서의 보안 프로그램이 필요함. 참여학생 델핀라즈는 “A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things” 논문을 통해 최근 UIoT 시스템의 동향과 수중 디바이스의 보안에 관한 요구사항을 분석 및 반영함
- 참여학생 김한기는 “A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application” 논문을 통해 경량 블록 암호 PIPO의 S-box 생성논리인 Branch number 3 이상을 갖는 방법을 제시하고, 높은 Branch number를 갖는 S-box들을 제안하여 적은 라운드에도 안전한 블록암호 설계를 가능하게 함
- 참여학생 전용진은 “Differential uniformity and linearity of S-boxes by multiplicative complexity” 논문을 통해 S-box의 안전성 척도와 효율성 지표인 multiplicative complexity의 관계성을 밝히고, multiplicative complexity 당 안전성의 하한을 제시함
- 참여학생 김기윤은 “Speeding Up LAT: Generating a Linear Approximation Table Using a Bitsliced Implementation” 논문을 통해 암호 분석에 사용되는 LAT 생성을 비트슬라이싱 기법으로 고속화 생성 방안을 제안함. 제안된 알고리즘은 16-bit S-box 기준 약 11일이 걸리는 LAT 생성을 1시간 반만에 끝내며, 병렬처리를 하면 3초 이내로 생성되어 큰 S-box의 효율적인 분석이 가능하게 함
- 참여학생 백승준은 “Quantum cryptanalysis of the full AES-256-based Davies-Meyer, Hirose and MJH hash functions” 논문을 통해 양자환경에서의 AES-256 기반 Davies-Meyer, Hirose, MJH 해시함수의 안전성을 분석하고 일반 충돌쌍 공격 및 free-start 충돌쌍 공격을 진행하여 해당 구조가 양자 컴퓨팅 환경에서 랜덤으로 충돌쌍을 얻는 것보다 빠른 공격이 있음을 제시함

▶ 국내 저널

- 극지는 극심히 낮은 기온 때문에 연구자의 활동 범위가 제한되어 보다 더 효과적으로 연구 데이터를 회수하는 기술이 요구됨. 참여학생 염선호는 “극한지 환경에서 무인기를 이용한 MQTT 기반 극한지 생물용 바이오로거 데이터 원격 회수 시스템 구현” 논문을 통해 데이터 원격 회수 효율성을 증대하기 위한 방법으로 무인기를 이용한 데이터 원격 회수 상황을 가정하고 데이터 전송 시스템을 MQTT 기술을 활용하여 구현함
- 극지의 환경적인 요인 때문에 무선 통신 네트워크의 신뢰성을 보장하기 어려우며 물적, 인적 자원 및 시간 등이 소모될 수 밖에 없음. 참여학생 염선호는 “극지 생물 바이오로거 데이터 원격 회수를 위한 결함 감내 네트워크” 논문을 통해 극지에서 원격지에 존재하는 데이터를 회수하기 위해 무인항공기(UAV)를 Data mule로 활용하는 결합 감내 네트워크를 제안함
- 참여학생 유현도는 “Gohr의 Speck32/64 신경망 구분자에 대한 분석과 Simon32/64에의 응용” 논문을 통해 Gohr가 제안한 신경만 구분자의 성능 향상의 이유를 원리적으로 분석하고 증명함. 해당 연구 결과를

Simon32/64에 적용하여 신경망 구분자의 성능 향상 방향성을 제시함

- 참여학생 박종현은 “블록암호 PRESENT에 대한 향상된 SITM 공격” 논문을 통해 경량 블록 암호 PRESENT에 대한 SITM 공격의 향상된 공격을 제안함
- 참여학생 백승준은 “양자 컴퓨팅 환경에서의 해시함수 충돌쌍 공격 동향” 논문을 통해 양자 컴퓨팅 환경에서의 해시함수 및 해시함수의 충돌쌍 공격에 대한 최신 연구 동향을 정리함. 해시함수의 안전성은 양자내성 암호의 안전성까지 영향을 미치므로 연구의 필요성을 밝힘

② 참여대학원생 학술대회 대표실적의 우수성

▶ 자체평가 대상 기간 내 국제 저널 7편, 국내 저널 30편 논문 등재의 성과를 냄

▶ 국제 학회

- 참여학생 우지은은 ICISC 2021에서 “Deep Learning-based Side-Channel Analysis on PIPO” 논문을 발표함. 본 논문은 국내 경량 블록 암호 PIPO 대상 딥러닝 기반 프로파일링 공격 및 비프로파일링 공격의 효율적인 기법을 제안함
- 참여학생 임성혁은 ICISC 2021에서 “Differential Fault Attack on Lightweight Block Cipher PIPO” 논문을 발표함. 본 논문은 국내 경량 블록 암호 PIPO 대상 단일 비트 오류 기반의 차분 오류 공격 논리를 제안함
- 참여학생 안성현은 WISA 2022에서 “Illegal Photo Shoot Detection Method Using Operating Frequency of Smartphone Camera” 논문을 발표함. 본 논문은 스마트폰 카메라의 동작 주파수를 이용해 불법 촬영 탐지 방안을 제안함.
- 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
- 참여학생 이세윤은 “Telecommunication for Quantum Computer” 포스터를 통해 6G에서 PQC를 사용하여 적절한 키 캡슐화 메커니즘(KEM)을 설계하고, 데이터 캡슐화 메커니즘(DEM)을 통해 6G에서 비밀 정보를 안전하게 공유할 수 있는 방법을 제안함
- 참여학생 델핀라즈는 우수 학술대회 WUWNet’21에서 “International Standardization for Maritime, Underwater Internet of Things and Digital Twin Applications”를 통해 2021년 4월 신설된 ISO/IEC JTC 1/SC 41/WG7 활동 내역을 소개함
- UIoT 환경의 기술적 문제 때문에 UIoT 애플리케이션을 위한 네트워크 관리 및 기기 관리 구축이 필요함. 참여학생 델핀라즈는 수중 음향 센서 네트워크(UWASN)를 위한 노드 이동성과 관련된 수중 네트워크 관리 및 장치 관리를 다룬 논문 “Underwater Internet of Things -Network and Device Management for Mobile Underwater Acoustic Sensor Networks”을 투고함
- 수중 음파 탐지기와 수중 광통신 등 다양한 수중 다이버 통신 수단이 도입돼 사용되며 통신을 위해 다양한 수중 차량과 통신할 수 있는 카메라로 AUV를 인식할 수 있는 제스처 검출 방식이 유일한 방법임. 참여학생 신하 쉬르티카는 “Underwater Autonomous Diver Gesture Detection System for communication between AUV and Human Diver” 논문을 통해 인공지능을 이용한 제스처 감지 방법을 제시함
- 해양 환경 탐자를 위한 UIoT 연구를 위한 수중 통신 장애 요소 분석이 필요함. 참여학생 신하 쉬르티카는 “Requirement Analysis for Channel Selection Mechanism using Machine Learning in Underwater Communications” 논문을 통해 MM/MB를 사용하는 수중 통신에서 기계 학습을 사용하

는 채널 매커니즘에 대한 개요를 제공하고 극지 통신에서도 적용 가능한 수중 통신에서 채널 선택을 위해 고려된 요구사항과 후보 기계 학습 알고리즘을 제공함. 해당 논문은 당해 학술대회에서 우수 논문으로 선정됨

- 참여 학생 최호진은 “Efficient parallel implementation methods of LSH-512 utilizing SIMD AVX-512” 논문을 통해 SIMD AVX-512를 활용한 국산 해시 함수 LSH 내부 연산 병렬화 방안을 제안하였음. LSH 내부 연산 구조와 AVX-512 명령어를 분석하여 내부 연산에서 가용할 수 있는 명령어를 제안하여 LSH 성능을 가속화 함
- 참여 학생 김영범은 “MFT : Metamorphic Fuzz Testing for Efficient Correctness Validation of Cryptographic Implementation” 논문을 통하여 구현 정확성 검증 방안 및 내부 취약점을 도출할 수 있는 방법론을 제안함. Metamorphic Testing은 기존의 CAVP의 한계점을 보완하는 검증 방안이며, Fuzz Testing은 소스 코드의 취약점을 도출하는 방안으로, 2개의 방안을 결합하여 암호 알고리즘 라이브러리에 대한 안전성 검증 방안 방법론을 제안하였음
- 참여 학생 김영범은 “Metamorphic Testing on NIST LWC Finalists” 논문을 통하여 NIST 경량 블록 암호 공모전에 제출된 알고리즘에 대한 Metamorphic Testing 적용 방안 및 결과를 제안하였음. Metamorphic Testing 방안은 기존의 암호 알고리즘 검증 방안인 CAVP의 한계점을 보완하고, 실제 네트워크 환경에서 발생할 수 있는 구현 정확성을 검증하는 방안으로, NIST LWC 공개 소스 코드에 대한 적용 방안 및 결과를 제안함
- 참여학생 김건우는 World Conference on Information Security Applications (WISA 2021) 국제 학술대회에서 “MUD for Infusion Pumps_ An Attempt to Reduce Network-based Attacks” 포스터를 발표함. 스마트 인퓨전 펌프에 존재하는 취약점에 대하여 MUD를 활용하여 필요한 트래픽만 송수신 가능하도록 허용함으로써, 가용성을 유지하고 DDoS 공격과 같은 위협에 노출되는 것에 대하여 방지하는 기술을 제안함.

▶ 국내 학회

- 참여학생 안성현은 2021 한국군사과학기술학회 종합학술대회에서 “효율적인 교차 디바이스 부채널 분석을 위한 프로파일링 디바이스 선택 방법” 논문을 통해 교차 디바이스 사이의 노이즈 차로 발생하는 분석 성능 저하를 줄이기 위한 프로파일링 디바이스 선택 방법론을 제안함
- 참여학생 김수진은 2021 정보보호학회 동계학술대회에서 “경량암호 PIPO에 대한 신경망 및 라벨 설정에 따른 프로파일링 부채널 분석” 논문을 통해 국내 경량 블록 암호 PIPO를 대상으로 프로파일링 부채널 분석 수행 시 신경망 및 라벨 설정에 따른 성능 비교를 보이고 가장 효과적인 신경망 구조를 제안함
- 참여학생 임성혁은 2021 정보보호학회 동계학술대회에서 “딥러닝 기반 비프로파일링 이차 부채널 분석 성능 향상 기법에 관한 연구” 논문을 통해 딥러닝 기반 이차 부채널 분석 수행 시 효과적인 라벨링 기법 및 활성 함수를 제안하고 이를 시뮬레이션 데이터 및 ASCAD 데이터를 대상으로 증명함
- 참여학생 안성현은 2021 정보보호학회 동계학술대회에서 “딥러닝을 활용한 스마트폰 카메라 불법 촬영 탐지 방안” 논문을 통해 스마트폰 카메라 모듈 동작 시 발생하는 전자파 신호 파형을 CNN 신경망을 이용하여 구별하는 방안을 제안함
- 참여학생 한재승은 2022 정보보호학회 하계학술대회에서 “AES CTR 모드에 대한 향상된 전력분석 기법” 논문을 통해 AES CTR 모드에 대하여 클러스터링 기법을 활용하여 공격 복잡도를 낮추는 향상된 전력분석 기법을 제안함.
- 참여학생 이종혁은 2022 정보보호학회 하계학술대회에서 “ARIA 암호 알고리즘에의 전력 글리치 다중 오류 주입 공격” 논문을 통해 ARIA 암호 알고리즘을 대상으로 전력 글리치 다중 오류 공격을 통해 공격 복잡도를 낮추는 방안을 제안함.
- 참여학생 김수진은 2022 정보보호학회 하계학술대회에서 “NIST PQC Round 3 격자 기반 PKE KEM의 소프트웨어 하드웨어 구현에 대한 부채널 분석 동향” 논문을 통해 NIST PQC Round 3 격자기반 PKE, KEM에

대한 소프트웨어 및 하드웨어 구현에 대한 부채널 분석 동향을 제시함.

- 참여학생 김연재는 2022 정보보호학회 하계학술대회에서 “글로벌 IT 보안 기업 CENSUS 사 Masked AES software library에 대한 잔여 1차 부채널 취약점 분석” 논문을 통해 CENSUS사에서 공개한 마스킹 AES 라이브러리에 대한 커플링 취약점을 제시함.
- 참여학생 우지은은 2022 정보보호학회 하계학술대회에서 “이종 디바이스 환경에서의 비지도 도메인 적응을 이용한 신규 프로파일링 부채널 분석” 논문을 통해 MMD loss를 통한 비지도 도메인 적용을 수행하여 이종 디바이스 환경에서의 프로파일링 부채널 분석 성능 향상 방안을 제안함.
- 참여학생 문혜원은 2022 정보보호학회 하계학술대회에서 “장치의 열 방출량을 이용한 오류 주입 공격 성공률 향상 방안 연구” 논문을 통해 EMMI를 이용하여 장치의 열 방출량을 관찰하고 오류주입 공격 성공률을 향상시킬 수 있는 방안을 제안함.
- 참여학생 한주홍은 “TCP 통신 환경 암호장비에 대한 최적화 요소 분석” 논문을 통해 암호장비의 가용성을 높일 수 있는 최적화 요소에 대해 분석하여 향후 암호장비 설계 시 최적화를 위해 고려해야 하는 지표 중 하나를 제시함
- 참여학생 이세윤은 “서버에서의 양자내성암호 기반 통합 암호 체계 제안” 논문을 통해 현재 NIST Round 3의 최종후보에 오른 PQC를 기반으로 하는 하이브리드 통합 암호화 체계 PQIES를 새롭게 제안하고, 복호화를 진행하는 서버측에서 제안하는 PQIES를 적용하여 발생 가능하는 문제점과 성능 측정을 살펴봄
- 참여학생 윤혜진은 “안드로이드 애플리케이션 인증방식의 취약점 분석 및 동향” 논문을 통해 안드로이드 앱에서 사용하는 인증방식 중 OAuth 2.0에 대해 소개하고 취약점을 분석함. 안드로이드 앱 인증 방식 구성에 맞는 EAP 매커니즘 기반 방식을 개발 및 이용함으로써 더 안전한 인증 방식이 안드로이드 앱 인증 방식으로 적용될 것을 기대함
- 참여학생 김태완은 “난수발생기에 따른 UDM 인증 벡터 생성 속도 분석” 논문을 통해 5G 네트워크는 인증을 진행할 때마다 안전한 난수 발생기를 사용하여 난수를 생성하고, 난수를 통해 인증 벡터를 생성해야 하기 때문에 NIST SP 800-90a에서 권장하는 DRBG에 따른 난수 및 인증 벡터의 생성 속도를 분석함
- 참여학생 정서우는 “양자 암호모듈 기반 드론 식별 및 정보 제공 기술 구현에 대한 연구” 논문을 통해 양자 엔트로피 기반의 난수 발생기가 탑재된 암호모듈을 이용하여 드론 간의 피아식별 및 위치 정보 등의 안전한 정보 제공 기술 구현 방법을 제안함
- 참여학생 김형엽은 “BB84 프로토콜 분석 및 양자 키 분배 표준화 동향” 논문을 통해 1984년 Bennet와 Brassard가 제안한 BB84 프로토콜과 양자 키 분배에 대한 표준화 동향을 소개함
- 참여학생 김태완은 “UTM 내 드론에서 사용 가능한 보안 파라미터 딥러닝 기반 탐지” 논문을 통해 딥러닝을 통해 UTM 내 드론에서 암호학적 난수의 안전성을 담당하는 잡음원(엔트로피 소스)을 식별하는 방법을 제시함
- 참여학생 김태완은 “검증필 암호모듈 기반 드론 식별 체계 연구” 논문을 통해 미국 FAA에서 설명하는 UTM 개요와 진행 중인 드론 식별 모듈 표준화를 정리하고, 안전한 드론 운용을 위한 검증필 암호모듈 기반 드론 식별 체계를 제안함
- 참여학생 정서우는 “상용 드론의 군 도입을 위한 검증필 암호모듈 상호호환 운용 환경 요구사항” 논문을 통해 상용 드론을 군에서 활용하기 위해 필요한 일부 보안 항목과 보안 항목별 필요한 암호알고리즘에 대해 설명하고, 국방 드론체계 구성요소 간 보안을 적용하기 위한 검증필 암호모듈 간의 상호호환성 제공 운용 요구사항을 제안함
- 참여학생 김형엽은 “드론 비행 데이터 저장 방법에 대한 연구” 논문을 통해 드론의 중요 데이터를 전송, 저장하기 위한 보안을 적용하기 이전에 드론의 비행 데이터를 저장하는 두 가지 방법으로 Sniffing 방식과 Relaying 방식을 제안함
- 참여학생 윤혜진은 “오프라인 환경의 디바이스에 인증을 위한 AHS 프로토콜 제안” 논문을 통해 개인정보보호를 위해 접근자와 인증 서버는 온라인 환경이고, 오프라인 환경의 디바이스가 접근자를 인증하는 프

로토콜을 제안함

- 참여학생 이세윤은 “한국형 UTM 내부 양자 보안 아키텍처 설계” 논문을 통해 UTM에 적용할 수 있는 양자 보안 시스템을 설계하여 양자 컴퓨터의 위협으로부터 한국형 UTM의 양자 보안 아키텍처 설계를 제안함
- 참여학생 송진교는 “ARM Cortex-A 환경에서 Falcon Round 3의 FFT 곱셈 최적화 연구”논문을 통해 ARMv8 환경에서 Falcon의 FFT 알고리즘의 최적화 방안에 대하여 최초로 제안함
- 참여학생 김영범은 “키 유도함수에 대한 Metamorphic Testing ‘ 설계논문을 통해 검증대상 키 유도함수 알고리즘에 대해 새로운 구현적합성 검증방법을 제안하고 실제 적용하였음
- 참여 학생 최호진은 “GPU 환경에서의 16-bit 자료형을 활용한 PIPO 암호 알고리즘 최적화 방안” 논문을 통해 GPU 아키텍처에서의 PIPO 암호 알고리즘 최적화 방안을 제안하였음. GPU 아키텍처에서 사용할 수 있는 인라인 어셈블리 PTX 명령어를 분석, PTX 명령어의 최소 연산 처리 자료형을 활용하여 국산 블록 암호 알고리즘 PIPO 최적화 구현 방안을 제안 및 기술하였음
- 참여 학생 안상우는 “CUDA GPU 환경에서의 Falcon Fast Fourier Sampling 연산을 위한 이중 재귀함수의 반복문 대체 기법” 논문을 통하여 GPU 환경에서의 NIST PQC Falcon 내부 연산 최적화 방안을 제안하였음. NIST PQC Falcon Reference 코드를 분석하여 Fast Fourier Sampling 연산의 성능 부하를 분석, 이중 재귀함수를 통한 반복문을 효과적으로 처리하였음
- 참여학생 김영범은 “블록체인의 구조적 문제 및 암호학적 취약점에 대한 동향 조사” 논문을 통해 암호학점 취약점에 대한 동향을 분석하고 향후 연구 전망을 제시함
- 참여학생 김영범은 “자율주행환경에서 PQC 적용분석을 위한 V2Verifier 분석 및 확장” 논문을 통해 자율주행 환경에서 사용하는 V2X/WAVE 프로토콜에 PQC를 적용 및 분석하여 향후 PQC 마이그레이션을 위해 고려해야 할 점을 제안함
- 참여학생 김영범은 “CPU 환경에서 최신 경량 암호 GIFT-COFB의 최적화 및 속도 개선과 구현” 논문을 통해 CPU 환경에서 C언어 기반의 GIFT 구현을 가속화 할 수 있는 방안을 제안함
- 참여 학생 최호진은 “CPU 환경에서의 AVX-512를 활용한 블록 암호 알고리즘 PIPO 벤치마킹” 논문을 통하여 Intel CPU 제품군에서 제공하는 AVX-512 SIMD 명령어를 통한 국산 블록 암호 알고리즘 PIPO 구현 방안을 제안하였음. PIPO의 내부 연산을 분석 및 AVX-512의 신규 명령어를 분석하여 AVX-512 범용 레지스터를 활용한 PIPO 병렬처리 방안을 제안하였음
- 참여 학생 안상우는 “NVIDIA GPU 환경에서 효율적인 병렬 작업 수행을 위한 더미 연산 구현 기법” 은 GPU 환경에서 더미 연산을 통한 스레드 병렬 작업에 대한 효율성 분석 및 결과를 제안하였음. GPU 환경에서 스레드는 동일한 연산을 수행하며, 분기문을 최소화하기 위해 더미 연산을 추가, 병렬 연산의 효율성 및 병목현상을 제거하는 방안을 제안하였음
- 참여 학생 최호진은 “SIMD AVX-512를 활용한 LEA 병렬 구현 방안” 논문을 통해 신규 SIMD AVX-512를 활용하여 국산 블록 암호 알고리즘 LEA 내부 동작 과정 병렬 처리 방안 및 AVX-512를 활용한 구현 방안을 제안함.
- 참여 학생 김영범은 “PQC 마이그레이션을 위한 고려사항 분석 및 최신연구 동향 조사” 논문을 통해 양자내성암호의 실제 적용에 대한 고려사항을 분석하였음. 기존의 프로토콜 및 암호체계에서 양자내성암호로의 전환에서 발생할 수 있는 고려사항과 프로토콜 적용의 실제 연구 사례를 분석하였음.
- 참여 학생 김영범은 “격자기반 다항식 곱셈 최적화 구현 동향” 논문을 통해 격자 기반 다항식 곱셈의 최신 연구 동향을 분석하였음. NTT 기반 곱셈의 최신 구현동향에 대해서 분석함
- 참여 학생 김영범은 “IoT 환경을 위한 경량암호 최적화 동향 분석” 논문을 통해 경량암호의 최신 연구 동향에 대하여 분석하였음. 또한, NIST LWC 프로젝트의 최종 진출 알고리즘들에 대한 최적화 방안에 대해 논의 하였음
- 참여 학생 김영범은 “자동차 OTA(Over The Air) 업데이트 보안 동향 분석”논문을 통해 OTA 환경에서 고려해야할 보안 사항에 대해 분석하였음. 보안에 사용되는 다양한 스킴이 OTA 환경에서 적용되는 방안에

대해 조사하였음

- 참여학생 전창열은 “Patterson 디코딩 기반 Classic McEliece 키 복호 연산에 관한 연구” 논문을 통해 NIST PQC 3라운드에 오른 부호기반암호인 Classic McEliece의 복호화 방법을 Patterson 알고리듬으로 변경하여 고속의 디코딩 방법을 제시함.
- 참여학생 전창열은 “유한체 상에서의 기약다항식 생성에 관한 연구” 논문을 통해 이진 Goppa 부호에서 사용하는 기약다항식 생성에 사용가능한 알고리듬을 설명하고 해당 알고리듬의 복잡도 분석을 통해 효율적인 기약다항식 생성 알고리듬을 분석함.
- 참여학생 전창열은 “유클리드 호제법과 이진 최대공약수 알고리듬을 이용한 최대공약수 고속 계산에 관한 연구” 논문을 통해 최대 공약수 생성 알고리즘을 소개하고, 이를 토대로 병합 알고리듬을 생성하여 고속으로 최대공약수를 계산 가능한 알고리즘을 제시함.
- 참여학생 전창열은 “다항식 몫환 F_p[X]〈Xˆn+1〉의 NTT 기반 곱셈 연산에 관한 연구” 논문을 통해 환에서의 곱셈 연산 시 사용 가능한 NTT 알고리듬을 소개하고 일반 곱셈 연산 대비 성능 향상 결과를 설명함.
- 움직이는 생물, 물체에 부착된 센서 디바이스에 저장된 데이터를 회수하기 위한 무인 비행체(UAV) 기반 원격 데이터 회수 센서 네트워크의 데이터 회수 비용 절감이 필요함. . 참여학생 황아리는 “무인 비행체(UAV) 기반 원격 데이터 회수 센서 네트워크의 임무 시간 단축을 위한 요구사항” 논문을 통해 무인 비행체(UAV) 비행 시간 단축을 위한 효율적인 경로 설정 요구사항을 제시함
- 극한지에서 장기적인 관찰을 요구하는 연구분야의 연구 데이터 확보를 목적으로 센서 수집 기능과 데이터 저장 기능이 통합된 ‘로거’가 활용됨. 참여학생 염선호는 “최근 정보통신 기술 극한지 네트워크 경량 원격 데이터 전송 시스템 설계에 관한 연구” 논문을 통해 극한지 연구 분야 연구자들이 현장의 환경 및 생물, 생태 정보를 수집하기 위해 사용하는 임베디드 센서 장치에 저장된 데이터를 극한지 통신 네트워크를 통해 원격으로 회수하기 위한 데이터 전송 시스템의 설계를 다룬 논문을 투고함. 당해 학술대회에서 우수 논문으로 선정됨
- 참여학생 유현도는 “경량 암호 CHAM을 사용한 암호학적 난수발생기 GPU 병렬 구현” 논문을 통해 최근 국내에서 제안한 경량 블록암호 알고리즘인 CHAM을 사용하는 암호학적 난수발생기를 구현하고, GPU를 사용한 고속화 구현을 통해 안전하면서 고속의 난수를 생성하는 난수발생기를 제시하였음
- 참여학생 김원일은 “MODBUS 프로토콜의 양자내성암호(PQC) 적용 방안에 관한 연구” 논문을 통해 산업 제어시스템에서 사용하고 있는 MODBUS 프로토콜에 최근 공모 진행 중인 양자내성암호를 적용하여 최신 암호가 적용된 안전한 MODBUS 프로토콜을 사용할 수 있는 방안에 관한 연구를 제시하였음
- 참여학생 유현도는 “이미지 센서 기반 난수발생기의 잡음원에 적용 가능한 헬스테스트 설계” 논문을 통해 이미지 센서를 물리적 잡음원으로 사용하는 난수발생기의 잡음원에 적용 가능한 헬스테스트를 실시간과 주기적인 단위로 설계하여 적용하는 방법에 관한 연구를 진행하고 설계한 테스트가 오류를 잡아내는 확률을 시간적으로 제시하였음
- 참여학생 류지은은 “그래프 기반 PDF 암호시스템 개선 방법에 관한 연구” 논문을 통해 양자내성암호로 사용가능한 그래프 기반 PDF 암호에 단점인 계산 복잡도를 줄일 수 있는 방향을 제시하였음.
- 참여학생 류지은은 “복수 그래프의 조합을 통한 그래프 기반 PDF 암호시스템 개선 방법 제안” 논문을 통해 양자내성암호인 그래프 기반 PDF 암호시스템의 안전성을 분석하고, 암호화 속도 개선을 위한 개선 방안을 제안함. 키 크기를 늘리지 않고 안전성을 보장하기 위하여 둘 이상의 그래프를 사용하여 암호문을 생성하는 방식을 통해 암호문 길이를 늘리지 않고 알고리즘을 개선할 수 있음을 보임. 이후 개선된 알고리즘을 사용할 경우 얻게 될 것으로 예상되는 안전성과 구현 효율성을 계산하여 제시함
- 참여학생 박영재는 “NTRU에 사용되는 유한체 역원 알고리즘 분석 및 성능 비교” 논문을 통해 양자내성암호인 NTRU에서 역원 계산을 위해 사용하는 Almost Inverse Algorithm의 3가지 버전을 조사하고 이를 NIST 양자내성암호 공모전 3라운드에 제출된 NTRU에 적용하여 성능을 비교 및 분석함. 나아가 공모전에 제출된

NTRU의 기존 역원 알고리즘을 상수 시간 내에 동작하는 역원 알고리즘으로 바꿔 적용할 경우와 성능을 비교하여 부채널 공격에 안전성을 확보했는지 확인함

- 참여학생 최영락은 “암호학적 은닉채널과 블랙박스 암호모듈의 보안 위협” 논문을 통해 안전한 암호 알고리즘을 사용하는 black box 암호모듈에 대한 은닉채널의 존재 가능성에 관하여 정리함. 허가되지 않은 방식으로 정보를 얻는 은닉채널의 유형을 3가지 예시와 함께 분류하고, 많은 암호모듈에서 활용되고 있는 RSA에 관한 은닉채널을 양자내성암호에도 비슷한 방식으로 적용할 수 있음을 수학적으로 분석함. 이를 통해 PQC를 사용하더라도 암호모듈이 block box 암호모듈일 경우 은닉채널이 존재할 가능성이 있음을 보임
- 참여학생 조세희는 “NIST 경량 해시함수 Ascon-Hash의 양자 충돌쌍 공격을 위한 MILP 모델 개발” 논문을 통해 NIST의 경량 암호 공모전의 마지막 라운드 후보인 Ascon-Hash를 대상으로 양자환경에서의 충돌쌍 공격을 위한 MILP 모델을 개발함
- 참여학생 김기윤은 “암호화된 랜섬웨어 데이터 복호화 가능한가?” 라는 주제로 2022 NetSec-KR에서 강연을 진행하여 랜섬웨어 감염파일의 복호화 사례 및 최신 랜섬웨어인 Hive의 암호학적 취약점을 활용한 데이터 복호화 방안을 제안함
- 참여학생 김건우는 “블록체인 기반의 스마트 HACCP 구축 사례 연구” 논문을 통해 블록체인 기술이 스마트 HACCP 시스템에 적용하는 것이 유용한지를 확인 하였으며, 구축사례를 통해 어떤 블록체인 적용 플랫폼이 스마트 HACCP 시스템에서 사용되는지 분석하였음. 또한 스마트 HACCP 시스템에 필요한 선제조건과 하이브리드 블록체인 사용에 대하여 제시함
- 참여학생 김건우는 “5G NSA 네트워크에서의 블록체인 기술 기반 키 관리를 위한 LEE-Ma 보안 프로토콜 취약점 분석” 논문을 통해 Lee-Ma가 제안한 블록체인 기반 5G 보안 프로토콜에 대해 정형화 검증 도구인 BAN-Logic을 통해 제안 프로토콜에 대한 취약점 분석을 하였으며, 그 결과 우수논문상에 선정됨
- 참여학생 손대현은 “이음 5G에서 허위기지국 탐지 정확도를 향상하기 위한 연합 학습 시스템 연구“ 논문을 발표함. 본 논문은 위치 기반의 허위 기지국 탐지 정확성을 학습하여 참여자들의 기계 학습 결과를 바탕으로 연합 학습을 실시한 결과를 통해 탐지 정확성을 향상시키는 연구를 제안함
- 참여학생 손대현은 “5G 네트워크상에서 Braeken이 제안한 대칭키 기반의 5G-AKA 인증 프로토콜 BAN Logic 정형화 검증“ 논문을 발표함. 본 논문은 5G-AKA 프로토콜상에서 상호인증 보장과 기존의 공개키가 아닌 대칭키를 이용한 Braeken의 프로토콜이 비밀키 K에 대한 인증이 단방향으로 이루어져 있는걸 확인하였으며, 개선방안을 제안함.
- 참여학생 오종민은 “IoV 네트워크에서의 BAN 논리를 이용한 정형화 검증” 논문을 통해 IoV(Internet of Vehicles) 네트워크의 프로토콜을 정형화 검증 도구인 BAN 논리를 이용하여 정형화 검증을 진행하였음. 프로토콜의 안전성을 분석하고 취약점을 발견하여 개선 방안을 제안하였고, 해당 연구 내용은 향후 IoT(Internet of Things) 프로토콜을 분석할 시 기초가 될 것으로 기대됨.
- 참여학생 오종민은 “웨어러블 디바이스 클라우드 프로토콜에서의 정형화 검증” 논문을 통해 일상생활에서 빈번하게 사용되고 있는 휴대용 전자기기인 웨어러블 디바이스 클라우드 상에서의 프로토콜을 정형화 검증 도구인 BAN 논리와 AVISPA Tool을 이용하여 정형화 검증을 진행하였음. 프로토콜의 안전성을 분석하고 취약점을 발견하여 개선 방안을 제안하였음.

③ 참여대학원생 특허, 기술이전, 창업 실적의 우수성

▶ 자체평가 대상 기간 내 특허 (등록 8건/출원 10건), 기술이전 3건, 소프트웨어 등록 1건의 성과를 냄

▶ 특허

- 차분 오류 공격 방법 및 장치 (등록)
  - ✓ 모듈로 덧셈의 대수적 표현을 이용한 랜덤 워드 오류 모델 기반의 LEA 대상 차분 오류 공격을 개발한 특허임

■ 블록암호에 대한 상관전력 분석 방법 및 장치 (등록)

✓ 비트 슬라이스 암호에 대한 상관전력 분석 수행 시 비트별 분석 성능 예측하는 방법을 개발한 특허임

■ LAC에 대한 부채널 분석 장치 및 방법 (등록)

✓ 격자기반 암호의 인코딩 연산에 대한 부채널 공격을 방지하기 위한 방법을 개발한 특허임

■ 오류 주입 공격 시스템 (등록)

✓ 오류 주입 공격시 인위적인 트리거 없이 완화된 환경에서 공격을 수행하는 방법을 개발한 특허임

■ 오류 주입 공격 장치 및 방법 (등록)

✓ AES 암호의 마지막 라운드 SubBytes 함수를 생략하는 오류를 통한 차분 오류 공격을 개발한 특허임

■ 전자서명 알고리즘의 부채널 분석 방법 및 그 장치 (등록)

✓ 마스킹된 PQC 전자서명 알고리즘에 대하여 딥러닝 기반 부채널 공격 방법을 개발한 특허임

■ 양자 엔트로피 기반 일회용 양자 비밀번호 생성 장치 및 방법

✓ 양자 방사선의 아날로그 잡음원을 발생하여 아날로그 잡음을 제공하는 양자 엔트로피 생성부, 상기 아날로그 잡음에 대한 디지털화를 통해 암호화 시드를 추출하는 암호화 시드 추출부, 및 상기 암호화 시드에 기초하여 일회용 양자 비밀번호(QTP)를 생성하고 상기 일회용 양자 비밀번호(QTP)의 발급 내역을 블록체인 상의 노드에 저장하는 QTP 생성부를 포함함

■ 안티-인버전 함수를 이용한 화이트박스 암호 인코딩 장치 및 방법 (등록)

- PC 또는 모바일 환경에서 소프트웨어로 암호 기능을 수행하는 경우 다양한 공격으로부터 안전하게 암호키를 보호할 수 있는 안티-인버전 함수를 이용한 화이트박스 암호 인코딩 장치 및 방법에 관해 기술함

■ 미디어 파일에 대한 안티 포렌식 해제 장치 및 방법 (등록)

✓ 미디어 파일을 암호화하여 데이터를 보호하는 기술은 범죄행위에서 안티 포렌식 기술로 작용함. 관련 데이터 분석을 위해 안티 포렌식 기술을 제공하는 애플리케이션을 역공학 분석하여 암호화된 데이터를 복호화하는 안티포렌식 해제 장치 및 방법을 개발함.

■ 경량 블록암호 PIPO에 대한 단일 바이트 오류 기반 신규 차분 오류 공격 (출원)

✓ 국내 경량암호 PIPO에 대하여 현실적인 가정에서 단일 바이트 오류를 기반으로 하는 차분 오류 공격을 개발한 특허임

■ 경량 블록암호 PIPO에 대한 신규 딥러닝 기반 프로파일링 및 비프로파일링 부채널 분석 (출원)

✓ 국내 경량암호 PIPO에 대하여 딥러닝 기반 효율적인 프로파일링 및 비프로파일링 공격 방법을 개발한 특허임

■ 소프트웨어 동작 감지 장치 및 방법 (출원)

✓ 딥러닝 기반 스마트폰 카메라 모듈의 동작을 구분해 내는 방법을 개발한 특허임

■ SHA-3 처리를 위한 그래픽 처리 장치 및 방법 (출원)

✓ 기존의 국제표준 해시함수 SHA-1의 충돌 쌍 공격방법 및 실제 충돌 쌍이 제안되었으며, 유사한 구조를 가지는 SHA-2에 대한 공격방법이 제안되고 있음. 이에 NIST는 새로운 구조를 가지는 신규 국제표준 해시함수 SHA-3를 발표하였음. 하지만 SHA-3는 소프트웨어 환경에서 기존 국제표준 해시함수보다 느린 성능을 보여줌. 본 특허에서는 소프트웨어 환경에서 SHA-3 성능 개선 및 GPU 장비를 활용한 해시함수 병렬처리 방안을 제안하였음. SHA-3의 내부 구조 변경, 메모리 접근 횟수 최소화 등의 방안을 제안하여 GPU 장비를 활용하는 여러 환경에서 효과적인 해시함수 처리방안을 기술하였음.

■ 기각 시퀀스 테이블을 이용한 기각 샘플링 병렬 최적화 장치, 방법 및 그 방법을 이용한 전자서명 및 암호화 연산 방법 (출원)

✓ 양자 컴퓨터의 발전에 따른 기존 공개 키 암호알고리즘 시스템의 대체가 필요한 상황에서 NIST는 양자 컴퓨터 환경에서도 안전한 전자서명/공개 키 암호알고리즘에 대한 공모전을 실시함. 해당 공모전에서 제출된 알고리즘 중 격자 기반 암호알고리즘에서는 기각 샘플링 연산을 사용하여 내부 연산을 구축하였음. 본 특허에서는 기각 샘플링에서 사용하는 상숫값을 기각 시퀀스 테이블로 구성하여 연산 최적화 방안 및

스레드 협력 병렬 연산을 통한 연산 최적화 방안을 기술하였음.

■ XTS 최적화를 위한 병렬처리 장치 및 방법 (출원)

✓ XTS는 파일 및 디스크 암호화 알고리즘으로 데이터 및 파일이 저장되어있는 디스크를 전체적으로 암호화하는 방식임. 실제 Window 10 환경에서 XTS-AES 디스크 암호화가 추가되는 등 다양한 환경에서 XTS 알고리즘이 적용됨. 본 특허에서는 GPU 아키텍처 환경에서의 XTS 파일 암호화 방식을 병렬적으로 처리하는 방법을 기술하였으며, 내부 곱셈 연산을 효과적으로 처리하여 병렬처리 성능 개선 방안을 기술함

■ 이미지 센서 기반 난수발생기 헬스 테스트 장치 및 방법 (출원)

- 이미지 센서를 잡음원으로 사용하는 난수발생기의 엔트로피 소스를 검정하여 난수발생기가 정상적으로 동작하고 있는지 확인할 수 있는 이미지 센서 기반 난수발생기 헬스 테스트 장치 및 방법에 관해 기술함

■ 일방향 함수를 이용한 암호 운영모드 기반의 화이트박스 암호화 방법 및 장치 (출원)

- 데이터 보호를 위해 블록암호를 사용하면서도 암호키의 노출을 방지하고 암호화 모듈을 통해 복호화가 불가능한 일방향 특성을 제공하는 기술에 관해 기술함

■ DLBN이 3 이상인 조건을 만족하는 확장 에스박스 및 이를 이용한 비트 연산 방법 (출원)

✓ 선형구간을 로테이션으로 사용하는 블록암호는 S-box의 DLBN이 높을수록 적은 라운드에서 높은 안전성을 달성함. 일반적인 S-box는 DLBN이 2이나, DLBN이 3 이상인 조건을 만족하는 확장구조와 이를 통해 개발된 확장 S-box를 기술함

■ FTS 색인데이터 기반의 삭제 채팅 메시지 복구 장치 및 방법 (출원)

✓ 모바일 및 PC용 메신저에서 주로 사용되는 SQLite 데이터베이스는 FTS (Full Text Search) 기능을 제공하기 위한 색인 데이터를 생성함. 색인 데이터는 일반 데이터와 별도로 관리되므로 색인데이터를 활용하여 삭제된 메시지를 복구하는 방법을 개발함.

▶ 기술이전

■ 무인이동체 보안을 위한 암호장비의 설계 기술

✓ 무인이동체에서 수집하는 데이터에 대하여 안전한 저장 및 전송뿐만 아니라 5G+ 기반 무인이동체 제어 데이터 통신을 안전하게 하는 암호장비 개발을 위한 기술임

■ 검증필암호모듈 KMULiB v2.1 기술

✓ Linux 및 Windows 기반 암호장비들을 위한 KMULiB v2.1 검증필암호모듈과 응용방법을 이전하였음

■ 화이트박스 암호화 기술

✓ 블록암호 LEA의 안전성을 강화한 WF-LEA를 통해 화이트박스를 구현하는 기술임

■ LEA 블록암호의 화이트박스 암호 구현 장치 및 방법 외 특허 1건 통상실시권 이전

✓ 블록암호 LEA의 4비트 치환함수를 이용한 화이트박스 암호 기술임

▶ 소프트웨어 등록

■ UHSDM(유에이치에스디엠)용 수중 가시광선 및 적외선 무선 통신 송신 출력 제어 프로그램

- S-DTN(seamless DTN)을 이용한 수중에서의 진보된 다이버 네트워크의 연결성을 보장하기 위한 소프트웨어임

4. 신진연구인력 현황 및 실적

▶ 연구교수 윤승환의 연구 활동

■ 암호모듈 및 보안제품의 평가/인증 방법에 기반한 설계, 구현에 관한 연구

■ 고속의 양자난수발생기 기반 5G+/6G 이동통신 보안 플랫폼 설계, 구현에 관한 연구

■ 자문 활동

✓ 양자난수 발생기에서 발생한 엔트로피와 FPGA를 활용한 스트림암호 모듈 개발에 대한 설명 및 실습 자문(2021.04.28.~2021.12.28.), 경기과학고등학교

✓ 라즈베리파이를 이용한 진난수 생성기 구현하는 방법에 대한 실습 자문(2022.01.25.), 경기과학고등학교

✓ 무선 통신 기술에 적용될 수 있는 키 교환 프로토콜 제안에 대한 자문(2022.05.01.~2022.12.31.), 경기과학고등학교

✓ 타원곡선 암호를 이용한 이미지 암호화 알고리즘 연구에 대한 자문(2022.05.01.~2022.12.31.), 경기과학고등학교

■ 국제 학회

✓ “Analysis of 5G AKA vulnerabilities through 5G Simulator,” SeoWoo Jung, Seunghwan Yun, Okyeon Yi, International Conference on Future Information & Communication Engineering (ICFICE 2022)

■ 국내 학회

✓ “양자 암호모듈 기반 드론 식별 및 정보 제공 기술 구현에 대한 연구,” 정서우, 윤승환, 이옥연, 2021년 한국정보보호학회 동계학술대회 (CISC-W’21)

▶ 연구교수 이재훈의 연구 활동

■ 다양한 네트워크 환경 및 IoT 기술을 활용한 융합보안 연구를 수행하고 있으며, 무인항공시스템, 국가기반시설 보안 설계 및 적용 연구, 상용 암호모듈의 호환성 관련 연구 등을 수행하고 있음

■ 무인항공시스템 보안 연구

✓ 무인항공 상호호환 가능한 보안 구조 설계 방안 연구

✓ 무인항공기 보안 체계 및 모듈 설계에 관한 연구

✓ 무인항공시스템 키 관리 체계 방안 연구

✓ 무인항공시스템 보안에이전트 설계 및 가용성 실험 연구

■ 국가기반시설 및 공공기관, 군 관련 보안 연구

✓ 국가 중요 기반 시설 산업제어 시스템 및 CCTV 보안 기술 연구 실증 시험

✓ 차세대 자율주행 교통신호제어 정보 수집 네트워크 가상사설망 구조 분석 및 자문

✓ 해군사관학교 및 공군사관학교 경계 감시 드론 보안 실증 시험

✓ 도서간 드론 운송 사업 보안 적용 사업 실증 시험

✓ 국립공원 관리 드론 시범 운행 사업 자문

✓ 군용 무인항공기 키 주입 시스템 설계 및 실증 연구

✓ 지자체 상하수도 관리 산업제어 시스템 보안 적용 사업 연구

✓ 상용암호모듈 군 도입 방안 연구 및 암호모듈 개발/평가

■ 교내학술연구

✓ 오프라인 환경에서의 인증체계 연구 세미나

✓ 드론 비행기록 장치 관련 연구 세미나

▶ 연구교수 박명서의 연구 활동

■ 암호 및 디지털 포렌식 분야 교육활동, 서원대학교

✓ 서원대학교 소프트웨어학부 소프트웨어응용 전공 에서 시간강사(2020~2021)

■ 스마트폰 백업 프로토콜 분석 연구
✓ 스마트폰 백업 프로토콜을 역으로 구현하여 백업기반 자동화된 데이터 추출 기법 개발
■ 암호화된 백업 데이터의 복호화에 관한 연구
✓ 암호화된 백업 데이터의 복호화 방안을 개발하여 백업 데이터의 포렌식적 활용 방법 제안

5. 참여교수의 교육역량 대표실적

▶ 인재 양성을 위한 노력

■ ‘무선보안특강’, ‘암호모듈평가및검증’ 등 다양한 교육 내용을 통해 KCMVP와 양자암호에 대한 이해와 더불어 검증필 암호모듈을 현실에 활용할 수 있는 방안에 대해 고찰할 수 있도록 하여 지식을 심어 주었음

■ 수중에서 고성능 수중통신 기술을 실현하기 위한 핵심 요소기술 ‘UHSDM, S-DTN(Seamless Delay Tolerant Network), 채널 선택 메커니즘, 핸드오버 메커니즘’의 기술 개발 및 논문지도, 극한지에서 센서 장치들의 데이터를 효율적으로 수거하기 위한 우선순위 설정, DTN기반 노드 및 메시지 메커니즘 논문지도를 위한 교육 일정을 수립, 델핀라즈(졸업), 염선호, 황아리, 신하 쉬르티카 연구원의 연구력 향상을 위한 세미나, 외부 도메인 전문가를 초빙 등을 진행하였음.

■ 유일선 교수는 ‘정보보호프로토콜’ 과목을 개설하여 초연결 시대의 핵심분야인 이동통신과 사물인터넷을 위한 보안 프로토콜과 보안 프로토콜의 정형화 검증기술을 강의함으로써 대학원생들의 전문·연구역량 강화에 기여함

▶ 강연

■ PQC 대전환시대 국내 기술 경쟁력 확보 전략 (2021.10.05.), 양자보안워크숍
✓ PQC 대전환시대 국내 암호 기술 경쟁력을 높이기 위한 전략에 대한 강연

■ 컴파일러 최적화 옵션은 부채널 분석에 아군인가? 적군인가? (2021.10.28.), 부채널정보분석 워크숍
✓ 소프트웨어 컴파일러에 따른 마스킹 대응기법의 취약점에 대한 강연

■ PQC 전환 준비 – 인력양성 및 시험 평가 (2021.11.09.), KISA
✓ PQC 전환에 대비한 인력양성 방향성 및 시험 평가 방법에 대한 강연

■ 부채널 분석 최신기술 동향 (2021.12.23.), 국립전파연구원
✓ 전자파로 활용 가능한 부채널 분석 최신기술 동향에 대한 강연

■ IC 칩 해킹 및 복제 가능 시나리오 교육 (2022.01.21.), KISA
✓ 금융 IC 카드에서 발생 가능한 부채널 공격 위협 및 사례에 대한 강연

■ 부채널 분석 방지 기술 특강 (2020.11.12.), 국방과학연구소
✓ 부채널 공격 방법 및 중요성 그리고 이에 대한 다양한 대응기법에 대한 강연

■ 양자내성암호 최적화 구현 동향 소개(2021.10.14.), 한국암호포럼
✓ IoT, 서버 환경에서의 PQC 최적화 구현 동향 및 분석에 대한 강연

■ 경량암호 및 양자내성암호 동향 소개(2021.10.25.), 삼성전자 무선사업부
✓ LWC 및 PQC의 현재 공모전 진행사항 및 최신 구현기법 분석에 대한 강연

■ 정보보호 전문가를 위한 암호교육(2022.03.23. ~ 2022.03.25.), 한국암호포럼
✓ KCMVP 개발을 위한 암호모듈 인터페이스 및 암호모듈 경계 등에 대한 강연

■ 암호모듈검증 KCMVP 전문교육 온라인 과정 (2022.05.03.~2022.05.04.) 한국인터넷진흥원
✓ KCCMVP 개발을 위한 암호 모듈 설계 방안 등에 대한 강연

■ IIMB-Lite: Lightweight Misbehavior Detection Approach for Insulin Infusion System(2022.5.50), ACM on ASIA Public-Key Cryptography
✓ 인슐린 주입 시스템을 위한 경량 오동작 감지 방법에 대한 강연

■ 독립형 5G 인증과 보안 기술(2022.06.07.), 국민대

✓ 독립형 5G 인증과 보안 기술에 관련 강연

▶ 워크숍

■ 제4회 부채널정보분석 워크숍(2021.10.28.~2021.10.29.)

✓ 부채널정보분석 워크숍을 주관하여 개최함

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 2건, 국제 학회 1건의 논문을 발표하였음

■ 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 수행하였음

■ 유일선 교수팀은 오세아니아 최정상급 명문대 보안관련 연구센터 혹은 연구실과 협력의향서를 체결함

✓ 2022년 5월 14일: 호주 월런공대학교 Institute of Cybersecurity and Cryptology (Director: Willy Susilo 교수)

✓ 2022년 5월 14일: 일본 큐슈대학교 사이버보안연구센터 (센터장: Kouichi SAKURAI 교수)

✓ 2022년 5월 14일: 대만 대만국립대학교 공성능 및 과학 컴퓨팅 센터 (센터장: Chi-Sheng SHIH 교수)

✓ 2022년 5월 14일: 중국 북경대학교 정보보호연구실 (Director: Zhong CHEN 교수)

✓ 2022년 5월 14일: 홍콩 홍콩대학교 핀테크 및 블록체인 연구실 (지도교수: Siu Ming YIU 교수)

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 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

■ 당초 계획인 파견 기간 9개월 이내에 SCIE급 3건, 기술문서 6건에 비해 SCIE급 논문의 정량적 목표를 달성하지 못했으나 이것은 저널사의 지연으로 인한 것으로, 나머지 한 논문은 현재 마이너 리뷰 단계이기에 곧 달성할 것으로 판단됨

■ 국민대학교와 조지아 주립대 간의 교류를 넓힐 기회로 활용될 것으로 보이며, 이것은 더 많은 긍정적인 학술적 효과를 낼 수 있을 것으로 기대됨

Ⅲ 연구역량 영역

□ 연구역량 대표 우수성과

▶ 자체평가 대상 기간 내 국제 저널 22편, 국내 저널 5편, 국제 학회 3편, 국내 학회 34편의 논문 발표, 수상 23건, 특허 (등록 15건/출원 10건) 등의 성과를 냄

▶ 국제 저널

- “Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-Based Profiling”, JeaSeung Han, TaeHo Lee, JiHoon Kwon, JooHee Lee, Il-Ju Kim, JiHoon Cho, Dong-Guk Han, and Bo-Yeon Sim, IEEE ACCESS. (SCIE, I.F=3.367)
- “Profiling Attack against RSA Key Generation Based on a Euclidean Algorithm”, Sadiel de la Fe, Han-Byeol Park, Bo-Yeon Sim, Dong-Guk Han, and Carles Ferrer, MDPI Information. (SCOPUS)
- “Improved Correlation Power Analysis on Bitslice Block Ciphers”, JeaSeung Han, Yeon-Jae Kim, Soo-Jin Kim, Bo-Yeon Sim, and Dong-Guk Han, IEEE ACCESS. (SCIE, I.F=3.367)
- “Deep-Learning-Based Side-Channel Analysis of Block Cipher PIPO With Bitslice Implementation”, Ji-Eun Woo, Jaeseung Han, and Dong-Guk Han, IEEE ACCESS. (SCIE, I.F=3.367)
- “Single-Byte Error-Based Practical Differential Fault Attack on Bit-Sliced Lightweight Block Cipher PIPO”, Seonghuuck Lim, Jaeseung Han, and Dong-Guk Han, IEEE ACCESS. (SCIE, I.F=3.367)
- “Experimental evaluation of differential fault attack on lightweight block cipher PIPO”, Seonghuuck Lim, and Dong-Guk Han, IET Information Security. (SCIE, I.F=1.371)
- “Novel Shuffling Countermeasure for Advanced Encryption Standard (AES) against Profiled Attack in Mobile Multimedia Services”, JongHyeok Lee, Jiyoon Kim, and Dong-Guk Han, Wireless Communications and Mobile Computing. (SCIE, I.F=2.146)
- “Secure and Optimal Secret Sharing Scheme for Color Images”, K.Shankar, David Taniar, Eunmok Yang, Okyeon Yi, Mathematics (SCIE, IF=2.258)
- “Convolution Neural Network-Based Sensitive Security Parameter Identification and Analysis”, Hyunki Kim, Donghyun Kim, Okyeon Yi, Hindawi WCMC (SCIE, IF=2.336)
- “Fast Implementation of SHA-3 in GPU Environment”, Hojin Choi and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “High-Speed Fault Attack Resistant Implementation of PIPO Block Cipher on ARM Cortex-A”, JinGyo Song, YoungBeom Kim and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “CRYSTALS-Dilithium on ARMv8”, YoungBeom Kim, JinGyo Song and Seog Chung Seo, Security and Communication Networks (SCIE, IF = 1.791)
- “Designing a New XTS-AES Parallel Optimization Implementation Technique for Fast File Encryption”, SangWoo An and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “Efficient Implementation of AES-CTR and AES-ECB on GPUs with Applications for High-speed FrodoKEM and Exhaustive Key Search”, Wai-Kong Lee, HwaJeong Seo, Seog Chung Seo, and Seong Oun Hwang, IEEE Transactions on Circuits and System II: Express Briefs (SCIE, IF = 3.292)
- “Accelerating Falcon on ARMv8”, YoungBeom Kim, JinGyo Song and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “Efficient Parallel Implementations of PIPO Block Cipher on CPU and GPU”, Hojin Choi and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)

- “Parallel Implementation of CRYSTALS-Dilithium for Effective Signing and Verification in Autonomous Driving Environment”, Seog Chung Seo, and SangWoo An, ICT Express (SCIE, IF = 4.754)
- “Optimized Implementation of PIPO Block Cipher on 32-bit ARM and RISC-V Processors”, YoungBeom Kim and Seog Chung Seo, IEEE Access (SCIE, IF = 3.367)
- “A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things”, Delphin Raj Kesari Mary, Eunbi Ko, Seung-Geun Kim, Sun-Ho Yum, Soo-Young Shin, Soo-Hyun Park, Sensors
- “A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application”, Hangi Kim, Yongjin Jeon, Giyoon Kim, Jongsung Kim, Boyeon Sim, Dongguk Han, Hwajeong Seo, Seonggyeom Kim, Seokhie Hong, Jaechul Sung, Deukjo Hong, IEEE ACCESS (I.F 3.745)
- “Differential uniformity and linearity of S-boxes by multiplicative complexity”, Yongjin Jeon, Seungjun Baek, Hangi Kim, Giyoon Kim, Jongsung Kim, Cryptography and Communication (I.F 1.73)
- “Speeding Up LAT: Generating a Linear Approximation Table Using a Bitsliced Implementation”, Giyoon Kim, Yongjin Jeon, Jongsung Kim, IEEE ACCESS (I.F 3.745)
- “Quantum cryptanalysis of the full AES-256-based Davies-Meyer, Hirose and MJH hash functions”, Seungjun Baek, Sehee Cho, Jongsung Kim, Quantum Information Processing (I.F 2.349)
- “A Study on Data Acquisition based on the Huawei Smartphone Backup Protocol”, Myungseo Park, Sehoon Lee, Okyeon Yi, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, I.F 2.395)
- “A Reused Key Attack on an Encrypted Mobile App Database: Case Study on KakaoTalk and ProtonMail”, Uk Hur, Myungseo Park, Jongsung Kim, Journal of Information Security and Applications (SCIE, I.F 3.872)
- “Forensic analysis of note and journal applications”, Sumin Shin, Giyoon Kim, Soram Kim, JongsungKim, Forensic Science International: Digital Investigation (SCIE, I.F 2.395)
- “Methods for recovering deleted data from the Realm database: Case study on Minitalk and Xabber”, Soram Kim, Giyoon Kim, Sumin Shin, Byungchul Youn, Jian Song, Insoo Lee, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, I.F 2.395)
- “Methods for decrypting the data encrypted by the latest Samsung smartphone backup programs in Windows and macOS” Soojin Kang, Giyoon Kim, Myungseo Park, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, I.F 2.395)
- “A study on LG content lock and data acquisition from apps based on content lock function”, Giyoon Kim, Myungseo Park, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, I.F 2.395)
- “Improved See-In-The-Middle Attacks on AES”, Jonghyun Park, Hangi Kim, Jongsung Kim, ICISC 2021, LNCS 13218, pp. 271-279, Springer, 2022.
- “A Study on the New Saturnin S-box with Improved Implementation Efficiency“, Hangi Kim, Jongsung Kim, Platform Technology Letters
- “Quantum cryptanalysis of the full AES-256-based Davies-Meyer, Hirose and MJH hash functions“, Seungjun Baek, Sehee Cho, Jongsung Kim, Quantum Information Processing (I.F 2.349)
- “Speeding Up LAT: Generating a Linear Approximation Table Using a Bitsliced Implementation“, Giyoon Kim, Yongjin Jeon, Jongsung Kim, IEEE ACCESS (I.F 3.745), Vol 10
- “Differential uniformity and linearity of S-boxes by multiplicative complexity“, Yongjin Jeon, Seungjun Baek, Hangi Kim, Giyoon Kim, Jongsung Kim, Cryptography and Communication (I.F 1.73)
- “Optimizing High-Speed Mobile Networks with Smart Collaborative Theory”, Fei Song, Letian Li, Ilsun

You, Shui Yu, Hongke Zhang, IEEE ACCESS (SCIE, IF=3.476)

- “A Secrecy Transmission Protocol with Energy Harvesting for Federated Learning”, Ping Xie, Fan Li, Ilsun You, Ling Xing, Honghai Wu, Huahong Ma, MDPI Sensors (SCIE, IF=4.35)
- “Federated intelligence of anomaly detection agent in IoTMD-enabled Diabetes Management Control System”, Philip Virgil Astillo, Daniel Gerbi Duguma, Hoonyong Park, Jiyoon Kim, bonam Kim, IlsunYou, Future Generation Computer Systems. (SCIE, IF=7.187)
- “Session Management for Security Systems in 5G Standalone Network”, Seongmin Park, Sungmoon Kwon, Youngkwon Park, Dowon Kim, Ilsun You, IEEE ACCESS (SCIE, IF=3.476)

▶ 국내 저널

- “극한지 환경에서 무인기를 이용한 MQTT 기반 극한지 생물용 바이오로거 데이터 원격 회수 시스템 구현”, 이정국, 염선호, 이진영, 황아리, 채지윤, 임지영, 임용곤, 최유성, 박수현, 전자공학회논문지 2022년 8월호
- “Gohr의 Speck32/64 신경망 구분자에 대한 분석과 Simon32/64에의 응용”, 성효은, 유현도, 염용진, 강주성, 정보보호학회논문지 2022년 4월 호
- “블록암호 PRESENT에 대한 향상된 SITM 공격”, 박종현, 김한기, 김종성, 정보보호학회논문지, 32권, 2호
- “양자 컴퓨팅 환경에서의 해시함수 충돌쌍 공격 동향”, 백승준, 조세희, 김종성, 정보보호학회지 2022년 2월 호
- “Vault 앱의 데이터 암호화 알고리즘 및 은닉 알고리즘 분석”, 최용철, 김기윤, 김종성, 디지털포렌식연구, 15권 4호, 2021
- “양자 컴퓨팅 환경에서의 Ascon-Hash에 대한 Free-Start 충돌 공격“, 조세희, 백승준, 김종성, 정보보호학회논문지, 32권, 4호
- “GIFT-128에 대한 SITM 공격: NIST 경량암호 최종 후보 GIFT-COFB 적용 방안 연구”, 박종현, 김한기, 김종성, 정보보호학회논문지, 32권, 4호
- “AND 연산자 축적을 통한 경량 S-boxes 생성 방법“, 전용진, 김종성, 정보보호학회논문지, 32권, 3호
- “안드로이드 환경에서의 지도 애플리케이션 아티팩트 분석 및 복호화 방안 연구“, 박귀은, 강수진, 김종성, 디지털포렌식연구, 16권 2호
- “안드로이드 기반 클라우드 스토리지 앱 크리덴셜 활용 및 아티팩트 분석“, 최용철, 김기윤, 김종성, 디지털포렌식연구, 16권 2호

▶ 국제 학회

- “Deep Learning-based Side-Channel Analysis on PIPO”, Ji-Eun Woo, Jaeseung Han, Yeon-Jae Kim, Hye-Won Mun, SeongHyuck Lim, Tae-Ho Lee, Seong-Hyun An, Soo-Jin Kim, and Dong-Guk Han, The 24th Annual International Conference on Information Security and Cryptology (ICISC 2021)
- “Differential Fault Attack on Lightweight Block Chiper PIPO”, SeongHyuck Lim, Jaeseung Han, Tae-Ho Lee, and Dong-Guk Han, The 24th Annual International Conference on Information Security and Cryptology (ICISC 2021)
- “Illegal Photo Shoot Detection Method Using Operating Frequency of Smartphone Camera”, Seong-Hyun An, Ji-Woo, Lee, and Dong-Guk Han, The 23th World Conference on Information Security Applications (WISA 2022)
- “Analysis of 5G AKA vulnerabilities through 5G Simulator”, SeoWoo Jung, Seunghwan Yun, Okyeon Yi, IEEE Region 10 Symp (2022 ICFICE)

■ “Analysis of Radioactive Decay Based Entropy Generator in the IoT Environments“, Taewan Kim, Seyoon Lee, Seunghwan Yun, Jongbum Kim, Okyeon Yi, 2022 한국정보보호학회 WISA

■ “Telecommunication for Quantum Computer”, Seyoon Lee, Taewan Kim, Changuk Jang, Okyeon Yi, 2022 한국정보보호학회 WISA (포스터)

■ “Efficient parallel implementation methods of LSH-512 utilizing SIMD AVX-512”, Hojin Choi and Seog Chung Seo, The 23rd World Conference on Information Security Applications (WISA 2022 Poster Section)

■ “MFT: Metamorphic Fuzz Testing for Efficient Correctness Validation of Cryptographic Implementation”, HyungJoon Yoon, YoungBeom Kim, Yongryeol Choi and Seog Chung Seo, The 23rd World Conference on Information Security Applications (WISA 2022 Poster Section)

■ “Metamorphic Testing on NIST LWC Finalists”, Yongryeol Choi, YoungBeom Kim and Seog Chung Seo, The 23rd World Conference on Information Security Applications (WISA 2022 Poster Section)

■ “MUD for Infusion Pumps: An Attempt to Reduce Network-based Attacks”, Daniel Gerbi Duguma, Gunwoo Kim, Bonam Kim, Ilsun You, The 23st World Conference on Information Security Applications (WISA 2022)

▶ 국내 학회

■ “효율적인 교차 디바이스 부채널 분석을 위한 프로파일링 디바이스 선택 방법”, 안성현, 임성혁, 이종혁, 한동국, 2021 한국군사과학기술학회 종합학술대회

■ “경량암호 PIPO에 대한 신경망 및 라벨 설정에 따른 프로파일링 부채널 분석”, 김수진, 우지은, 김연재, 안성현, 문혜원, 한동국, 2021 한국정보보호학회 동계학술대회

■ “딥러닝 기반 비프로파일링 이차 부채널 분석 성능 향상 기법에 관한 연구”, 임성혁, 문혜원, 한동국, 2021 한국정보보호학회 동계학술대회

■ “딥러닝을 활용한 스마트폰 카메라 불법 촬영 탐지 방안”, 안성현, 이현호, 우지은, 김연재, 한동국, 2021 한국정보보호학회 동계학술대회

■ “AES CTR 모드에 대한 향상된 전력분석 기법”, 한재승, 한동국, 2022 한국정보보호학회 하계학술대회

■ “ARIA 암호 알고리즘에의 전력 글리치 다중 오류 주입 공격”, 이종혁, 임성혁, 문혜원, 한동국, 2022 한국정보보호학회 하계학술대회

■ “NIST PQC Round 3 격자 기반 PKE KEM의 소프트웨어 하드웨어 구현에 대한 부채널 분석 동향”, 김수진, 한동국, 2022 한국정보보호학회 하계학술대회

■ “글로벌 IT 보안 기업 CENSUS 사 Masked AES software library에 대한 잔여 1차 부채널 취약점 분석”, 김연재, 한동국, 2022 한국정보보호학회 하계학술대회

■ “이종 디바이스 환경에서의 비지도 도메인 적응을 이용한 신규 프로파일링 부채널 분석”, 우지은, 한동국, 2022 한국정보보호학회 하계학술대회

■ “장치의 열 방출량을 이용한 오류 주입 공격 성공률 향상 방안 연구”, 문혜원, 지재덕, 한동국, 2022 한국정보보호학회 하계학술대회

■ “TCP 통신 환경 암호장비에 대한 최적화 요소 분석”, 한주홍, 이옥연, 2021 한국정보보호학회 동계학술대회

■ “서버에서의 양자내성암호 기반 통합 암호 체계 제안”, 이세윤, 김태완, 이옥연, 2021 한국정보보호학회 동계학술대회

■ “안드로이드 애플리케이션 인증방식의 취약점 분석 및 동향”, 윤혜진, 이옥연, 2021 한국정보보호학회 동계학술대회

■ “난수발생기에 따른 UDM 인증 벡터 생성 속도 분석”, 김태완, 이옥연, 2021 한국정보보호학회 동계학술대회

- “양자 암호모듈 기반 드론 식별 및 정보 제공 기술 구현에 대한 연구”, 정서우, 윤승환, 이옥연, 2021 한국정보보호학회 동계학술대회
- “BB84 프로토콜 분석 및 양자 키 분배 표준화 동향”, 김형엽, 이옥연, 2021 한국정보보호학회 동계학술대회
- “UTM 내 드론에서 사용 가능한 보안 파라미터 딥러닝 기반 탐지”, 김현기, 김태완, 이옥연, 2022 한국인터넷정보학회 춘계학술발표대회
- “검증필 암호모듈 기반 드론 식별 체계 연구“, 김태완, 이세윤, 윤승환, 이옥연, 2022 한국정보보호호학회 하계학술대회
- “상용 드론의 군 도입을 위한 검증필 암호모듈 상호호환 운용 환경 요구사항”, 정서우, 김현기, 이옥연, 2022 한국정보보호호학회 하계학술대회
- “드론 비행 데이터 저장 방법에 대한 연구”, 김형엽, 김태완, 이재훈, 이옥연, 2022 한국정보보호호학회 하계학술대회
- “오프라인 환경의 디바이스에 인증을 위한 AHS 프로토콜 제안“, 윤혜진, 장찬국, 이재훈, 이옥연, 2022 한국정보보호학회 하계학술대회
- “한국형 UTM 내부 양자 보안 아키텍처 설계”, 이세윤, 김태완, 위한샘, 이옥연, 2022 한국정보보호학회 하계학술대회
- “ARM Cortex-A 환경에서 Falcon Round 3의 FFT 곱셈 최적화 연구”, 송진교, 김영범, 서석충, 2021 한국정보보호학회 동계학술대회
- “키 유도함수에 대한 Metamorphic Testing 설계”, 김영범, 송진교, 서석충, 2021 한국정보보호학회 동계학술대회
- “GPU 환경에서의 16-bit 자료형을 활용한 PIPO 암호 알고리즘 최적화 방안”, 최호진, 서석충, 2021 한국정보보호학회 동계학술대회
- “CUDA GPU 환경에서의 Falcon Fast Fourier Sampling 연산을 위한 이중 재귀함수의 반복문 대체 기법”, 안상우, 서석충, 2021 한국정보보호학회 동계학술대회
- “블록체인의 구조적 문제 및 암호학적 취약점에 대한 동향 조사”, 김동천, 김영범, 서석충, 2021 한국정보보호학회 하계학술대회
- “PQC-DSA 기반 블록체인 기술 동향 조사”, 김동천, 서석충, 2022 한국통신학회 동계종합학술발표회
- “자율주행환경에서 PQC 적용분석을 위한 V2Verifier 분석 및 확장”, 김영범, 서석충, 2022 한국통신학회 동계종합학술발표회
- “CPU 환경에서 최신 경량 암호 GIFT-COFB의 최적화 및 속도 개선과 구현”, 최용렬, 김영범, 서석충, 2022 한국통신학회 동계종합학술발표회
- “CPU 환경에서의 AVX-512를 활용한 블록 암호 알고리즘 PIPO 벤치마킹”, 최호진, 서석충, 2022 한국통신학회 동계종합학술발표회
- “NVIDIA GPU 환경에서 효율적인 병렬 작업 수행을 위한 더미 연산 구현 기법”, 안상우, 서석충, 2022 한국통신학회 동계종합학술발표회
- “SIMD AVX-512를 활용한 LEA 병렬 구현 방안”, 최호진, 서석충, 2022 한국정보보호학회 하계학술대회
- “PQC 마이그레이션을 위한 고려사항 분석 및 최신연구 동향 조사”, 강혜리, 김영범, 서석충, 2022 한국정보보호학회 하계학술대회
- “격자기반 다항식 곱셈 최적화 구현 동향”, 김영범, 서석충, 2022 한국정보보호학회 하계학술대회
- “IoT 환경을 위한 경량암호 최적화 동향 분석”, 최용렬, 김영범, 서석충, 2022 한국정보보호학회 하계학술대회
- “자동차 OTA(Over The Air) 업데이트 보안 동향 분석”, 신동현, 김영범, 서석충, 2022 한국정보보호학회 하계학술대회

■ “Patterson 디코딩 기반 Classic McEliece 키 복호 연산에 관한 연구”, 전창열, 김동찬, 2022 한국통신학회 동계학술대회
■ “유한체 상에서의 기약다항식 생성에 관한 연구”, 전창열, 최장혁, 김동찬, 2022 한국통신학회 동계학술대회
■ “유한체의 랜덤 순서 집합 생성 기법에 관한 연구”, 이제원, 전창열, 최장혁, 김동찬, 2022 한국통신학회 동계학술대회
■ “다항식 몫환 F_p[X]/<X^n-1>의 이산 푸리에 변환 기반 곱셈에 관한 연구”, 최장혁, 전창열, 김동찬, 2022 한국통신학회 동계학술대회
■ “유클리드 호제법과 이진 최대공약수 알고리듬을 이용한 최대공약수 고속 계산에 관한 연구”,김영효, 김민지, 이제원, 전창열, 김동찬, 2022 하계 통신학회 종합학술발표회
■ “다항식 몫환 F_p[X]〈X^n+1〉의 NTT 기반 곱셈 연산에 관한 연구”, 이제원, 김민지, 김영효, 전창열, 김동찬, 2022 하계 통신학회 종합학술발표회
■ “경량 암호 CHAM을 사용한 암호학적 난수발생기 GPU 병렬 구현”, 유현도, 강주성, 염용진, 2021 한국통신학회 추계종합 학술발표회
■ “MODBUS 프로토콜의 양자내성암호(PQC) 적용 방안에 관한 연구”, 김원일, 강주성, 염용진, 2021 한국통신학회 추계종합 학술발표회
■ “이미지 센서 기반 난수발생기의 잡음원에 적용 가능한 헬스테스트 설계”, 유현도, 강주성, 염용진, 2021 한국통신학회 동계종합 학술발표회
■ “그래프 기반 PDF 암호시스템 개선 방법에 관한 연구”, 류지은, 강주성, 염용진, 2021 한국통신학회 동계종합 학술발표회
■ “블록암호 SIMECK에 대한 양자회로 설계 및 구현”, 노준영, 백승준, 박종현, 조세희, 김종성, 정보보호학회 동계 학술대회
■ “NIST 경량 해시함수 Ascon-Hash의 양자 충돌쌍 공격을 위한 MILP 모델 개발”, 조세희, 백승준, 김종성, 2022 한국인터넷정보학회 춘계학술발표대회
■ “GIFT-COFB 위조 공격”, 박종현, 김기윤, 김종성, 2022 한국인터넷정보학회 춘계학술발표대회
■ “DPAPI 기반 크리덴셜 위조를 통한 클라우드 데이터 획득 : Cisco Webex 및 Zoom에 대한 사례연구”, 허욱, 김기윤, 김종성, 2022 한국인터넷정보학회 춘계학술발표대회
■ “TMAP 애플리케이션의 사용자 위치 데이터 분석”, 박귀은, 강수진, 김종성, 2022 한국인터넷정보학회 춘계학술발표대회
■ “특정 환경을 위해 설계된 해시함수 및 블록암호 동향”, 조수정, 권주아, 서재원, 이수현, 임효은, 조세희, 박종현, 김종성, 한국정보보호학회 하계 학술대회
■ “S-box 확장구조 효율성 분석“, 전용진, 김종성, 한국인터넷정보학회 춘계학술발표대회
■ “디지털 포렌식 관점에서의 인공지능 활용 동향“, 이용진, 방수경, 박귀은, 김종성, 정보보호학회 하계 학술대회
■ “SNS 애플리케이션의 디지털 포렌식 동향“, 박세준, 원채은, 이민정, 김종성, 정보보호학회 하계 학술대회
■ “iOS 및 Android Vault 앱 암호화 알고리즘 분석 및 패스워드 복구 방안“, 최용철, 김기윤, 김종성, 디지털포렌식 하계 학술대회
■ “이음 5G에서 허위기지국 탐지 정확도를 향상하기 위한 연합 학습 시스템 연구”, 박훈용, 손대현, 김건우, 유일선, 2022 한국정보보호학회 하계학술대회(CISC-S’22)
■ “IoV 네트워크에서의 BAN 논리를 이용한 정형화 검증”, 오종민, 손대현, 김보남, 유일선, 2022 한국정보보호학회 하계학술대회(CISC-S’22)
■ “블록체인 기반의 스마트 HACCP 구축 사례 연구”, 김건우, 임아정, 김보남, 유일선, 2022 한국정보보호

학회 하계학술대회(CISC-S’22)

- “5G 네트워크상에서 Braeken이 제안한 대칭키 기반의 5G-AKA 인증 프로토콜 BAN Logic 정형화 검증”, 손대현, 박훈용, 김보남, 유일선, 2022 한국융합보안학회 하계학술대회
- ” 웨어러블 디바이스 클라우드 프로토콜에서의 정형화 검증 “, 오종민, 김지윤, 김보남, 유일선, 2022 한국융합보안학회 하계학술대회
- ” 5G NSA 네트워크에서의 블록체인 기술 기반 키 관리를 위한 Lee-Ma 보안 프로토콜 취약점 분석 “, 김건우, 임아정, 김보남, 유일선, 한국융합보안학회 하계학술대회

▶ 수상

- 과학기술정보통신부장관 표창장
- 대한전자공학회 공로상
- 2021 한국통신학회 추계학술대회 우수논문상
- 2021 국가암호 공모전 대상 1건, 우수상 1건, 장려상 1건, 특별상 1건 수상
- 2021 국가암호 경진대회 대상 1건, 최우수상 1건, 우수상 2건 수상
- 2021 한국정보보호학회 국제논문상 수상
- 2021 한국정보보호학회 동계학술대회 우수논문상 1건, 정보보호학회장상 1건, 행정안전부 장관상 1건 수상
- 2021 한국디지털포렌식학회 KDS 챌린지 장려상 수상
- 2021 사이버안보 논문 공모전 장려상
- 2021 국가 암호기술 전문인력 양성과정 우수상
- 2021 경량 PIPO 대칭키 암호 고속구현, SCA, 활용사례 경진대회 국가보안기술연구소 소장상
- 2022 한국인터넷정보학회 춘계학술발표대회 우수논문상
- 2022 한국통신학회 동계학술대회 우수논문상
- 2022 우수신진연구자 한국인터넷진흥원 원장상 수상
- 2022 한국멀티미디어학회 춘계학술대회 우수논문상
- 2022 한국정보보호학회 하계학술대회 정보보호학회장상
- 2022 한국정보보호학회 하계학술대회 행정안전부 장관상 수상
- 2022 WISA Best Poster Award 수상
- 2022 WISA Best Student Paper Award 수상
- 2022 HACK@SEC 2022 Winners 2nd 수상
- 2022 한국융합보안학회 하계학술대회 우수논문상

▶ 특허

- 차분 오류 공격 방법 및 장치 (등록)
- 블록암호에 대한 상관전력 분석 방법 및 장치 (등록)
- LAC에 대한 부채널 분석 장치 및 방법 (등록)
- 오류 주입 공격 시스템 (등록)
- 오류 주입 공격 장치 및 방법 (등록)
- 전자서명 알고리즘의 부채널 분석 방법 및 그 장치 (등록)
- 양자보안 통신장치 통합형 영상 감시 시스템 및 방법 (등록)
- 양자보안 통신장치 통합형 지능형 교통신호 제어 시스템 및 방법 (등록)
- 양자보안 통신장치 통합형 수배전반 보안 시스템 및 방법 (등록)
- 양자보안 통신장치 통합형 PLC/HMI 제어 시스템 및 방법 (등록)
- 양자보안 통신장치 통합형 자율이동체 이동기록 시스템 및 방법 (등록)

■ 양자보안 통신장치 통합형 자율이동체 식별 시스템 및 방법 (등록)
■ 비행체에서의 잡음원 도출 장치 및 방법 (등록 결정)
■ 양자 엔트로피 기반 일회용 양자 비밀번호 생성 장치 (출원)
■ 안티-인버전 함수를 이용한 화이트박스 암호 인코딩 장치 및 방법 (등록)
■ 미디어 파일에 대한 안티 포렌식 해제 장치 및 방법 (등록)
✓ 미디어 파일 은닉 기능에 대한 은닉 해제 방법에 대한 연구임
■ 경량 블록암호 PIPO에 대한 단일 바이트 오류 기반 신규 차분 오류 공격 (출원)
■ 경량 블록암호 PIPO에 대한 신규 딥러닝 기반 프로파일링 및 비프로파일링 부채널 분석 (출원)
■ 소프트웨어 동작 감지 장치 및 방법 (출원)
■ SHA-3 처리를 위한 그래픽 처리 장치 및 방법 (출원)
■ 기각 시퀀스 테이블을 이용한 기각 샘플링 병렬 최적화 장치, 방법 및 그 방법을 이용한 전자서명 및 암호화 연산 방법 (출원)
■ XTS 최적화를 위한 병렬 처리 장치 및 방법 (출원)
■ 이미지 센서 기반 난수발생기 헬스 테스트 장치 및 방법 (출원)
■ 일방향 함수를 이용한 암호 운영모드 기반의 화이트박스 암호화 방법 및 장치 (출원)
■ DLBN이 3 이상인 조건을 만족하는 확장 에스박스 및 이를 이용한 비트 연산 방법 (출원)
✓ DLBN이 3 이상인 조건을 만족하는 확장구조와 이를통한 확장 S-box를 개발한 특허임
■ FTS 색인데이터 기반의 삭제 채팅 메시지 복구 장치 및 방법 (출원)
✓ SQLite FTS 데이터베이스의 색인 데이터를 활용하여 삭제된 메시지를 복구하는 특허임

▶ 참여교수 교육대표실적
■ 보안 강연
✓ 양자내성암호 최적화 구현 동향 소개(2021.10.14.), 한국암호포럼
✓ 경량암호 및 양자내성암호 동향 소개(2021.10.25.), 삼성전자 무선사업부
✓ 정보보호 전문가를 위한 암호교육(2022.03.23. ~ 2022.03.25.), 한국암호포럼
✓ 암호모듈검증 KCMVP 전문교육 온라인 과정 (2022.05.03.~2022.05.04.) 한국인터넷진흥원
✓ “IIMB-Lite: Lightweight Misbehavior Detection Approach for Insulin Infusion System”, Ilsun You, Philip Virgil Astillo, ACM on ASIA Public-Key Cryptography (1.741)
✓ 독립형 5G 인증과 보안 기술(2022.06.07.), 국민대

▶ 기술이전
■ 무인이동체 보안을 위한 암호장비의 설계 기술
■ 검증필암호모듈 KMULiB v2.1 기술
■ 화이트박스 암호화 기술
■ LEA 블록암호의 화이트박스 암호 구현 장치 및 방법외 특허 1건 통상실시권 이전

▶ 소프트웨어 등록
■ UHSDM(유에이치에스디엠)용 수중 가시광선 및 적외선 무선 통신 송신 출력 제어 프로그램 등록

▶ 국제 표준
■ ISO/IEC JTC 1/SC 41 국제표준 총회에서 신설된 “해양/수중 IoT 및 디지털 트윈 어플리케이션” 작업반(WG; Working Group)인 WG 7 의장
✓ 2021년 11월 제10차 SC41 국제표준 총회에서 WG 7 의장으로서 회의를 주도함

✓ 2022년 2월 ‘WG 7 1st Open Workshop’ 개최

✓ 2022년 4월 ‘SC41 Webinar on IoT and Digital Twin Standardization’에서 ‘Maritime IoT and Digital Twin’ 발표

✓ 2022년 5월 제11차 SC41 국제표준 총회에서 WG 7 의장으로서 회의를 주도함

▶ 국내 표준

■ 과기정통부가 발간하는 ‘ICT 표준전략맵’ 작성에 참여하여 수중통신 기술의 국내외 표준화 전략 방향을 제시

✓ 2021년 12월 ICT 표준화전략맵 Ver. 2022 발간

▶ 연구비 수주 실적

■ 자체평가 대상 기간 총 41건의 연구를 수행하였으며, 총연구비 6,483,822,394원, 수입금액 4,957,403,281원을 달성하였음

▶ 연구비 수주실적 표(자체평가 대상 기간 2021.9.1.~2022.8.31.)

총 41건			합계	6,483,822,394	4,957,403,281
연번	과제번호	연구과제명	기간	총연구비	수입금액
1	A2022-0297	국방정보통신망-상용망(5G) 연동을 위한 보안 기술개발	2022-04-01~ 2022-12-31	200,000,000	200,000,000
2	A2022-0172	“국방 KCMVP 검증필 OO모듈“을 납품 용역	2022-03-11~ 2022-09-30	250,000,000	125,000,000
3	A2022-0171	드론용 보안 스마트 항공전자 슈트 개발	2022-01-01~ 2022-12-31	480,000,000	144,332,590
4	A2022-0057	5G+ 기반 6G 이동통신 정보보안 기술 연구	2022-01-01~ 2022-12-31	350,000,000	350,000,000
5	A2022-0049	상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구	2022-01-01~ 2022-12-31	150,000,000	0
6	A2022-0053	국가공공 정보시스템 안전성 및 활용성 제고를 위한 차세대 암호체계 개발	2022-01-01~ 2022-12-31	210,000,000	84,000,000
7	A2022-0269	양자내성암호 활용을 위한 전환 정책 및 절차에 관한 연구	2022-04-15~ 2022-10-31	60,000,000	42,000,000
8	A2022-0199	양자컴퓨팅 환경에 대비한 분산자원 플랫폼 관리용 암호 기술 연구(2/3)	2022-02-24~ 2023-02-23	90,000,000	90,000,000
9	A2021-0578	딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발(2차년도)	2021-12-01~ 2022-11-30	100,000,000	45,741,567
10	A2022-0051	무선 은닉채널 위험성 검증 연구	2022-01-01~ 2022-12-31	50,000,000	50,000,000
11	A2022-0054	고신뢰 온-디바이스 딥러닝 가속기 설계를 위한물리채널 기반 취약점 검증 및 대응기술 개발	2022-01-01~ 2022-12-31	144,000,000	144,000,000
12	A2022-0058	(ICT 전문연구실) SCR-Friendly 대칭키 암호 및 응용 모드 개발(2단계-3차년도)	2022-01-01~ 2022-12-31	340,000,000	340,000,000

13	A2022-0078	AI 기반 선도적 실전문제해결 연구인재 양성(3차년도)	2022-01-01~ 2022-12-31	500,000,000	500,000,000
14	A2022-0245	하드웨어 기반 양자내성 PKE/KEM 알고리즘의 안전성 분석 및 대응기술 연구	2022-04-01~ 2022-10-31	45,000,000	28,636,364
15	A2022-0258	AM-01장치 전압 및 전자파 글리칭 기반 보안성 분석 도구 제작	2022-03-14~ 2022-08-31	47,500,000	21,590,909
16	A2022-0268	PQC 알고리즘 구현 최적화 및 부채널분석 대응 최신 기술 연구	2022-04-15~ 2022-10-31	80,000,000	50,909,091
17	A2022-0056	GPU/ASIC 기반 암호알고리즘 고속화 설계 및 구현 기술개발	2022-01-01~ 2022-12-31	330,000,000	330,000,000
18	A2022-0058	(ICT 전문연구실) SCR-Friendly 대칭키 암호 및 응용 모드 개발(2단계-3차년도)	2022-01-01~ 2022-12-31	340,000,000	340,000,000
19	A2022-0196	dm-crypt류 기반 암호화 기법 연구	2022-03-17~ 2022-11-25	130,000,000	7,398,224
20	A2022-0238	랜섬웨어 대응 기술 분석을 통한 필수 검증요소 도출에 관한 연구	2022-04-01~ 2022-10-31	50,000,000	31,818,182
21	A2022-0246	(공동)모바일 기반(iOS) 안티포렌식 소프트웨어 정보은닉 방식 연구	2022-04-01~ 2022-10-31	70,000,000	44,545,455
22	A2022-0255	랜섬웨어 동향 및 암호기능 상세분석 용역	2022-04-06~ 2022-11-30	85,500,000	62,181,818
23	A2022-0092	부호기반 암호의 안전성 및 효율성에 관한 연구(2/3)	2022-03-01~ 2023-02-28	58,864,000	58,864,000
24	A2022-0186	차세대 양자내성 공개키 암호알고리즘에 대한 SW/HW 구현최적화 및 구현적합성 연구(1/5)	2022-03-01~ 2023-02-28	131,246,000	131,246,000
25	A2022-0244	Lattice 기반 PQC 구현적합성 검증방법 및 키 설정 방안 연구	2022-04-01~ 2022-10-31	60,000,000	38,181,818
26	A2022-0025	Flying BS 기반 극지 생물 바이오로거 데이터 원격 회수 기술 개발(3/3)	2022-01-01~ 2022-12-31	82,500,000	57,750,000
27	A2022-0170	극한지 관측 정보 네트워크 구조 설계/검증(2/5)	2022-01-01~ 2022-12-31	120,000,000	50,856,924
28	A2022-0176	수중 SNS 포스팅을 지원하는 다이버 데이터 심리스 커뮤니케이션 개발	2022-01-01~ 2022-12-31	100,000,000	54,817,656
29	A2022-0210	IoT 기반 수중 네트워크 연동 서비스 플랫폼 기술 표준개발(4차년도)	2022-01-01~ 2022-12-31	108,000,000	46,742,288
30	A2022-0239	해상통신 네트워크 연동기술 설계(2/5)	2022-01-01~ 2022-12-31	40,000,000	17,601,529
31	A2022-0295	AI기반 어선안전 설계 데이터플랫폼 개발 및 실증 (1/5)	2022-04-01~ 2022-12-31	80,000,000	22,067,380
32	A2022-0032	모듈형 스마트 패션 플랫폼 연구센터(1/2)	2022-03-01~ 2023-02-28	1,083,000,000	1,000,000,000
33	A2022-0136	단안 영상 기반 사용자 중심 3차원 인터랙션을 위한 경량 비전 기술 연구(2/3)	2022-03-01~ 2023-02-28	95,818,000	95,818,000
34	A2022-0344	Color Consistency 처리 모듈 개발	2022-05-16~	50,000,000	22,727,273

			2022-11-30		
35	A2022-0195	제1형 당뇨환자의 안전하고 신뢰성 있는 치료를 위한 인슐린 펌프 보안 내재화 연구: 비정상행위 탐지 기술 및 보안 프로토콜을 중심으로(1/2)	2022-03-01~ 2023-02-28	130,013,558	130,013,558
36	A2022-0259	5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발	2022-01-01~ 2022-12-31	101,380,836	70,380,836
37	A2022-0334	IoT/IIoT 디바이스 안전성 보장을 위한 취약점 보안검증 기술 개발	2022-04-01~ 2022-12-31	60,000,000	60,000,000
38	A2022-0335	안전한 5G 특화망 도입 및 구축을 위한 보안 고려사항 연구	2022-04-01~ 2022-11-30	50,000,000	50,000,000
39	S2022-0052	화이트박스암호 기반 키보호 메커니즘 개발	2022-05-16~ 2022-08-15	22,000,000	10,000,000
40	S2021-0320	공동활용연구장비-HP 다이버 서버	2021-11-08~ 2021-11-12	200,000	181,819
41	S2021-0324	크로스미디어 통합광고 효과분석 시범조사	2021-11-08~ 2022-01-31	8,800,000	8,000,000

1. 참여교수 연구역량

1.1 국내 및 해외기관 연구비 수주 실적

<표 3-1> 최근 1년간(2021.9.1.-2022.8.31.) 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(2021.9.1.~2022.8.31.) 실적	비고
정부 연구비 수주 총 입금액	9,858,736	4,775,582	약 1.5배
산업체(국내) 연구비 수주 총 입금액	763,070	181,818	약 0.7배
해외기관 연구비 수주 총 (환산)입금액	0	0	
참여교수 수	10	11	
1인당 총 연구비 수주액	1,062,180	450,673	약 1.3배

1.2 연구업적물

① 참여교수 연구업적물의 우수성

▶ 국제 저널

■ Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-Based Profiling

✓ 후양자 암호 중 NIST 3라운드 후보인 격자 기반 암호 Crystals-Dilithium을 대상으로 단일 파형 분석이 가능한 딥러닝 기반 프로파일링 공격 기법을 제안하였음

■ Improved Correlation Power Analysis on Bitslice Block Ciphers

✓ 비트슬라이스 암호의 상관전력분석 성능 향상을 위한 비트별 분석 성능을 예측 기법을 제안하였음

■ “Deep-Learning-Based Side-Channel Analysis of Block Cipher PIPO With Bitslice Implementation”
  ✓ 비트슬라이스 암호 PIPO에 대한 딥러닝 기반 부채널 분석 기법을 제안하였음
■ “Experimental evaluation of differential fault attack on lightweight block cipher PIPO”
  ✓ 비트슬라이스 암호 PIPO에 대한 단일 비트 반전 기반 차분 오류 공격을 제안하고 EM-FI를 수행하였음
■ “Single-Byte Error-Based Practical Differential Fault Attack on Bit-Sliced Lightweight Block Cipher PIPO”
  ✓ 비트슬라이스 암호 PIPO에 대한 단일 바이트 오류 기반 신규 차분 오류 공격을 제안하고 EM-FI를 수행하였음
■ “Novel Shuffling Countermeasure for Advanced Encryption Standard (AES) against Profiled Attack in Mobile Multimedia Services”
  ✓ 모바일 환경에서의 AES 프로파일링 공격에 대한 신규 셔플링 대응기법을 제안하였음
■ Secure and Optimal Secret Sharing Scheme for Color Images
  ✓ 하이브리드 최적 SIMON 암호로 보안(k, k) 다중 비밀 공유(SKMSS) 체계를 개발하여 이미지를 보호할 때 더 많은 계산을 수행한 후에도 비밀 이미지의 품질이 유지 가능하도록 하였음
■ A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things
■ Quantum cryptanalysis of the full AES-256-based Davies-Meyer, Hirose and MJH hash functions
  ✓ AES-256 기반의 DM, Hirose, MJH 해시함수에 대한 양자환경에서의 충돌쌍 공격을 제안하였음
■ A Reused Key Attack on an Encrypted Mobile App Database: Case Study on KakaoTalk and ProtonMail
  ✓ 스트림 암호의 키 재사용 공격 취약점을 활용하여 평문 수집 및 예측을 통한 암호화된 데이터의 복호화 방안을 제안하였음
■ Methods for recovering deleted data from the Realm database: Case study on Minitalk and Xabber
  ✓ Realm 데이터베이스에서 데이터 삭제시 나타나는 특성을 분석하여 실제 애플리케이션을 대상으로 삭제된 메시지의의 복구 방안을 제안하였음
■ Parallel Implementation of CRYSTALS-Dilithium for Effective Signing and Verification in Autonomous Driving Environment
  ✓ GPU 환경에서의 NIST 표준화 대상 양자내성암호 알고리즘인 Crystals-Dilithium 대한 효과적인 연산 처리 방안을 제안하였으며, 자율 주행 환경 프로토콜에서의 성능 평가 결과를 제시하였음
■ Efficient Implementation of AES-CTR and AES-ECB on GPUs with Applications for High-speed FrodoKEM and Exhaustive Key Search
  ✓ GPU 환경에서의 AES-ECB 및 AES-CTR 운용 모드에 대한 최적화 방안을 제안하였음. 해당 방안은 데이터 병렬 암호화를 비롯한 NIST PQC 알고리즘의 키 캡슐화 방안에서 적용 가능함
■ Optimizing High-Speed Mobile Networks with Smart Collaborative Theory
  ✓ 인지 및 지능형 사물 인터넷의 더 나은 커뮤니케이션 솔루션을 구축하기 위해 취약점을 분석하고 MARS(Mobile-Aware Resource Sharing) 개념을 제안하였음.
■ A Secrecy Transmission Protocol with Energy Harvesting for Federated Learning
  ✓ 연합 학습(Federated Learning)에서 딥 러닝의 성능 향상을 위해 비밀 전송 프로토콜을 제안하였음.
■ Federated intelligence of anomaly detection agent in IoTMD-enabled Diabetes Management Control System
  ✓ 이식형 사물 인터넷 의료 기기(IoTMD)에서의 시스템 보안 방어를 위해 딥 러닝 기반 이상 감지 시스템을 제안하였음.
■ Session Management for Security Systems in 5G Standalone Network
  ✓ MUD를 활용하여 필요한 트래픽만 송수신 가능하도록 허용함으로써, 스마트 인퓨전 펌프에 존재하는 취약점을 방지하는 기술에 대해 제안하였음

▶ 국제 학회

■ MUD for Infusion Pumps_ An Attempt to Reduce Network-based Attacks

✓ 5G 핵심 네트워크 보안을 위해 5G StandAlone에서 보안 시스템에 반드시 필요한 사용자를 위한 효율적인 세션 관리 기법을 소개함.

■ Analyzing RRC Replay Attack and Securing Base Station with Practical Method

✓ 3GPP 표준 문서를 기반으로 5G NSA(Non-Standalone) 네트워크에서 RRC(Radio Resource Control) 패킷을 이용한 재생 공격 가능성에 대한 분석을 제시하였음.

▶ 국내 학회

■ 딥러닝 기반 비프로파일링 이차 부채널 분석 성능 향상 기법에 관한 연구

✓ 비프로파일링 이차 부채널 분석에 효율적인 라벨링 기법 및 활성 함수를 제안하였으며 두 바이트 조합이 요구되는 전력 파형에 대한 실험적 평가를 최초로 입증하였음

■ AES CTR 모드에 대한 향상된 전력분석 기법

✓ AES CTR 모드에서 클러스터링 기법을 적용하여 공격 복잡도를 낮추는 방안을 제안하였으며 실험적 평가로 공격의 효율성을 입증하였음

■ ARIA 암호 알고리즘에의 전력 글리치 다중 오류 주입 공격

✓ ARIA 암호 알고리즘을 대상으로 전력 글리치를 이용한 다중 오류 주입 공격 시스템을 구축하고 국내에서 최초로 실험적 평가를 입증하였음

■ 블록체인 기반의 스마트 HACCP 구축 사례 연구

✓ 스마트 HACCP 시스템에서의 블록체인 기술의 적합성 확인 및 구축 사례 분석을 통해 어떤 블록체인 플랫폼이 스마트 HACCP에 효과적인지 분석하였음. 또한 스마트 HACCP에 필요한 선제조건에 대해 제안하였음.

■ 5G NSA 네트워크에서의 블록체인 기술 기반 키 관리를 위한 LEE-Ma 보안 프로토콜 취약점 분석

✓ 블록체인 기반 5G 보안 프로토콜에 대해 정형화 검증 도구인 BAN-Logic을 통해 제안 프로토콜에 대한 취약점 분석을 진행하였음

■ 이음 5G에서 허위기지국 탐지 정확도를 향상하기 위한 연합 학습 시스템 연구

✓ 위치 기반의 허위기지국 탐지 정확성을 학습하여 참여자들의 기계 학습 결과를 바탕으로 연합 학습을 실시한 결과를 통해 탐지 정확성을 향상 시키는 연구를 제안하였음

■ 5G 네트워크상에서 Braeken이 제안한 대칭키 기반의 5G-AKA 인증 프로토콜 BAN Logic 정형화 검증

✓ 5G AKA 프로토콜 상에서 상호인증 보장과 기존의 공개키가 아닌 대칭키를 이용한 Braeken의 프로토콜이 비밀키 K에 대한 인증이 단방향으로 이루어져 있는걸 확인했으며, 개선방안을 제안하였음

■ IoV 네트워크에서의 BAN 논리를 이용한 정형화 검증

✓ IoV 네트워크의 프로토콜을 정형화 검증 도구인 BAN 논리를 이용하여 정형화 검증을 진행하였음. 프로토콜의 안전성을 분석하고 취약점을 발견하여 개선 안을 제안하였음

■ 웨어러블 디바이스 클라우드 프로토콜에서의 정형화 검증

✓ 웨어러블 디바이스 클라우드 상에서의 프로토콜을 정형화 검증 도구인 BAN 논리와 AVISPA Tool을 이용하여 취약점 분석을 진행하였으며, 개선방안을 제안하였음

▶ 국내 저널

■ 극한지 환경에서 무인기를 이용한 MQTT 기반 극한지 생물용 바이오로거 데이터 원격 회수 시스템 구현

■ 극지 생물 바이오로거 데이터 원격 회수를 위한 결함 감내 네트워크

■ Gohr의 Speck32/64 신경망 구분자에 대한 분석과 Simon32/64에의 응용

- Crypto에 제안된 Dodis의 신경만 구분자가 다루지 않았던 성능 향상의 원인을 수학적으로 분석하였음

▶ 국내 특허 등록
- ■ 차분 오류 공격 방법 및 장치 (‘21.09)
- ■ 블록암호에 대한 상관전력 분석 방법 및 장치 (‘21.09)
- ■ LAC에 대한 부채널 분석 장치 및 방법 (‘21.10)
- ■ 오류 주입 공격 시스템 (‘21.11)
- ■ 오류 주입 공격 장치 및 방법 (‘21.12)
- ■ 전자서명 알고리즘의 부채널 분석 방법 및 그 장치 (‘22.03)
- ■ 양자보안 통신장치 통합형 영상 감시 시스템 및 방법 (‘21.12)
- ■ 양자보안 통신장치 통합형 지능형 교통신호 제어 시스템 및 방법 (‘22.01)
- ■ 양자보안 통신장치 통합형 수배전반 보안 시스템 및 방법 (‘22.05)
- ■ 양자보안 통신장치 통합형 PLC/HMI 제어 시스템 및 방법 (‘22.05)
- ■ 양자보안 통신장치 통합형 자율이동체 이동기록 시스템 및 방법 (‘22.05)
- ■ 양자보안 통신장치 통합형 자율이동체 식별 시스템 및 방법 (‘22.05)
- ■ 비행체에서의 잡음원 도출 장치 및 방법 (등록 결정)
- ■ 안티-인버전 함수를 이용한 화이트박스 암호 인코딩 장치 및 방법 (‘21.10)

▶ 국내 특허 출원
- ■ 경량 블록암호 PIPO에 대한 단일 바이트 오류 기반 신규 차분 오류 공격 (‘21.12)
- ■ 경량 블록암호 PIPO에 대한 신규 딥러닝 기반 프로파일링 및 비프로파일링 부채널 분석 (‘21.12)
- ■ 소프트웨어 동작 감지 장치 및 방법 (‘21.03)
- ■ SHA-3 처리를 위한 그래픽 처리 장치 및 방법 (‘21.12)
- ■ 기각 시퀀스 테이블을 이용한 기각 샘플링 병렬 최적화 장치, 방법 및 그 방법을 이용한 전자서명 및 암호화 연산 방법 (‘22.03)
- ■ XTS 최적화를 위한 병렬 처리 장치 및 방법 (‘22.03)
- ■ 이미지 센서 기반 난수발생기 헬스 테스트 장치 및 방법 (‘21.12)
- ■ 일방향 함수를 이용한 암호 운영모드 기반의 화이트박스 암호화 방법 및 장치 (‘21.12)
- ■ 양자 엔트로피 기반 일회용 양자 비밀번호 생성 장치 (22.07)

② 이공계열 참여교수 특허, 기술이전, 창업 실적의 우수성

▶ 소프트웨어 등록
- ■ UHSDM(유에이치에스디엠)용 수중 가시광선 및 적외선 무선 통신 송신 출력 제어 프로그램 등록

▶ 특허 등록
- ■ 차분 오류 공격 방법 및 장치
  - ✓ 모듈로 덧셈의 대수적 표현을 이용한 랜덤 워드 오류 모델 기반의 LEA 대상 차분 오류 공격을 개발한 특허임
- ■ 블록암호에 대한 상관전력 분석 방법 및 장치
  - ✓ 비트 슬라이스 암호에 대한 상관전력 분석 수행 시 비트별 분석 성능 예측하는 방법을 개발한 특허임
- ■ LAC에 대한 부채널 분석 장치 및 방법

✓ 격자기반 암호의 인코딩 연산에 대한 부채널 공격을 방지하기 위한 방법을 개발한 특허임

■ 오류 주입 공격 시스템

✓ 오류 주입 공격시 인위적인 트리거 없이 완화된 환경에서 공격을 수행하는 방법을 개발한 특허임

■ 오류 주입 공격 장치 및 방법

✓ AES 암호의 마지막 라운드 SubBytes 함수를 생략하는 오류를 통한 차분 오류 공격을 개발한 특허임

■ 전자서명 알고리즘의 부채널 분석 방법 및 그 장치

✓ 마스킹된 PQC 전자서명 알고리즘에 대하여 딥러닝 기반 부채널 공격 방법을 개발한 특허임

■ 양자보안 통신장치 통합형 영상 감시 시스템 및 방법

■ 양자보안 통신장치 통합형 지능형 교통신호 제어 시스템 및 방법

■ 양자보안 통신장치 통합형 수배전반 보안 시스템 및 방법

■ 양자보안 통신장치 통합형 PLC/HMI 제어 시스템 및 방법

■ 양자보안 통신장치 통합형 자율이동체 이동기록 시스템 및 방법

■ 양자보안 통신장치 통합형 자율이동체 식별 시스템 및 방법

■ 비행체에서의 잡음원 도출 장치 및 방법 (등록 결정)

■ 안티-인버전 함수를 이용한 화이트박스 암호 인코딩 장치 및 방법

▶ 특허 출원

■ 경량 블록암호 PIPO에 대한 단일 바이트 오류 기반 신규 차분 오류 공격

✓ 국내 경량암호 PIPO에 대하여 현실적인 가정에서 단일 바이트 오류를 기반으로 하는 차분 오류 공격을 개발한 특허임

■ 경량 블록암호 PIPO에 대한 신규 딥러닝 기반 프로파일링 및 비프로파일링 부채널 분석

✓ 국내 경량암호 PIPO에 대하여 딥러닝 기반 효율적인 프로파일링 및 비프로파일링 공격 방법을 개발한 특허임

■ 소프트웨어 동작 감지 장치 및 방법

✓ 딥러닝 기반 스마트폰 카메라 모듈의 동작을 구분해 내는 방법을 개발한 특허임

■ SHA-3 처리를 위한 그래픽 처리 장치 및 방법

■ 기각 시퀀스 테이블을 이용한 기각 샘플링 병렬 최적화 장치, 방법 및 그 방법을 이용한 전자서명 및 암호화 연산 방법

■ XTS 최적화를 위한 병렬 처리 장치 및 방법

▶ 기술이전

■ 무인이동체 보안을 위한 암호장비의 설계 기술

✓ 무인이동체에서 수집하는 데이터에 대하여 안전한 저장 및 전송뿐만 아니라 5G+ 기반 무인이동체 제어 데이터 통신을 안전하게 하는 암호장비 개발을 위한 기술임

■ 검증필암호모듈 KMULiB v2.1 기술

✓ Linux 및 Windows 기반 암호장비들을 위한 KMULiB v2.1 검증필암호모듈과 응용방법을 이전하였음

■ LEA 블록암호의 화이트박스 암호 구현 장치 및 방법 외 특허 1건 통상실시권 이전

✓ 블록암호 LEA의 4비트 치환함수를 이용한 화이트박스 암호 기술임

③ 연구의 수월성을 대표하는 연구업적물 (최근 1년(2021.9.1.-2022.8.31.))

연번	대표연구업적물 설명

1	▶ Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-Based Profiling [한재승, 이태호, 권지훈, 이주희, 김일주, 조지훈, 한동국, 심보연, “Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-Based Profiling” , IEEE ACCESS 9 (2021): 166283-166292.] NIST PQC Round 3 전자서명 최종후보 중 하나인 CRYSTALS-DILITHIUM에 대한 딥러닝 기반 프로파일링 부채널 분석을 제안했다. DILITHIUM의 키생성과 서명생성 과정에 존재하는 NTT연산이 수행될 때 방출되는 전력 정보를 이용했으며 단일 전력 파형만으로 DILITHIUM의 비밀키 s1, s2를 분석했다. 서명생성 과정에서는 s1과 s2 모두 복구할 수 있으나, 키 생성 과정에서는 s1만을 복구할 수 있으므로 s2에 대한 추가적인 공격위치 (샘플링, 덧셈, 라운딩, 패킹)를 제안했다. 본 연구의 결과는 후양자 암호 도입에 앞서 부채널 공격에 대한 안정성 평가 및 대응기법 개발의 필요성을 보여주며 안전한 후양자 암호 설계에 활용될 것으로 기대한다.
2	▶ Improved Correlation Power Analysis on Bitslice Block Cipher [한재승, 김연재, 김수진, 심보연, 한동국, “Improved Correlation Power Analysis on Bitslice Block Cipher” , IEEE ACCESS 10 (2022): 39387-39396.] 비트 슬라이스 구조는 S-Box를 비트별 연산 형태로 변형하여 병렬화하는 구현 방법으로 메모리를 줄이는 등 경량 환경에서 이점을 보인다. 본 연구는 비트슬라이스 구현된 블록암호를 대상으로 효과적인 상관전력분석 기법을 제안했다. 기존 상관전력분석은 레지스터가 갖게 되는 중간값 중 분석에 적절한 중간값을 선택하여 분석을 수행했다. 하지만, 비트슬라이스 블록암호의 경우 위와 같은 방법으로 선택할 수 있는 동등한 값(S-Box의 첫번째 비트, 두번째 비트 등)이 여러개 존재한다. 본 연구에서는 대상암호의 S-Box 연산 특징을 이용해 효과적인 중간값을 탐색하는 알고리즘을 제안했다. 본 연구의 결과는 IoT의 발전에 따른 경량환경에서의 보안 문제가 대두되고 있는 현재 부채널 공격에도 안전한 IoT 환경을 구성하는데 활용될 것으로 기대한다.
3	▶ Secure and Optimal Secret Sharing Scheme for Color Images [K.Shankar, David Taniar, Eunmok Yang, Okyeon Yi, “Secure and Optimal Secret Sharing Scheme for Color Images”, Mathematics 2021, 9, 2360.] 현대의 통신 트렌드로 인해 5G 네트워크에서 생성되고 전송되는 멀티미디어 데이터의 양이 기록적인 수준에 도달했다. 멀티미디어 애플리케이션은 사이버 범죄자에게 공격받고 나중에 불법적인 이유로 사용되는 경향이 있는 개인 데이터를 포함하는 방대한 양의 이미지를 전달한다. 보안은 5G/6G 플랫폼의 새롭고 고유한 기능을 고려하고 채택해야 한다. 암호 절차, 특히 비밀 공유(SS)는 몇 가지 특별한 품질과 용량을 가지고 기밀 데이터를 처리하기 위해 고안될 수 있다. 본 논문은 하이브리드 최적 SIMON 암호로 보안(k, k) 다중 비밀 공유(SKMSS) 체계를 개발했다. 제안된 SKMSS 방법은 비밀 이미지 자체에 대해 해시 및 블록 암호를 수행하는 것을 기반으로 안전하게 생성된 노이즈 구성 요소 집합을 구성한다. 노이즈가 있는 이미지를 기반으로 Hybrid Optimal SIMON 암호로 암호화하여 공유를 생성하여 안전하게 전송된다. 이것은 가벼운 암호화 방법이며 계산 복잡성을 줄이는 데 도움된다. Hybrid Particle Swarm Optimization 기반 Cuck Search Optimization Algorithm은 복구된 비밀 이미지의 피크 신호 대 노이즈 비율 값을 분석하여 키를 생성한다. 이렇게 하면 이미지를 보호할 때 더 많은 계산을 수행한 후에도 비밀 이미지의 품질이 유지된다.

4	▶ Convolution Neural Network-Based Sensitive Security Parameter Identification and Analysis [Hyunki Kim, Donghyun Kim, Okyeon Yi, “Convolution Neural Network-Based Sensitive Security Parameter Identification and Analysis”, Hindawi WCMC, Volume 2022, Article ID 9584894] 잡음원들이 수집될 때 발생되는 정보들을 통해 그들을 식별할 수 있음을 나타낸다. 난수 생성 중 암호모듈에 예측 불가능성을 제공하는 소스들을 수집하는 단계(stage)에서 잡음원들이 식별 가능하다면 그 데이터의 특성에 따라 미래의 값들을 예측이 가능해질 수도 있다. 따라서 임의의 암호모듈을 물리적으로 획득하였을 때, 학습된 모델로 암호모듈에서 사용하는 엔트로피 소스를 식별하여 난수를 분석할 수 있다는 공격 시나리오를 세운다.
5	▶ Fast implementation of SHA-3 in GPU Environment [Hojin Choi and Seog Chung Seo, IEEE Access 9 (2021): 144574-144586] 기존 국제표준 해시함수 SHA-1에 대한 충돌쌍 공격 방안 및 실제 충돌쌍이 제시되었다. 이에 SHA-1과 유사한 구조인 SHA-2에 대한 공격 방법이 제안되었음. 이에 NIST에서는 기존의 국제표준 해시함수와 다른 구조인 Sponge-Structure 및 Keccak Algorithm 기반 SHA-3 국제표준 해시함수를 제안하였음. 하지만 SHA-3는 기존 국제표준 해시함수 대비 소프트웨어 환경에서 느린 성능을 보여줌. 본 연구에서는 GPU 환경에서의 SHA-3 최적화 방안을 제안하였음. SHA-3 내부 구조 분석 및 구조 변경, GPU 인라인 어셈블리 활용, 메모리 사용 최소화 등을 제안하였음. 본 연구는 GPU 아키텍처를 활용하는 소프트웨어 환경 및 서버 환경에서 대량의 메시지를 해싱하는 데이터 관리 측면에서 크게 활용될 것으로 기대됨
6	▶ Accelerating Falcon on ARMv8 [YoungBeom Kim, Jingyo Song and Seog Chung Seo, IEEE Access 10 (2022): 44446 - 44460] 양자 컴퓨터의 발전에 따라 인수분해 및 이산로그를 기반으로 하는 RSA 체계의 공개 키 암호알고리즘 시스템의 큰 위협이 되고 있음. 이에 NIST는 양자 컴퓨터 환경에서 안전한 양자 내성 암호알고리즘 공모전을 진행 중임. 하지만 양자 내성 암호알고리즘은 큰 서명 길이, 큰 키 길이, 성능 부하 등 다양한 고려사항이 존재함. 이에 양자 내성 암호알고리즘의 최적화 연구는 필수적으로 진행되어야 함. Falcon은 NIST PQC 공모전에 제출된 양자 내성 전자서명 알고리즘으로 격자 기반의 수학적 난제를 기반으로 함. Falcon은 FFT, NTT의 연산을 활용하여 내부 구조를 설계하였음. 본 논문에서는 Falcon의 핵심연산인 ARMv8 환경에서의 FFT, NTT 연산 레지스터 스케줄링 설계 및 최적화 방안 도출을 통해 Falcon 연산 최적화 연구 결과를 도출함. 본 연구 결과는 차세대 양자 내성 암호알고리즘 시스템의 전환에서 효과적인 기여를 할 것으로 기대됨.

7	▶ A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things [Delphin Raj Kesari Mary, Eunbi Ko, Seung-Geun Kim, Sun-Ho Yum, Soo-Young Shin, Soo-Hyun Park "A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things", Sensors 21, No. 24: 8262] 기존 IoT의 기술을 발전, 응용시켜 해양학, 다이버 네트워크 모니터링, 심해 탐사 및 조기 경보 시스템 같은 응용 프로그램을 개발되고 있고 제한된 UIoT 환경에는 지상에서 활용되고 있는 암호 프로토콜 및 모듈을 직접 적용할 수 없기 때문에 UIoT 환경에서의 보안 프로그램이 필요하다. 본 연구실에서는 최근 UIoT 시스템의 동향과 수중 디바이스의 보안에 관한 요구사항을 분석 및 반영한 논문을 투고했다.
8	▶ 극한지 환경에서 무인기를 이용한 MQTT 기반 극한지 생물용 바이오로거 데이터 원격 회수 시스템 구현 [이정국, 염선호, 이진영, 황아리, 채지윤, 임지영, 임용곤, 최유성, 박수현 "극한지 환경에서 무인기를 이용한 MQTT 기반 극한지 생물용 바이오로거 데이터 원격 회수 시스템 구현", 전자공학회논문지, Vol.59, No.1, pp.47-59, 2022] 극지는 극심히 낮은 기온 때문에 연구자의 활동 범위가 제한되어 보다 더 효과적으로 연구 데이터를 회수하는 기술이 요구된다. 본 연구실에서는 데이터 원격 회수 효율성을 증대하기 위한 방법으로 무인기를 이용한 데이터 원격 회수 상황을 가정하고 데이터 전송 시스템을 MQTT 기술을 활용하여 구현하였다.
9	▶ 극지 생물 바이오로거 데이터 원격 회수를 위한 결함 감내 네트워크 [이진영, 염선호, 이정국, 황아리, 임용곤, 박수현 "극지 생물 바이오로거 데이터 원격 회수를 위한 결함 감내 네트워크", 전자공학회논문지, Vol.59, No.1, pp.36-46, 2022] 극지의 환경적인 요인 때문에 무선 통신 네트워크의 신뢰성을 보장하기 어려우며 물적, 인적 자원 및 시간 등이 소모될 수밖에 없다. 본 연구실에서는 극지에서 원격지에 존재하는 데이터를 회수하기 위해 무인항공기(UAV)를 Data mule로 활용하는 결합 감내 네트워크를 제안한다.
10	▶ QGohr의 Speck32/64 신경망 구분자에 대한 분석과 Simon32/64에의 응용 [성효은, 유현도, 염용진, 강주성 "Gohr의 Speck32/64 신경망 구분자에 대한 분석과 Simon32/64에의 응용", 한국정보보호학회 논문지, Vol.32, No.2, pp.391-404, 2022.] Aron Gohr는 경량 블록암호 Speck에 대해 딥러닝 기술에 기반한 암호분석 기법을 제안하였으며, 이는 기존의 차분분석 방식보다 높은 정확도로 선택적 평문 공격을 가능하게 한 방법이다. 본 연구실에서는 이러한 딥러닝 기반 암호분석의 동작 원리에 대해 확률분포를 이용하여 분석하고 이를 경량 블록암호 Simon에 적용한결과를 제시하였다. 또한, 암호분석 알고리즘 내부에서 신경망의 예측값 확률분포가 Speck과 Simon의 각 라운드 함수특성에 따라 차이가 있음을 규명한고, 이를 통해 Aron Gohr가 제시한 암호분석의 핵심기술인 신경망 구분자의 성능 개선방향을 제시한다.

11	▶ Quantum cryptanalysis of the full AES-256-based Davies-Meyer, Hirose and MJH hash functions [Seungjun Baek, Sehee Cho, Jongsung Kim, Quantum Information Processing 21 (2022): 163.] DM, Hirose, MJH 해시모드는 블록암호를 기반으로 하는 해시모드이며, 높은 인지도를 갖고 있다. 본 논문에서는 미래에 도래하게 될 양자컴퓨팅 환경에서의 충돌쌍 공격을 수행하였다. 기존 축소 라운드 AES-256 기반 Davies-Meyer, Hirose, MJH가 공격된 바 있으나, 높은 공격 복잡도 때문에 전체 라운드가 공격이 이루어진 적은 없었다. 본 연구실에서는 자유 변수 기술을 기반으로 한 새로운 선택키 차분 경로를 제시하였고, 이를 통해 최초로 전체 라운드 AES-256 기반 해시 함수들을 공격하는 데 성공하였다. 이 공격들은 양자 컴퓨터에서 구동 가능한 Grover's algorithm을 차분 경로에 적용함으로써 성공할 수 있으며, 본 논문에서는 이에 대한 상세한 복잡도 분석을 제시하였다.
12	▶ A Reused Key Attack on an Encrypted Mobile App Database: Case Study on KakaoTalk and ProtonMail [Uk Hur, Myungseo Park, Jongsung Kim, Journal of Information Security and Applications 67 (2022): 103181.] 스트림 암호와 CTR 및 OFB 모드를 사용하는 블록암호는 동일한 Key와 IV가 재사용된 경우 동일한 키스트림의 XOR로 동작한다. 따라서, Key와 IV가 재사용된 암호문 데이터와 평문 데이터를 동시에 획득할 수 있다면 키스트림을 복구할 수 있다. 이후 복구된 키스트림과 나머지 암호문을 XOR 연산하면 데이터를 복호화할 수 있으며, 이를 키 재사용 공격이라 한다. 본 연구실에서는 실제 키 재사용 공격이 가능한 두 가지 애플리케이션 데이터를 분석하여 키 정보 없이 암호화된 데이터를 복호화하는 방안을 제시하였다.
13	▶ Deep-Learning-Based Side-Channel Analysis of Block Cipher PIPO With Bitslice Implementation [우지은, 한재승, 한동국, "Deep-Learning-Based Side-Channel Analysis of Block Cipher PIPO With Bitslice Implementation", IEEE ACCESS 10 (2022): 69303-69311.] 비트 슬라이스 구현을 사용하는 암호알고리즘 특성상 S-Layer의 출력값은 하나의 레지스터가 아니라 여러 개의 레지스터로 나누어 병렬적으로 저장되어있다. 또한, 딥러닝 기반 부채널 분석은 데이터의 특성에 따라 신경망의 공격 성능이 달라진다. 따라서 본 연구에서는 비트 슬라이스 구현 기반의 데이터에서 효과적인 라벨링 기법을 각각 프로파일링 분석, 비프로파일링 분석으로 나누어서 제안했다. 제안하는 라벨링 방법의 공격 성능을 보기 위해 비트 슬라이스 기반 경량 블록 암호인 PIPO-64/128을 이용하였다. 실험을 통해 프로파일링 분석에서는 ID(identity) 라벨링 기법, 비프로파일링 분석에서는 BE(binary encoding) 라벨링 기법이 제일 효과적임을 보였다. 본 연구의 결과는 PIPO 암호가 탑재된 도구의 부채널 안전성 검증에 큰 역할을 할 수 있을 것으로 기대한다.
14	▶ Experimental evaluation of differential fault attack on lightweight block cipher PIPO [임성혁, 한동국, "Experimental evaluation of differential fault attack on lightweight block cipher PIPO", IET Information Security 1751-8709 (2022)] 비트 슬라이스 구조는 S-Box를 비트별 연산 형태로 변형하여 병렬화하는 구현 방법으로 메모리를 줄이는 등 경량환경에서 이점을 보인다. 본 연구는 비트슬라이스 구현된 블록암호 PIPO를 대상으로 차분 오류 공격 기법을 처음 제안했다. 지정 바이트 위치에 랜덤한 단일 비트 반전 오류를 기반으로 한다. 각 비트에 대한 오류를 획득할 수 있으면 약 64개의 오류 암호문을 통해 98.8%의 확률로 올바른 비밀키를 획득할 수 있다. 본 연구에서는 EM-FI를 기반으로 단일 비트 반전 오류를 유도하고 실제 디바이스에서 충분히 실현 가능한 공격임을 증명하였다. 본 연구의 결과는 IoT의 발전에 따른 경량환경에서의 보안 문제가 대두되고 있는 현재 오류주입 공격에도 안전한 IoT 환경을 구성하는데 활용될 것으로 기대한다.

15	▶ Single-Byte Error-Based Practical Differential Fault Attack on Bit-Sliced Lightweight Block Cipher PIPO [임성혁, 한재승, 한동국, “Single-Byte Error-Based Practical Differential Fault Attack on Bit-Sliced Lightweight Block Cipher PIPO”, IEEE ACCESS 10 (2022): 67802-67813.] 이전에 연구되었던 PIPO 암호 알고리즘에 대한 차분 오류 공격은 단일 비트 반전 오류를 기반으로 하고 있다. 비트 슬라이스 구현은 바이트 단위 오류가 발생하면 암호문 전체에 영향을 준다는 특징을 보인다. 본 연구는 비트 슬라이스 구현된 PIPO를 대상으로 랜덤 위치 단일 바이트 오류 기반의 완화된 공격자 가정을 가지는 차분 오류 공격을 제안하였다. 암호문을 통해 어느 바이트 위치에 어떤 비트가 반전되었는지 확인하기 위한 알고리즘을 제안하였으며 EM-FI를 통해 공격의 실현 가능성을 증명하였다. 약 32개의 오류 암호문으로 이전 연구 결과와 비교하였을 때 우수한 성능을 보인다. 본 연구의 결과는 IoT의 발전에 따른 경량환경에서의 보안 문제가 대두되고 있는 현재 오류주입 공격에도 안전한 IoT 환경을 구성하는데 활용될 것으로 기대한다.
16	▶ Novel Shuffling Countermeasure for Advanced Encryption Standard (AES) against Profiled Attack in Mobile Multimedia Services [이종혁, 김지윤, 한동국, “Novel Shuffling Countermeasure for Advanced Encryption Standard (AES) against Profiled Attack in Mobile Multimedia Services”, Wireless Communications and Mobile Computing 6495546 (2022)] 모바일 멀티미디어 서비스는 무선 통신 및 모바일 기기의 발달로 많은 사용자에게 인기를 얻고 있다. 본 연구는 모바일 서비스 환경에서 발생 가능한 부채널 공격 방어를 위한 대응기법을 제안하였다. 이전 연구에서 제안된 하이딩 기법은 허점이 존재하였으며 노이즈가 존재하는 환경을 선택하지 않았다. 본 연구에서는 기존 대응책의 취약성 원인을 분석하고 이를 완벽하게 해결할 수 있는 새로운 셔플링 기법을 제안하였다. 새로운 대응책은 AES의 바이트 독립/종속 연산에 각각 셔플링 방식과 더미 연산 방식의 무작위 삽입을 균일하게 적용하는 방법이다. 본 연구의 결과는 모바일 멀티미디어 서비스 사용이 증가하고 있는 현재 부채널 공격에도 안전한 모바일 환경을 구성하는데 활용될 것으로 기대한다.
17	▶ Parallel Implementation of CRYSTALS-Dilithium for Effective Signing and Verification in Autonomous Driving Environment [Seog Chung Seo and SangWoo An, ICT Express] 자율주행 환경에서 각 차량은 실시간으로 Basic Security Messages (BSM)을 송/수신하면서 수많은 서명과 검증을 수행해야 한다. 본 논문에서는 양자내성암호 Crystals-Dilithium 전자서명 알고리즘에 대한 연산 최적화 방안을 제안하였음. 효율성을 위해 더미 연산 기반 워프 발산 감소 기법, 병렬 구현 NTT(Number Theoretic Transform) 기반 다항식 곱셈, 거부 시퀀스 테이블을 사용한 거부 샘플링 프로세스 최적화 등과 같은 여러 최적화 방안을 제안함. 본 논문에서 제안한 CRYSTALS-Dilithium 소프트웨어는 기성 자율주행 차량 OBU(On-Board Unit)인 NVIDIA Jetson AGX Xavier의 CPU에서 Dilithium 소프트웨어와 비교하여 최대 19.41배의 성능 향상을 제공함.

18	▶ A Study on Scalar Multiplication Parallel Processing for X25519 Decryption of 5G Core Network SIDF Function for mMTC IoT Environment [Changuk Jang, Juhong Han, Akshita Maradapu Vera Venkata Sai, Yingshu Li, Okyeon Yi, " A Study on Scalar Multiplication Parallel Processing for X25519 Decryption of 5G Core Network SIDF Function for mMTC IoT Environment", Hindawi WCMC, Volume 2022, Article ID 4087816] 5G 통신이 표준화되고 널리 사용되는 통신 매체가 되면, 특정 5G 네트워크 표준 및 요구사항에 따라 구현되어야 한다. 이러한 요구사항 중 하나는 SUCI라는 사용자 비밀 식별자이다. SUCI는 이전 세대 이동통신 네트워크의 취약점이었던 IMSI(International Mobile Subscriber Identity)의 노출을 방지한다. IMSI와 달리 SUCI는 앞서 언급한 취약성을 방지하기 위해 대칭 키 암호화 알고리즘을 사용하여 암호화 및 전송된다. 그러나 첫 번째 단말기가 암호화되려면 홈 네트워크와 키를 교환해야 하며, 이러한 SUCI 암호화를 위한 키 교환은 공개키 암호화 방식인 Elliptic Curve Integrated Encryption Scheme(ECIES) 키 교환 알고리즘을 통해 수행된다. 그러나 ECIES는 대칭 키 암호화 알고리즘에 비해 더 많은 컴퓨팅 리소스를 사용한다. 또한 5G의 mMTC 요건을 충족시키기 위해 5G 가입자 ID deconcealing 기능(SIDF)을 단시간 내에 최소 100만 개의 SUCI를 해독해야 한다. 이것은 IoT를 위한 mMTC 서비스를 제공하기 위해 5G 홈 네트워크에 큰 부담을 준다. 따라서 본 논문에서는 mMTC IoT 환경에서 5G SIDF를 구성하는 방법을 제안한다. 제안된 5G SIDF 구성의 핵심 방법은 GPU를 사용하는 것입니다. 본 제안은 SIDF에서 수행되는 모든 암호화 작업을 GPU를 사용하여 병렬 처리함으로써 mMTC 환경의 부하를 줄이기 위한 것으로, 특히 공개키 암호화 알고리즘의 병렬화에 중점을 두었다. 또한 다양한 5G 보안 제품에 대한 설문조사를 통해 본 논문에서 제안한 방법을 비교하였다.
19	▶ Federated intelligence of anomaly detection agent in IoTMD-enabled Diabetes Management Control System [Philip Virgil Astillo, Daniel Gerbi Duguma, Hoonyong Park, Jiyoon Kim, bonam Kim, IlsunYou, Future Generation Computer Systems, Vol.128, march 2022, p.395-405] 이식형 사물인터넷인 IoTMD는 의료분야에서 환자를 위해 제공되는 서비스가 개인 자신의 상태를 관리할 수 있도록 개선된 기능이다. 이중 당뇨병 관리 제어 시스템(DMCS)은 환자의 안전에 큰 위험을 초래하는 사이버 보안 위협에 직면해 있다. 그러므로 본 연구에서는 당뇨병 관리 제어 시스템에서 추정 모델과 분류 모델을 이용한 딥 러닝(DL) 기반 이상 감지 시스템을 각각 비교하여 정상적인 동작에서 벗어나는 시스템을 탐지할 수 있는 효과적인 솔루션을 제안하였다. 더 나아가 환자의 민감한 정보가 포함된 데이터셋의 프라이버시를 유지하기 위해 독립 학습(IL) 및 연합 학습(FL)을 구현하여 당뇨병 환자의 프라이버시를 유지하면서 당뇨병 관리 제어 시스템의 내부 및 외부로부터 잠재적 위협이 될만한 요인들도 감지할 수 있다.
20	▶ Session Management for Security Systems in 5G Standalone Network [Seongmin Park, Sungmoon Kwon, Youngkwon Park, Dowon Kim, Ilsun You, IEEE ACCESS] 5G 코어 네트워크는 비액세스 스트래텀(NAS), 하이퍼 텍스트 전송 프로토콜(HTTP), 패킷 포워딩 제어 프로토콜(PFCP), GPRS 터널링 프로토콜(GTP) 등 다양한 프로토콜을 사용하며, 각 프로토콜이 사용하는 인터페이스의 패킷은 식별이 어려운 아이덴티티로 관리된다. 이러한 인터페이스의 관계를 실시간으로 분석하는 것은 통합 세션 관리의 중요한 핵심입니다. 본 연구에서는 기존의 NFGW에서는 감당할 수 없지만 5G SA의 보안 시스템에 반드시 유용한 사용자를 위한 효율적인 세션 관리 체계를 소개하며 기존의 NGFW와 5G IPS 시스템 간의 성능을 채택된 계획과 비교하여 이 계획이 5G SA 네트워크에서 실현 가능한지 확인했다.

2. 산업·사회에 대한 기여도

▶ 한동국 교수는 부채널 분석 연구회 회장을 맡아 2018년 10월부터 매년 부채널 분석 워크숍을 주관하여 현재 4회째 개최하였고, 특히 4회에서는 부채널정보분석 워크숍으로 개칭하면서 암호뿐만 아니라 다양한 분야에서 부채널 보안기술의 중요성을 알리고 있음. 또한 학생, 연구소, 그리고 기업 사이에 부채널 보안에 대한 지식 공유의 장을 생성하는데 기여하고 있음.

▶ 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. 다양한 암호 강연을 통해 이를 알리고 또한 금융 IC 카드에 대한 실제 부채널 공격을 소개함으로써 부채널 분석에 취약하지만 실생활에 널리 사용되는 제품에 대한 안전성을 지적하여 향후 예견되는 산업·사회적 피해를 사전에 예방할 수 있을 것으로 기대됨

▶ 이옥연 교수는 군용 드론 보안과 이동통신 보안 연구를 꾸준히 진행하고 있으며, 이를 양자 엔트로피 기반 난수 발생기 등의 양자보안과 융합시키는 연구 또한 진행 중임. 2021년까지 한국암호포럼 의장을 맡아서 국내 암호학의 발전에 노력하였고, 국내 암호산업의 활성화와 관련 정책을 수립하는 데에 기여하였음. 2022년에는 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 기여하고 있음.

▶ 서석충 교수는 저성능 기기 및 고성능 기기 환경에서의 암호알고리즘 최적화 방안 및 고속 설계 연구로 결과를 도출하고 있음. 암호알고리즘 서비스 환경에서 사용하는 각 환경의 특징, 레지스터, 메모리 크기, 성능 부하 등 암호알고리즘이 탑재되는 기기를 여러 관점으로 분석하여 환경별 최적화 방안을 도출함. 그뿐만 아니라 암호알고리즘 구조, 내부 연산, 성능 부하 구간 등을 고려하여 암호알고리즘 자체 최적화 방안을 도출하였음. 이러한 연구 결과를 통해 암호알고리즘의 연산 성능 부하를 최소화, 양질의 보안 서비스를 제공할 수 있을 것으로 기대됨

▶ 양자 컴퓨터의 발전에 따라 기존 인수분해, 이산로그의 수학적 난제를 기반으로 하는 RSA 공개 키 알고리즘 시스템 체계의 안전성에 대한 위협이 발생함. 이로 인해 NIST에서는 양자 컴퓨터 환경에 안전한 양자내성 암호알고리즘 공모전 사업을 진행 중임. 하지만 양자내성 암호알고리즘은 기존의 공개 키 암호알고리즘 시스템보다 느린 성능, 큰 서명길이 및 큰 공개 키 길이 등 고려사항이 존재함. 이에 PQC 알고리즘 최적화 연구는 필수적으로 진행되어야 함

▶ NIST 공모전에 제출된 격자 기반 암호알고리즘은 NTT, FFT, 기각 샘플링와 같은 세부 연산으로 내부 구조를 설계하였음. 서석충 교수는 차세대 양자내성 암호알고리즘의 최적화 구현 방안 연구 결과를 도출하고 있음. 격자 기반 암호알고리즘 세부 연산 최적화 연구를 진행 및 연구 결과에 따라 차세대 양자 내성 암호알고리즘 시스템으로의 변환 과정에서 연구 결과물이 효과적으로 활용될 것으로 기대됨

▶ 김동찬 교수는 양자내성 암호 중 하나인 부호기반 암호에 대한 안전성 분석을 지속적으로 진행하고 있음. 현재 NIST가 진행 중인 양자내성암호 공모전은 현재 최종라운드 심사를 진행하고 있으며, 한국에서도 KpqC를 진행 중임. 해당 공모전은 국내형 양자내성 암호의 표준 제정을 목표로 하고 있으며, 김동찬 교수는 해당 공모전에 부호기반 암호의 공모를 목표로 연구하고 있음. 해당 연구를 통해 양자내성 암호의 흐름을 파악할 수 있으며, 나아가 KCMVP에 적용할 수 있는 암호의 개발이 기대됨

▶ 강주성, 염용진 교수는 난수발생기의 잡음원 분포, 엔트로피 추정법, 안전성 분석, 경량환경에서의 적용 등의 연구를 진행하여 자체 평가기간 동안 특허 등록 1건, 특허 출원 2건, 국내 논문지 1편, 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 난수발생

기 사용에 대한 토대를 마련하여 난수발생기의 취약성으로 발생할 수 있는 산업·사회적 피해를 최소화하는데 이바지할 수 있을 것으로 기대됨

▶ 김종성 교수는 양자컴퓨팅 환경에서의 블록암호 분석 및 설계에 관한 연구를 진행하여 자체 평가기간 동안 국제저널 1편, 국내학술대회 2편의 성과를 내고 지속적으로 진행중임. 현재 IBM을 선두로한 양자컴퓨터의 개발은 전 세계적인 관심을 받고 있음. 고전 컴퓨팅 환경에서의 암호분석 기술들은 대부분이 양자컴퓨팅 환경에서 더 강해지는 경향이 있음. 미래의 양자컴퓨팅 환경을 고려했을 때, 블록암호의 양자 저항성에 관한 연구가 필요하고 양자 저항성을 갖는 블록암호의 설계가 필요함. 그러므로 현재 연구 중인 분야는 앞으로 국내 미래 암호기술 발전에 도움이 될 것으로 기대됨

▶ 김종성 교수는 한국인터넷진흥원과 평가기간을 포함한 다년간의 연구를 진행하여 랜섬웨어 분석에 관한 연구를 지속적으로 진행하고 있음. 자체 평가기간 동안 국내·외에 다수의 피해를 입힌 Hive 랜섬웨어에 대한 복호화 방법을 개발하여 세계적인 관심을 받고 있음. 세부 사항은 arXiv에 등록하여 공개하였으며, 한국 인터넷진흥원 및 과기정통부와 협업하여 복호화도구 제작 및 배포 작업을 통해 랜섬웨어 피해를 완화하는데 도움이 될 것으로 기대됨

▶ 유일선 교수는 5G 보안연구회 위원장으로 2018년부터 매년 5G보안 워크숍을 주관하여 현재 5회째 개최하였음. 특히 2022년 5G 특화망 즉, 이음(e-Um) 5G의 원년을 맞이하여 5G 특화망의 확산과 활성화를 위한 전략과 해결과제가 무엇인지를 논의하였으며 이와 더불어 안전한 5G 특화망 서비스를 위해 정보보안의 중요성을 알림

▶ 유일선 교수는 현재 과학기술정보통신부 5G 보안 협의회 기술분과장으로 분과 회의를 통해 주요 선진국의 5G보안 정책, 5G 핵심 네트워크 보안위협 및 대응기술, 5G 보안 국제 표준화 동향등 측정 주제별로 심층 논의하고 이에 대한 정책방향 및 제도적 개선방안 모색에 기여하고 있음.

3. 연구의 국제화 현황

① 참여교수의 국제적 학술활동 참여 실적 및 현황

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

▶ 한동국 교수는 The 25th Annual International Conference on information Security and Cryptology (ICISC) 국제 학술대회의 Program committee로 활동함

▶ 유일선 교수는 한국정보보호학회 제 23회 정보보호응용 국제 컨퍼런스 (WISA 2022) 프로그램 위원장으로 활동함

▶ 유일선 교수는 제5회 최신 네트워크 보안 국제 워크숍 (ARES ENS 2022) 워크숍 조직 위원장으로 활동함

▶ 유일선 교수는 제9회 ACM 아시아 공개키 암호 워크숍 (APKC 2022)에서 인슐린 펌프를 위한 경량의 비정상 행위탐지를 주제로 초청강연을 함

▶ 유일선 교수는 SCIE 저널 Intelligent Automation & Soft Computing(IF: 3.401, JCR Q2)의 Associate Editor-in Chief로 활동함

▶ 유일선 교수는 SCIE 저널 Information Sciences(IF: 8.233, JCR Q1)의 Associate Editor로 활동함

▶ 유일선 교수는 SCIE 저널 IEEE Access(IF: 3.476, JCR Q2)의 Associate Editor로 활동함

▶ 유일선 교수는 Scopus 저널 Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (Scopus Q2)의 Editor-in Chief로 활동함

▶ 유일선 교수의 국제 저술 활동: Mobile Internet Security (Springer CCIS, Volume 1544) ISBN: 978-981-16-9576-6

▶ 유일선 교수는 IFIP Working Group 8.4 member로 활동함

▶ 유일선 교수는 유럽의 정상급 보안 연구그룹인 오스트리아 Secure Business Austria (SBA)의 Academic Member로 활동함

② 국제 공동연구 실적

1) <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	이옥연	David Kim	United States of America / Georgia State University	2.336의 IF를 갖는 Hindawi WCMC에 “Convolution Neural Network-Based Sensitive Security Parameter Identification and Analysis” 논문을 게재함. 본 논문은 잡음원들이 수집될 때 발생되는 정보들을 통해 그들을 식별할 수 있음을 나타내고, 임의의 암호모듈을 물리적으로 획득하였을 때, 학습된 모델로 암호모듈에서 사용하는 엔트로피 소스를 식별하여 난수를 분석할 수 있다는 공격 시나리오를 세움	https://doi.org/10.1155/2022/9584894
2	한동국	Sadiel de la Fe, Carles Ferrer	Spain / Universitat Autonoma de Barcelona	MDPI Information에 “Profiling Attack against RSA Key Generation Based on a Euclidean Algorithm” 논문을 게재함. 본 논문은 확장 유클리드 알고리즘의 바이너리 버전에 의존하는 RSA 키 생성 과정을 대상으로 한 프로파일링 부채널 분석 방법을 제안함.	10.3390/info12110462
3	이옥연	Yingshu Li	United States of America / Georgia State University	2.146의 IF를 갖는 Hindawi WCMC에 “A Study on Scalar Multiplication Parallel Processing for X25519 Decryption of 5G Core Network SIDF Function for mMTC IoT Environment” 논문을 게재함. 본 논문은 mMTC IoT 환경에서 GPU를 사용하여 5G SIDF를 구성하는 방법을 제안함. 본 제안은 SIDF에서 수행되는 모든 암호화 작업을 GPU를 사용하여 병렬 처리함으로써 mMTC 환경의 부하를 줄이기 위한 것으로, 특히 공개키 암호화 알고리즘의 병렬화에 중점을 두었음. 또한, 다양한 5G 보안 제품에 대한 설문조사를 통해 본 논문에서 제안한 방법을 비교하였음.	https://doi.org/10.1155/2022/4087816

③ 외국 대학 및 연구기관과의 연구자 교류 실적 및 계획

▶ 이옥연 교수팀은 ‘5G와 클라우드 융합환경에서의 안전한 UTM 서비스를 위한 보안기술 연구 및 인력 양성’을 통해 21년 8월부터 22년 4월까지 국제 공동연구를 수행함

- ■ 해외 협력 기관은 미국 조지아 애틀랜타의 중심 업무지구에 있는 조지아 주립대 컴퓨터과학과에 소속되어 있으며, 차세대 네트워크, 무선통신, 알고리즘 디자인, 보안 및 사생활 보호, 인공지능, 빅데이터 등의 다양한 분야에 수많은 업적을 내고 있음
- ■ 파견된 학생들은 세계 각국에서 모인 다양하며 우수한 학생들과 수준 높은 공동연구 활동을 수행했음. 또한, 과제 책임자들과의 주간 미팅을 통해, 많은 연구 경험을 공유했음.
- ■ 국민대학교와 조지아 주립대 간의 교류를 넓힐 기회로 활용될 것으로 보이며, 이것은 더 많은 긍정적인 학술적 효과를 낼 수 있을 것으로 기대됨
- ■ 국민대학교는 조지아 주립대학교의 Yingshu Li 교수팀과의 파견연구를 통해 기존 국민대학교가 보유하지 못한 엣지 클라우드 기술을 접목하여 UTM과 엣지 클라우드의 융합환경에서의 보안 연구를 수행했음
- ■ 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