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

<table>
<tr><td>접수번호</td><td colspan="10">-</td></tr>
<tr><td>신청분야</td><td colspan="5">산업 · 사회 문제 해결분야</td><td>단위</td><td colspan="3">전국</td></tr>
<tr><td rowspan="4">학술연구분야
분류코드</td><td rowspan="2">구분</td><td colspan="2">관련분야</td><td colspan="2">관련분야</td><td colspan="3">관련분야</td></tr>
<tr><td>중분류</td><td>소분류</td><td>중분류</td><td>소분류</td><td>중분류</td><td colspan="2">소분류</td></tr>
<tr><td>분류명</td><td>컴퓨터학</td><td>정보보호</td><td>수학</td><td>응용수학</td><td>전자/정보통신공학</td><td colspan="2">정보통신</td></tr>
<tr><td>비중(%)</td><td colspan="2">50%</td><td colspan="2">30%</td><td colspan="3">20%</td></tr>
<tr><td>교육연구
단명</td><td colspan="10">국문) 안전한 초연결사회를 위한 문제해결형 정보보안 교육연구단</td></tr>
<tr><td></td><td colspan="10">영문) Institute of Information Security Education for Secure Hyperconnected Society</td></tr>
<tr><td rowspan="6">교육연구
단장</td><td colspan="2">소 속</td><td colspan="8">국민대학교 금융정보보안학과</td></tr>
<tr><td colspan="2">직 위</td><td colspan="8">교수</td></tr>
<tr><td rowspan="4">성명</td><td>국문</td><td colspan="2">이옥연</td><td>전화</td><td colspan="5" rowspan="4">[redacted]</td></tr>
<tr><td></td><td></td><td></td><td>팩스</td></tr>
<tr><td rowspan="2">영문</td><td colspan="2" rowspan="2">Yi, Okyeon</td><td>이동전화</td></tr>
<tr><td>E-mail</td></tr>
<tr><td rowspan="2">연차별
총 사업비
(백만원)</td><td colspan="2">구분</td><td>1차년도
('20.9~'21.2)</td><td>2차년도
('21.3~'22.2)</td><td>3차년도
('22.3~'23.2)</td><td>4차년도
('23.3~'24.2)</td><td>5차년도
('24.3~'25.2)</td><td>6차년도
('25.3~'26.2)</td><td>7차년도
('26.3~'27.2)</td><td>8차년도
('27.3~'27.8)</td></tr>
<tr><td colspan="2">국고지원금</td><td>258,720</td><td>562,301</td><td>566,160</td><td>700,783</td><td>517,440</td><td>517,440</td><td>517,440</td><td>258,720</td></tr>
<tr><td colspan="3">총 사업기간</td><td colspan="8">2020.9.1.-2027.8.31.(84개월)</td></tr>
<tr><td colspan="3">자체평가 대상기간</td><td colspan="8">2022.9.1.-2023.8.31.(12개월)</td></tr>
</table>

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

2023년 12월 26일

작성자	교육연구단장	이 옥 연	(인)
확인자	국민대학교 산학협력단장	이 인 형	(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
■ 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 대외협력체계를 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 검증, 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</td></tr>
</table>

	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 ▶ 선정평가 당시 본 연구단에서 제안한 연구 역량 향상을 위한 대학원생 지원을 계획하였음 ■ 자체 평가 기간 내에 국제 저널 15건, 국내 저널 14건, 국제 학회 20건, 국내 학회 51건, 수상 24건을 달성하였음
연구역량 영역 성과	▶ 지속 가능한 발전을 선도하기 위해 본 연구단에서는 학부 및 대학원생에 대한 교육과 함께 다양한 연구를 진행하였음 ■ 자체평가 기간 내에 정부 44건, 산업체 14건 총 58건의 연구를 진행하였음 ■ 총 58건의 연구를 통해 59억에 해당하는 연구비를 수주해냈음 ■ 이 외에도 국제 저널 15건, 국내 저널 14건, 국제 학회 20건, 국내 학회 51건, 수상 24건, 강연 19건, 워크숍 4건, 국내특허(등록 7건, 출원 32건), 국제특허(출원 2건), 소프트웨어 등록 12건, 국내 표준 3건 등 많은 연구 결과를 내었음 ▶ 연구 결과를 기반으로 4건의 기술이전을 시행하였으며 다양한 매체를 통해 산업·사회에 대한 기여하였음
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 ▶ 다양한 융합교육 및 랩별 심화 연구를 통해 다양한 연구성과를 내었음 ▶ 자체평가 대상 기간(2022.09.01.~2023.08.31.)동안 국제 저널 15건, 국내 저널 14건, 국제 학회 20건, 국내 학회 51건, 수상 24건, 강연 19건, 워크숍 4건, 국내특허(등록 7건, 출원 32건), 국제특허(출원 2건), 기술이전 4건, 소프트웨어 등록 12건, 국내 표준 3건의 실적을 달성하였음 ▶ 해당 기간 동안 석사 7명, 박사 1명, 석박사통합 1명을 확보하였으며, 석사 졸업생 15명, 박사 졸업생 4명을 배출하였음
미흡한 부분 / 문제점 제시	▶ 코로나19(COVID-19)로 인해 국제적 교류 및 산학협력에 미진했음
차년도 추진계획	▶ 본 교육연구단의 단계기간(2022~2024)에서의 목표는 정보보안 대외협력체계 강화임 ■ 해당 목표를 위해 산업계의 전문가를 중심으로 한 정보보안 실무과정 운영, 재학생의 인턴 파견 추진을 계획중임 ■ 국내외 정보보안 IT 기업들과의 산학 네트워크를 구축하고 이를 토대로 한 유기적 산학협력 체계정착을 계획 중임 ■ 또한, 정보보안 기술개발과 커뮤니케이션의 활성화를 위한 보안기술 통합 테스트베드를 구축할 예정임 ■ 대외협력체계 강화를 위해 연구소, 산업계의 다양한 전문가와 함께 하는 교육과정 개설과 산업계의 정보보안 문제 해결을 위한 컨소시엄 구축을 계획하고 있음

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)	기준학기	전체교수 수			참여교수 수		
		전임	겸임	계	전임	겸임	계
금융정보보안학과	2022년 2학기	11	2	13	11	-	11
	2023년 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
-					

<표 1-3> 교육연구단 참여교수 지도학생 현황 (단위: 명, %)

신청학과(부)	기준학기	대학원생 수											
		석사			박사			석·박사 통합			계		
		전체	참여	참여비율(%)	전체	참여	참여비율(%)	전체	참여	참여비율(%)	전체	참여	참여비율(%)
금융정보보안학과	2022년 2학기	27	27	100	11	8	73	2	3	150	40	38	95
	2023년 1학기	19	19	100	10	8	80	1	2	200	30	29	96.6
참여교수 대 참여학생 비율		1 : 3.45 (22년 2학기) / 1 : 2.64 (23년 1학기)											

▶ 본 교육연구단 대학원은 총 11명의 교수진 참여중
▶ 본 교육연구단 대학원은 2022년 2학기 석사 27명, 박사 8명, 석·박사 통합 2명 재학 중이었으며, 전체 참여비율 95%를 달성하였음(석·박사 통합과정 수료생 1명 참여함)
▶ 본 교육연구단 대학원은 2023년 1학기 석사 19명, 박사 8명, 석·박사 통합 1명 재학 중이었으며, 전체 참여비율 96.6%를 달성하였음(석·박사 통합과정 수료생 1명 참여함)

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(2022.09.01.~2023.08.31.)동안 신청서에 작성된 37개의 교과 구성 중 4개 교과를 신규 개설하여 운영하였으며, 이는 전체 교과 구성 중 약 70%에 해당함(누적)
  - ✓ 2020.09.01.~2021.08.31.기간은 12개 교과를 운영함(신규 개설)
  - ✓ 2021.09.01.~2022.08.31.기간은 10개 교과를 운영함(신규 개설)
- ■ 교육연구단의 참여교수들은 교과과정 외에도 운영하는 랩을 통해 통신 보안, 디바이스 보안, 암호기술, AI 응용 분야에 관한 심화 연구를 수행중
- ■ 연구를 통해 얻은 연구성과는 국내외 학술대회와 논문지에 발표하였으며, 공모전 참여, 특허출원 등의 추가적인 성과를 내었음
- ■ 자체평가 기간 내에 국제 저널 15건, 국내 저널 14건, 국제 학회 20건, 국내 학회 51건, 특허 등록 7건, 특허 출원 34건, 기술이전 4건의 실적 달성
- ■ 자체평가 기간 내에 정부 44건, 산업체 14건 총 58건의 연구를 진행하였음

▶ 코로나19(COVID-19)로 인해 국제적 교류는 미진하였음

II 교육역량 영역

□ 교육역량 대표 우수성과

▶ 자체평가 대상 기간 내 국제 저널 15건, 국내 저널 14건, 국제 학회 20건, 국내 학회 51건, 수상 24건, 강연 19건, 워크숍 4건, 국내특허(등록 7건, 출원 32건), 국제특허(출원 2건), 기술이전 4건, 소프트웨어 등록 12건, 국내 표준 3건 등의 성과를 냄

▶ 국제 저널

- “A method for decrypting data infected with Hive ransomware”, Giyoon Kim, Soram Kim, Soojin Kang, Jongsung Kim, Journal of Information Security and Applications (SCIE, I.F=5.6)
- “Quantum rebound attacks on reduced-round ARIA-based hash functions.”, Seungjun Baek, and Jongsung Kim, ETRI Journal (SCIE, I.F=1.4)
- “A study on cloud data access through browser credential migration in Windows environment”, Uk Hur, Soojin Kang, Giyoon Kim, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, I.F=2.0)
- “DIM-Based Random Number Generation Using Quantum Noise Resources”, Hansaem Wi, Seyoon Lee, and Okyeon Yi, Hindawi WCMC (SCIE, I.F=2.146)
- “Analysis of Distinguishable Security between the One-Time Password Extraction Function Family and Random Function Family”, Hyunki Kim and Okyeon Yi, MDPI Applied Science, (SCIE, I.F=2.838)
- “Rider Optimization with Deep Learning Based Image Encryption for Secure Drone Communication”, JN. Kannaiya Raja1, E. Laxmi Lydia, T Archana Acharya, K. Radhika, Eunmok Yang and Okyeon Yi, IEEE ACCESS. (SCIE, I.F=3.367)
- “Energy Optimization Techniques in Underwater Internet of Things: Issues, State-of-the-Art, and Future Directions” Delphin Raj Kesari Mary, Eunbi Ko, Dong Jin Yoon, Soo-Young Shin and Soo-Hyun Park, water 2022 (MDPI, I.F=3.4)
- “Practical Entropy Accumulation for Random Number Generators with Image Sensor-Based Quantum Noise Sources”, Youngrak Choi, Yongjin Yeom, and Ju-Sung Kang, MDPI Entropy. (SCIE, I.F=2.738)
- “End-to-End Post-Quantum Cryptography Encryption Protocol for Video Conferencing System Based on Government Public Key Infrastructure”, Yeongjae Park, Hyeondo Yoo, Jieun Ryu, Young-Rak Choi, Ju-Sung Kang, Yongjin Yeom, MDPI Applied System Innovation. (I.F=2.725)
- “APSec1.0: Innovative Security Protocol Design with Formal Security Analysis for the Artificial Pancreas System“, Jiyoon Kim, Jongmin Oh, Daehyeon Son, Hoseok Kwon, Philip Virgil Astillo and Ilsun You, Sensors (SCIE, I.F=6.3)
- “Chosen-Ciphertext Clustering Attack on CRYSTALS-KYBER Using the Side-Channel Leakage of Barrett Reduction”, Bo-Yeon Sim, Aesun Park, and Dong-Guk Han, IEEE Internet of Things Journal. (SCIE, I.F=10.238)
- “Deep-Learning Based Nonprofiling Side-Channel Attack on Mask Leakage-Free Environments Using Broadcast Operation”, Seonghyuck Lim, Hye-Won Mun, and Dong-Guk Han, IEEE ACCESS. (SCIE, I.F=3.476)
- “Optimized Implementation of PIPO Block Cipher on 32-bit ARM and RISC-V Processors “ by

YoungBeom Kim and Seog Chung Seo, IEEE ACCESS (SCIE, IF=3.476)

- "Signature Split Way for PQC-DSA Compliant with V2V Communication Standards" by YoungBeom Kim and Seog Chung Seo, MDPI Applied Sciences (SCIE, IF=2.838)
- "AVX512Crypto: Parallel Implementations of Korean Block Ciphers Using AVX-512" by YongRhyel Choi, Hojin Choi, and Seog Chung Seo, IEEE ACCESS (SCIE, IF=3.476)

▶ 국내 저널

- "Skinny-128-384 와 Romulus-N 의 SITM 공격." , 박종현, 김종성, 정보보호학회논문지, 32권 5호
- "iOS 환경에서의 협업 툴 아티팩트 분석 및 크리덴셜 활용 방안 연구" , 박귀은, 이민정, 강수진, 김소람, 김종성, 디지털포렌식연구 17권 2호
- "볼륨 암호화 및 백업 응용프로그램에 대한 복호화 방안 연구" , 박귀은, 이민정, 강수진, 김기윤, 김종성, 정보보호학회논문지, 33권 3호
- "Dm-crypt류 기반 암호화 사용 흔적 조사 및 주요 데이터 수집 절차" , 이민정, 박귀은, 강수진, 김기윤, 허욱, 김소람, 박수영, 이인수, 김종성, Contemporary Review of Forensic science 7호
- "모바일 인스턴트 메신저에 대한 TMTO 및 GAN 모델을 활용한 안전성 분석" , 백승준, 전용진, 허욱, 김종성, 정보보호학회지 32권 6호
- "무선랜 환경에서 양자 엔트로피 칩 기반 암호모듈을 적용한 드론 피아식별과 안전한 정보 제공 기술 제안" , 정서우, 윤승환, 이옥연, 정보보호학회논문지, 2022년 10월호
- "수중 노이즈 상황에서의 기하학 기반 적외선 통신 채널 모델" 발카시나 스베틀라나, 황아리, 이진영, 염선호, 박수현, 전자공학회논문지 2022년 11월호
- "NTRU를 결합한 하이브리드 세션 보호 프로토콜을 이용한 금융 오픈 API 환경의 거래 세션 안전성 강화" , 권수진, 김덕상, 박영재, 류지은, 강주성, 염용진, 정보보호학회논문지 2023년 2월호
- "블랙박스 암호모듈에 적용 가능한 CRYSTALS-Kyber의 은닉채널 공격과 IP카메라의 잠재적 보안 위협" , 최영락, 강주성, 염용진, 한국통신학회논문지 2023년 6월호
- "5G 특화망의 성공적 정착을 위한 보안 고려사항 연구", 김건우, 손대현, 박훈용, 박성민, 김영수, 김환국, 김보남, 유일선, 정보기술융합공학논문지, 13권 1호, 2023
- "레이저 오류 주입 공격 성공률 향상을 위한 전자파 및 열 정보 활용 시스템" , 문혜원, 지재덕, 한동국, 정보보호학회논문지, 32권, 5호
- "이종 디바이스 환경에 효과적인 신규 딥러닝 기반 프로파일링 부채널 분석" , 우지은, 한동국, 정보보호학회논문지, 32권, 5호
- "NIST PQC 공모전 동향 분석 및 표준화 대상 & Round 4 알고리즘 소개" , 김동천, 김영범, 서석충, 한국정보보호학회 학회지 2023년 4월호
- "수중 센서 데이터의 SNS 포스팅 서비스 설계 및 구현", 이정국, 염선호, 이진영, 박수현, 박철웅, 신수영, 한국통신학회논문지, 2023년 8월호

▶ 국제 학회

- "A study on cloud data access through browser credential migration in Windows environment" , Uk Hur, Soojin Kang, Giyoon Kim, Jongsung Kim, DFRWS USA 2023 Conference
- "Study on MC-Optimal S-Box Circuits" , Yongjin Jeon, Seungjun Baek, Jongsung Kim, International Conference on Platform Technology and Service (PlatCon) 2023
- "Pros and Cons of Switching between LTE and Wi-Fi in Maritime" Shrutika Sinha, G. Pradeep Reddy, Soo-Hyun Park, International Conference on Green and Human Information Tech 2023 (ICGHIT 2023)
- "A Survey of Deep/Machine Learning in Maritime Communications" Shrutika Sinha, Soo Yeon Kwon,

Soo Hyun Park, 2023 International Conference on Ubiquitous and Future Networks (2023 ICUFN)

- “End-to-End PQC Encryption Protocol for GPKI Based Video Conferencing Systems”, Yeongjae Park, Hyeondo Yoo, Jieun Ryu, Young-Rak Choi, Ju-Sung Kang, Yongjin Yeom, 2023 IEEE 3rd International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB 2023)
- “Formal Security Analysis for TLS 1.3 using AVISPA tool“, Jongmin Oh, Daehyeon Son, Jiyoon Kim and Ilsun You, The 6th International Symposium on Mobile Internet Security (MobiSec 2022)
- “Blockchain Applied 5G Authentication and Key Agreement Evaluation“, Hoseok Kwon, Gunwoo Kim, Ajung Im, Bonam Kim and Ilsun You, The 6th International Symposium on Mobile Internet Security (MobiSec 2022)
- “A study on machine learning-based false base station detection method in 5G“, Hoonyong Park, Daehyeon Son, Gunwoo Kim and Ilsun You, The 6th International Symposium on Mobile Internet Security (MobiSec 2022)
- “Differential Fault Attack on AES using Maximum Four Bytes Faulty Ciphertexts”, Jae-Won Huh and Dong-Guk Han, The 25th Annual International Conference on Information Security and Cryptology (ICISC 2022)
- “Simulation of Vehicle-to-Vehicle Communication based on selected PQC-DSA“, YoungBeom Kim, Seog Chung Seo, The 6th International Symposium on Mobile Internet Security (MobiSec 2022)
- “AVX512Crypto : Parallel Implementation methods of Korean Block Cipher using AVX-512“, YongRyel Choi, Hojin Choi, Seog Chung Seo, The 6th International Symposium on Mobile Internet Security (MobiSec 2022)
- “High-Performance Kyber implementation on ARMv7-based ARM Neon Technology“, YoungBeom Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Accelerating Key Derivation Function on GPU Architectures“, DongCheon Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Accelerating Key Derivation Function on GPU Architectures“, DongCheon Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Efficient Implementation of Kyber on MSP430 Environment“, DongHyun Shin, YoungBeom Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Implementation of Montgomery Reduction and Butterflies for CRYSTALS-Dilithium on RISC-V“, YongRyeol Choi, YoungBeom Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “V2V-MHT Accelerated V2V Authentication Framework using Merkle Hash Tree“, YoonSun Han, YoungBeom Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Optimization Study of Parallel Implementation“, SeongJun Choi, DongCheon Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Tabling GHash in LEA-GCM and optimizing“, JaeSeok Lee, DongCheon Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Efficient implementation of multiplication reduction over NIST prime P-384 for 8-bit AVR Processor“, MinGi Kim, YoungBeom Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)

▶ 국내 학회

- “NIST LWC 최종 후보 Ascon-XOF에 대한 안전성 분석”, 조세희, 백승준, 김종성, 2022 정보보호학회 동계 학술대회
- “협업 툴 TeamUp과 Agit 데이터베이스 복호화 방안 및 아티팩트 분석 연구”, 박세준, 이용진, 박지수, 박귀은, 김종성, 2022 정보보호학회 동계 학술대회
- “드론 보안 시스템의 PQC 마이그레이션에 대한 연구”, 윤혜진, 김태완, 장찬국, 이옥연, 2022 한국정보보호학회 동계학술대회
- “5G 상용망 연동을 위한 탈부착형 하드웨어 암호모듈 설계”, 김형엽, 정서우, 위한샘 이옥연, 2022 한국정보보호학회 동계학술대회
- “양자 키 분배 기술과 활용 동향”, 나태경, 이세윤, 김현기, 이옥연, 2022 한국정보보호호학회 동계학술대회
- “AHS 프로토콜을 적용한 드론 인증 시스템”, 윤혜진, 장찬국, 이재훈, 이옥연, JCCI 2023 (제 33회 통신정보 합동학술대회)
- “이동통신망과-국방광대역통합망 연동을 위한 qSIM 기반 인증의 필요성 연구”, 김형엽, 최지훈, 위한샘, 이옥연, 2023 한국정보보호호학회 하계학술대회
- “HMAC-SHA1 알고리즘을 사용하는 OTP 단말기의 평문과 키 추정 연구”, 나태경, 윤승환, 이옥연, 2023 한국정보보호호학회 하계학술대회
- “양자암호통신장비를 활용한 광대역 네트워크 운영환경에 대한 암호학적 안전성 분석 및 활용방안”, 윤혜진, 장찬국, 이재훈, 이옥연, 최지훈, 2023 한국정보보호학회 하계학술대회
- “극한지 빅데이터를 위한 남극 IoT 네트워크 엔티티”, 염선호, 윤동진, 황아리, 임용곤, 박수현, 2022 한국통신학회 추계종합학술대회
- “Key factors for Maritime Communications: Challenges and Trends”, Shrutika Sinha , ARi Hwang, Sun-Ho Yum, Jinyoung Lee, Soo-Hyun Park, The 33rd Joint Conference on Communications and Information (JCCI 2023)
- “Federated Learning-Internet of Underwater Things”, Shrutika Sinha, Soo-Hyun Park, Annual Conference of KIPS 2023 (ACK 2023)
- “이미지센서 기반 진난수생성기에 적용 가능한 효율적인 엔트로피 축적 방법”, 유현도, 최영락, 강주성, 염용진, 2022 한국통신학회 추계학술대회
- “Jetson nano 환경에서의 경량 암호학적 난수발생기 병렬 구현”, 박영재, 유현도, 강주성, 염용진, 2023 한국통신학회 동계학술대회
- “병렬 잡음원 기반 난수발생기에 적합한 엔트로피 건전성 시험”, 류지은, 유현도, 강주성, 염용진, 2023 한국통신학회 동계학술대회
- “자동화된 정형화 검증 도구를 사용한 완전 순방향 비밀성을 지원하는 TLS 1.2 프로토콜에 관한 PAL 3급의 보안성 검증 분석“, 오종민, 김지윤, 김보남, 유일선, 2023 한국정보보호학회 하계학술대회 (CISC-S’23)
- “블록체인과 머클해시트리를 이용한 데이터 무결성검증에 관한 연구 스마트 HACCP의 CCP 데이터를 중심으로“, 임아정, 김보남, 유일선, 2023 한국정보보호학회 하계학술대회 (CISC-S’23)
- “이음 5G에서 연합 학습 시스템 연구“, 박훈용, 손대현, 김건우, 유일선, 2023 한국정보보호학회 하계학술대회 (CISC-S’23)
- “5G 초기 인증단계에서 Linkability 공격에 대응 가능한 5G-AKA’ 프로토콜 취약점 분석“, 손대현, 오종민, 박영신, 유일선, 2023 한국 스마트미디어학회 종합학술대회에서 (KISM-S’23)
- “설명 가능한 XGBOOST 기반의 허위 기지국 탐지 기법“, 손대현, 박훈용, 유일선, 2023 한국정보보호학회

하계학술대회 (CISC-S'23)

- "5G 초기인증의 순방향 비밀성 지원을 위한 5G-IPAKA 보안 프로토콜 취약점 분석", 김건우, 박훈용, 권호석, 김보남, 유일선, 2023 한국 스마트미디어학회 종합학술대회에서 (KISM-S'23)
- "경량 블록 암호 PIPO에 대한 도메인 지향 마스킹 기법", 김연재, 한동국, 2022 한국정보보호학회 동계학술대회
- "CRYSTALS-KYBER 다항식 곱셈의 하드웨어 병렬 구현에 대한 상관 전력 분석", 김수진, 한동국, 2022 한국정보보호학회 동계학술대회
- "SEED 마스킹의 일차 부채널 분석 취약점과 대응기법", 김주환, 한재승, 한동국, 2022 한국정보보호학회 동계학술대회
- "하드웨어 구현 CRYSTALS-KYBER 암호문 비교 연산에 대한 부채널 분석", 김수진, 한동국, 2022 한국정보보호학회 동계학술대회
- "DDR4 DRAM의 소프트웨어 기반 Rowhammer 기법과 전자파 오류주입 기반 Ehammer 기법에 관한 연구", 허재원, 박형동, 여인국, 김다연, 권건우, 한동국, 2023 한국정보보호학회 하계학술대회
- "반복 학습을 통한 딥러닝 기반 비프로파일링 부채널 분석 성능을 향상 방안", 김주환, 한동국, 2023 한국정보보호학회 하계학술대회
- "비교 연산 기반 상수시간 CDT 샘플링에 대한 단일 파형 분석", 최건희, 허재원, 한재승, 한동국, 2023 한국정보보호학회 하계학술대회
- "노트북의 가상메모리 할당/해제를 통한 은닉 채널 형성", 안현준, 한동국, 2023 한국정보보호학회 하계학술대회
- "Google 사 Project Vault AES-128 하드웨어 모듈에 대한 상관 전력 분석", 기윤서, 한재승, 한동국, 2023 한국정보보호학회 하계학술대회
- "스마트폰 디스플레이 변화에 따른 은닉 채널 형성 방안", 노혜빈, 김진웅, 한재승, 한동국, 2023 한국정보보호학회 하계학술대회
- "부채널 분석을 통한 USIM 복제 최신 동향 연구", 최아록, 한재승, 한동국, 2023 한국정보보호학회 하계학술대회
- "KpqC 전자서명 후보 AIMer에 대한 부채널 및 오류주입 공격", 한재승, 허재원, 이상엽, 권지훈, 한동국, 2023 한국정보보호학회 하계학술대회
- "GPU 환경에서의 해시 기반 전자 서명 SPHINCS+ FORS 최적화 방안", 최호진, 서석충, 2022 한국정보보호학회 동계학술대회
- "MS office2013+ 다중 파일 크래킹 방안", 최호진, 서석충, 2022 한국정보보호학회 동계학술대회
- "GPU 환경에서의 국산 해시 함수 LSH 벤치마킹", 최성준, 최호진, 서석충, 2022 한국정보보호학회 동계학술대회
- "GPU 아키텍처 상에서의 격자 기반 양자 내성 암호 최적화 동향", 김동천, 최호진, 서석충, 2022 한국정보보호학회 동계학술대회
- "IoT 환경에서의 격자 기반 양자 내성 암호 최적 구현 동향", 최용렬, 김영범, 서석충, 2022 한국정보보호학회 동계학술대회
- "AVR 환경에서 표준화 대상 양자내성암호 Crystals Kyber 최적화 구현 연구", 김영범, 서석충, 2022 한국정보보호학회 동계학술대회
- "8-bit AVR 환경에서의 PIPO, CHAM 최적화 구현", 신동현, 김영범, 서석충, 2022 한국정보보호학회 동계학술대회
- "ARMv7 기반 Cortex-A에서의 Kyber 구현 최적화 연구", 김영범, 서석충, 2023 한국정보보호학회 하계학술대회
- "GPU환경에서의 PBKDF2-HMAC-SHA2 최적화", 김동천, 서석충, 2023 한국정보보호학회 하계학술대회

■ “16-bit MSP430환경에서 kyber 고속화 구현“, 신동현, 김영범, 서석충, 2023 한국정보보호학회 하계학술대회
■ “RISC-V 환경에서 CRYSTALS-Dilithium의 Montgomery Reduction 및 Butterfly 연산 최적 구현“, 최용렬, 김영범, 서석충, 2023 한국정보보호학회 하계학술대회
■ “V2V-MHT: Merkle Hash Tree를 활용한 IEEE 802.11p WAVE 프로토콜 V2V 서명 검증 가속화“, 한윤선, 김영범, 서석충, 2023 한국정보보호학회 하계학술대회
■ “GPU 환경에서의 Scrypt 알고리즘 병렬 구현 최적화 연구“, 최성준, 김동천, 서석충, 2023 한국정보보호학회 하계학술대회
■ “LEA-GCM GPU상 동일 키에 따른 tabling, constant memory 사용 및 최적화“, 이재석, 김동천, 서석충, 2023 한국정보보호학회 하계학술대회
■ “8-bit AVR 환경에서 P-384 곱셈 Reduction 연산 최적화“, 김민기, 김영범, 서석충, 2023 한국정보보호학회 하계학술대회
■ 부호 기반 키체결 PALOMA의 섞음 연산 SHUFFLE에 관한 연구, 김민지, 박동현, 김동찬, 한국정보보호학회 하계학술대회, 2023 (6월)
■ Barrett Reduction과 Montgomery Reduction을 기반으로 한 RSA 비밀키 연산 고속화에 관한 연구, 김민지, 김동찬, 동계 통신학회 종합학술발표회, 2023 (2월)
■ “지능형 연안어선 운항안전 모듈 상위 설계”, 염선호, 임용곤, 이정국, 박수현, 2022 대한조선학회 추계학술대회

▶ 수상
■ 2022 국가암호 공모전 장려상 1건
■ 2022 한국정보보호학회 동계학술대회 정보보호학회장상 2건
■ 2022 한국정보호호학회 동계학술대회 우수논문상 1건
■ 2022 부채널분석연구회 한국정보보호학회장상 1건
■ 2022 MobiSec ETRI Best Student Paper 1건
■ 2022 국가 암호기술 전문인력 양성과정 최우수상 1건, 우수상 2건
■ 2022 부채널분석경진대회 부채널분석연구회 회장상 1건
■ 2022 부채널분석경진대회 한국전자통신연구원 원장상 1건
■ 2022 Mobisec ETRI Best Poster Award 1건
■ 2023 한국정보보호학회 하계학술대회 정보보호학회장상 2건
■ 2023 한국정보보호학회 하계학술대회 차세대 우수 여성과학자상 1건
■ 2023 한국정보보호학회 하계학술대회 정보보호학회장상 1건
■ 2023 한국정보호호학회 하계학술대회 우수논문상 1건
■ 2023 부채널분석경진대회 부채널분석연구회 회장상 1건
■ 2023 부채널분석경진대회 국가보안기술연구소 소장상 1건
■ 2023 한국정보보호학회 충청지부 학술대회 국가보안기술연구소장상 1건, 정보보호학회장상 1건 수상
■ 2023 부채널분석연구회 부채널분석연구회장상 1건
■ 2023 ICEIB 2023 Best conference paper award 1건
■ 2023 제6회 부채널정보분석 워크숍 차세대 정보보호 여성 과학기술인상 1건

▶ 참여교수 교육대표실적
■ 보안 강연
✓ 국정원 신입직원 대상 부채널분석 특강(2022.09.02.), 국가정보원
✓ 양자시대와 정보보안, QIS(Quantum Information Science) (2022.09.02.) 전파통신법포럼

✓ 보안 패러다임의 변화와 미래보안의 Keyword 제언 (2022.09.22.) 안랩 ISF 세미나
✓ 랜섬웨어 대응 및 복호화 기술(2022.10.01.), 국가보안기술연구소
✓ Crystals-Kyber와 Dilithium 최신 구현 동향, 국가수리과학연구소, 2022.10.19., 2022.11.09.
✓ 스마트 공장 등 디지털 전환과정에서 겪는 보안 위협사례 및 보안 강화 전략 (2022.11.28.) KoiTa 한국산업기술진흥협회
✓ 암호모듈 난수발생기 구현 및 엔트로피 테스트, 건국대학교 SW 중심대학사업단, 2022.12.02.
✓ KISA 암호팀 대상 부채널분석 교육 특강(2022.12.19.-20), 한국인터넷진흥원
✓ 랜섬웨어 대응 및 복호화 기술(2023.03.09.), 국가정보원
✓ 순천향대학교 정보보안학과 초청강연(2023.03.24.), 순천향대학교
✓ 경량암호(2023.04.11.), 삼성전자
✓ 숭실대학교 AI보안연구센처 초청강연(2023.04.25.), 숭실대학교
✓ 암호모듈 검증기준과 시험방법, 건국대학교 SW 중심대학사업단, 2023.05.15.
✓ 성신여자대학교 융합보안학과 초청강연(2023.05.24.), 성신여자대학교
✓ NIST 격자기반암호 소개, 한국전자통신연구원, 2023.07.03.
✓ 랜섬웨어 공격, 대응 및 복호화 기술(2023.07.12.), 국가정보원
✓ 제 12호 정보보호의날 초청강연(2023.07.12.), 한국인터넷진흥원
✓ 암호모듈 전문교육 기초과정 (암호모듈 검증 파트), 한국인터넷진흥원, 2023.07.20.~21
✓ 랜섬웨어 대응 및 복호화 기술(2023.08.04.) 국가보안기술연구소

■ 워크숍
✓ 제 5회 부채널정보분석 워크숍 (2022.10.27.~2022.10.28.)
• 부채널정보분석 워크숍을 주관하여 개최함
✓ 제 6회 MobiSec 2022 워크숍 (2022.12.15.~2022.12.17.)
• MobiSec 2022 워크숍을 주관하여 개최함
✓ 제 6회 5G보안 워크숍 (2023.4.6.~2023.4.7.)
• 5G보안 워크숍을 주관하여 개최함
✓ 제 1회 랜섬웨어대응연구회 워크숍 (2023.5.4.)
• 랜섬웨어 대응 워크숍을 주관하여 개최함

▶ 국내특허
[등록]
■ 양자보안 통신장치 통합형 원방감시 제어 시스템 및 방법 (등록)
■ 5G SIDF 암호처리장치 및 그 방법 (등록)
■ 인공신경망을 이용한 RSA 암호에 대한 부채널 분석 방법 및 장치 (등록)
■ 무선통신 기기 및 이의 동작방법 (등록)
■ 수중 사물 인터넷의 온톨로지 기반 통신 매체 선택 방법 및 이를 수행하는 수중 통신 장치(등록)
■ 수중 네트워크 관리 시스템 및 그의 동작 방법(등록)
■ 부채널 공격에 안전한 행렬 곱 연산을 수행하기 위한 장치 및 방법(등록)
[출원]
■ 스마트기기용 양자보안 통신 제공장치 및 방법
■ 양자암호 기반의 수하물 식별 장치 및 방법
■ 양자암호 기반의 영상 식별 장치 및 방법
■ 무인 비행체 및 이의 비행 경로 설정 방법

■ 무인 비행체 및 이의 센서 장치 구동 제어 방법, 및 통신 시스템
■ 무인 비행체를 통한 센서 상태 확인 방법
■ 지상 네트워크 및 수중 네트워크 간 주소 상호 운용성을 위한 게이트웨이 장치 및 그 동작 방법
■ 고 지연의 Tum-IoT 네트워크에서 다중 통신 스펙트럼 기반 서비스 요청 추론 기법
■ 수중 네트워크에서의 트랜잭션 동작
■ 수중 무선 통신 시스템을 이용한 수중 무선 네트워크 구성 방법
■ 다중-모드 수중통신 장치
■ 수중 네트워크 관리 시스템 및 그의 동작 방법
■ 이미지 센서 기반 엔트로피 축적 장치 및 방법, 이를 이용한 진난수생성기
■ 모드버스 오류 처리 장치 및 방법
■ 군집화 알고리즘을 이용한 블록암호 CTR 운영모드 부채널 분석 방법 및 장치
■ 비지도 도메인 적응을 이용한 프로파일링 부채널 분석 방법 및 장치
■ 블록암호에 대한 4바이트 이하 오류 기반의 차분 오류 분석 방법 및 장치
■ 경량 블록 암호 PIPO에 대한 Domain-Oriented Masking 적용 방법
■ 스마트폰 소리 재생 시 누설되는 전자기파를 이용한 은닉 채널
■ 가상메모리 할당 및 해제를 이용한 은닉채널 형성 방법 및 장치
■ 경량 블록 암호 PIPO에 대한 Threshold Implementation 적용 방법
■ 크리스탈 카이버 연산 장치에 대한 상관 전력 분석 방법 및 장치
■ 경량 블록 암호 PIPO에 대한 Re-Consolidating Masking 적용 방법
■ 인공 신경망의 오분류 유도 방법 및 파라미터 복원 방법과 이를 위한 장치
■ 부채널 공격을 방지하기 위한 암호문 비교 장치 및 방법
■ 다항식 연산 기반의 보안 알고리즘의 연산 처리 방법, 그리고 이를 구현하기 위한 장치
■ 부채널 공격을 방지하기 위한 암호문 비교 장치 및 방법
■ 이미지 센서 기반 엔트로피 축적 장치 및 방법, 이를 이용한 진난수생성기
■ 모드버스 오류 처리 장치 및 방법
■ 마르코프 패스워드 테이블을 이용한 다중 파일 패스워드 크래킹 장치 및 방법
■ 인퓨전 펌프를 위한 머드 기반의 네트워크 관리 방법 및 장치
■ BMANF를 활용한 그룹 키 기반 프로토콜 수행 방법 및 BMANF 노드

▶ 국제특허
■ DPAPI 기반의 데이터 재생성을 통한 클라우드 데이터 획득 장치 및 방법 (출원)
■ 양자 엔트로피 기반 일회용 양자 비밀번호 생성 장치 및 방법 (출원)

▶ 기술이전
■ 양자키 유도 함수를 활용한 암호키 생성 방법 및 이를 수행하는 암호키 생성 장치
■ 화이트박스 암호화 기술
■ 양자내성암호 알고리즘 Kyber의 고속구현 기술 이전
■ 심리스 DTN 프로토콜을 사용한 수중통신 장치 및 그 통신방법

▶ 소프트웨어 등록
■ 경량 데이터베이스(SQLite)에 대한 비밀번호 검증 및 복호화 프로그램 등록
■ 드론 제어 데이터 관리를 위한 Replaying(재생) FDR(비행데이터기록) 장치용 프로그램 등록
■ 공간정보 기반 식별용 에이전트 모듈(리눅스) 등록

■ 암호모듈 기반 식별 체계용 시험 프로그램(윈도우) 등록
■ Curve25519를 이용한 Kyber의 SETUP 프로그램 등록
■ NTRU(엔트루)가 적용된 모드버스 TLS(티엘에스) 통신 프로그램 등록
■ 측정 보고서(Measurement Report) 학습 데이터 전처리기 프로그램
■ 허위기지국 비정상 데이터 생성기
■ 경량 블록암호 피포(PIPO)의 안전한 하드웨어 마스킹 코드
■ 신경망 활성 함수 소프트맥스(Softmax) 입력 대상 오분류를 유도하기 위한 비트 반전 시뮬레이션 알고리즘
■ CUDA C 기반 고정 길이 파라미터에 대한 PBKDF2-HMAC-SHA Family 고속 생성 방안
■ 수중 SNS(소셜 네트워크 서비스)를 위한 S-DTN(심리스 전공지연 감내 네트워크) 기반 이종망 데이터 전송 중계 프로그램

▶ 국제 표준(해당없음)

▶ 국내 표준
■ TTA 정보통신표준화위원회 신규 표준화 과제 “양자키분배 후처리에 대한 시험방법” 채택
■ 사물인터넷융합포럼 표준화 제안, “보안 강화된 블록암호에 대한 결합 상관 부채널 분석 기술 요구사항 및 절차”, IoTFS-0250.
■ 사물인터넷융합포럼 표준화 제안, “전압 전자파 이종 오류원 기반 오류 주입 분석 기술 요구사항 및 절차”, IoTFS-0251.

1. 교육과정 구성 및 운영

1.1 교육과정 구성 및 운영 현황과 계획

▶ 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
■ 확률론 및 응용, 증명가능 안전성론(대학원), 보안 S/W 구현, 고급응용수학, 병렬암호구현(대학원), 수리통계학, 대칭키 암호, 정보보호프로토콜(대학원), 복소함수론 및 응용, 암호분석 과목을 주요 과목으로 선정하고 연차별로 과목 개설을 하고 있음

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)	2022년 2학기	2	0	0	2
	2023년 1학기	5	1	1	7
	계	7	1	1	9
배출 (졸업생)	2022년 2학기	15	4		0
	2023년 1학기	0	0		0
	계	15	4		0

2.2 교육연구단의 우수 대학원생 확보 및 지원 계획

▶ 우수 대학원생 확보 노력

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

▶ 우수 대학원생 지원 계획

- 국민대학교 일반대학원은 우수한 신입생을 적극 유치하고자 '성곡장학금' (수업료 전액), '교수 추천 우수 신입생 장학금' (수업료의 50 % 지원), '교육 조교 장학금' (수업료의 50 %), '연구 조교 장학금' (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 미래가 요구하는 과학 인재로 성장할 기회를 제공함

▶ 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

- ■ 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 석사과정 또는 석·박사 통합과정 입학자, 재학 중 저명한 국제학술지(SCI, SSCI, SCIE, A&HCI, SCOPUS)에 논문을 100% 게재한 자, 학·석사 연계과정으로 선발된 자에 대해 1학기 수업 연한을 단축할 수 있도록 하고 있음
- ■ SCI 논문 출판 외에도 유명 국제 학회에 제출된 논문 또한 우수한 학술활동의 결과물로 판단할 수 있으며 해당 결과에 대한 인센티브를 부여함으로써 연구활동 결과물의 질적 향상을 야기할 것으로 기대함
- ■ 상기 해당하는 저널 혹은 학술대회에 논문이 선정되지 않은 대학원생들에 대해서도 출판 혹은 발표한 논문의 수가 기준을 초과한 대학원생들에 대해 성실함을 인센티브를 지급하여 꾸준한 학술활동을 진행할 동기를 부여하고 있음
- ■ 오프라인으로 진행되는 교류 행사에 필요한 항공 운임비 및 체류비를 지원하여 원활한 연구가 진행될 수 있도록 지원하고 있음
- ■ 정보보안 기술을 활용한 다양한 사례를 기반으로 한 국제 학술대회에서 관련 결과물에 대한 발표 및 참석에 대해 지원하고 있음
- ■ 참여대학원생들이 연구 분야의 국제학술대회 및 포럼 등과 같은 저명한 학술교류 네트워크에 참석하도록 함으로써, 연구 결과 교류 및 폭 넓은 논의를 통해 초연결사회에서 요구되는 문제를 발굴 및 해결 할 수 있는 실전 감각을 익힐 수 있도록 적극 지원하고 있음
- ■ 과제 교육비를 통해 미래 암호 워크숍, 위험관리 워크숍, 랜섬웨어대응연구회 워크숍, 5G 보안 워크숍, CPS 보안 워크숍, 공급망 보안 워크숍, 국제 표준화 워크숍, 양자보안 워크숍, IoT 보안 워크숍, 차세대 인프라 보안 워크숍 등에 참석을 지원하여 참여대학원생의 연구 능력을 향상시켰음
- ■ 국내·외 전문가 초청 강연을 진행하여 전공 분야 최신 연구주제 집중특강 및 교수/국내외전문가/대학원생 간 3자 간담회 등을 통해 연구 활동과 학문에 대한 다양한 경험과 열정을 공유함으로써 대학원생에게 미래가 요구하는 과학 인재로 성장할 기회를 제공함
- ■ 본 교육연구단은 전담 행정인력을 1명 채용할 수 있도록 지원하고 있으며, 산학협력단 내에 배정된 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> 2023.2월 졸업한 교육연구단 소속 학과(부) 참여대학원생 취(창)업률 실적

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				
2023년 2월 졸업자	석사	15	1	0	0	14	12	89
	박사	4			0	4	4	

▶ 김한기 학생은 비선형 연산 수가 적은 S-Box의 설계 및 응용에 관한 암호학 연구를 기반으로 국내 안전한 금융 보안에 기여하는 금융보안원에 취업하였음

▶ 김소람 학생은 IoT 기기와 데이터베이스의 포렌식 분석 연구를 기반으로 국가 핵심 보안 기술 연구를 담당하는 국가보안기술연구소에 취업하였음

▶ 최용철 학생은 모바일 환경에서의 Vault앱 은닉 및 암호화 알고리즘의 포렌식 분석 연구를 기반으로 디지털 포렌식 컨설팅 업무를 담당하는 HM컴퍼니에 취업하였음

▶ 박종현 학생은 부채널 정보 기반 블록암호의 효율적인 키복구 연구를 진행하여 정보보호제품의 안전성과 신뢰성을 보증하는데 기여하는 한국시스템보증에 취업하였음

▶ 장찬국 학생은 이동 통신 보안 연구를 기반으로 국민대학교에 연구교수로 취업하여 이동통신 암호 기술 고도화와 함께 보안 시스템 설계, 개발 등의 연구를 진행하고 있음

▶ 김현기 학생은 펌웨어 내의 암호모듈 수행 연구를 기반으로 In-Car와 Out-Car 영역 전반의 소프트웨어와 인프라를 안정적, 효율적, 혁신적으로 지원하는 기업인 현대 오토에버에 취업하였음

▶ 김태완 학생은 이동 통신 보안과 방사선 동위 원소 기반의 양자 난수에 대한 연구 기반으로 국방력 강화와 자주국방 완수에 기여하는 국방과학연구소에 취업하여 국방에 필요한 무기 및 국방과학기술에 대한 기술적 조사, 연구, 개발 및 시험 등을 담당함

▶ 이세윤 학생은 이동 통신 보안 및 양자 내성 암호에 관한 연구를 기반으로 KT에 취업하여 암호 기술 고도화와 함께 보안 시스템 설계, 개발 등의 연구를 진행하고 있음

▶ 정서우 학생은 방첩사령부에 취업하여, 군사보안, 국방 내의 암호 기술 고도화를 위한 보안 시스템 설계, 개발 등의 연구를 진행하고 있음

▶ 유현도 학생은 양자 난수에 기반한 난수발생기 후처리 알고리즘 개발 및 병렬 구현에 관한 연구를 기반으로 차량사이버보안 관련 컨트롤 타워로써 차량 보안 강화를 위한 보안 기술을 개발하고 차량에 적용하도록 지원하는 기업인 현대 자동차에 취업하였음

▶ 김수진 학생은 소프트웨어, 하드웨어 구현된 양자 내성 암호 부채널 분석 안전성 연구를 기반으로 국가보안기술연구소에 취업하여 소프트웨어 보안 기술 연구 업무를 수행하고 있음

▶ 김연재 학생은 소프트웨어, 하드웨어 구현된 블록 암호 부채널 분석 안전성 연구를 기반으로 LIG 넥스원에 취업하여 암호 장비의 전자파 취약점 분석 업무를 진행하고 있음

▶ 안성현 학생은 전자파 신호 처리 및 분석 연구를 기반으로 LIG 넥스원에 취업하여 드론에 대한 안전성 분석 업무를 진행하고 있음

▶ 문혜원 학생은 소프트웨어 구현 암호가 탑재된 암호 장비의 안전성 분석 연구를 기반으로 쿤텍(주)에 취업하여 화이트박스 암호 구현 및 안전성 분석 업무를 진행하고 있음

▶ 우지은 학생은 소프트웨어 구현 암호 부채널 분석 안전성 연구를 기반으로 코나아이에 취업하여 스마트 카드 암호 구현 업무를 진행하고 있음

▶ 전창열 학생(2023.2. 졸업)은 부호기반 양자내성 암호를 연구하여 이를 기반으로 국민은행에 취업하여 금융 서비스 보안 솔루션을 개발하고 있음

3. 참여대학원생 연구실적의 우수성

① 참여대학원생 저명학술지 논문의 우수성

▶ 자체평가 대상 기간 내 국제 저널 15편, 국내 저널 13편 논문 등재의 성과를 냄

▶ 국제 저널

- 참여학생 김기윤은 “A method for decrypting data infected with Hive ransomware” 논문을 통해 국제적으로 이슈가 되었던 Hive 랜섬웨어에 감염된 파일의 복구 방안을 세계 최초로 제시하고 이를 실험적으로 증명하였음.
- 참여학생 백승준은 “Quantum rebound attacks on reduced-round ARIA-based hash functions” 논문을 통해 ARIA 블록암호를 기반으로 하는 해시함수의 양자 보안성을 상세히 분석하고, 이전 관련 연구에 오류가 존재함을 보임.
- 참여학생 허욱은 “A study on cloud data access through browser credential migration in Windows environment” 논문을 통해 윈도우 환경의 다양한 브라우저에서 사용자 크리덴셜을 사용한 클라우드 데이터 획득 방법을 제시함.
- 참여학생 최영락은 “Practical Entropy Accumulation for Random Number Generators with Image Sensor-Based Quantum Noise Sources” 논문을 통해 암호 시스템의 기반이 되는 난수에 관한 연구로 이미지 센서 기반 양자 난수 발생기에 대한 엔트로피 축적 방법을 제안함.
- 참여학생 박영재는 “End-to-End Post-Quantum Cryptography Encryption Protocol for Video Conferencing System Based on Government Public Key Infrastructure” 논문을 통해 End-to-End 통신에서 GPKI를 활용하는 화상회의 보안 시스템 구축 방식을 제안함.
- 참여학생 오종민은 “APSec1.0: Innovative Security Protocol Design with Formal Security Analysis for the Artificial Pancreas System“ 논문을 통해 의료사물인터넷(MIoT) 중 대표적인 인공 췌장 시스템의 보안 취약점을 보완하고 보안 요구사항을 고려한 새로운 보안 프로토콜을 제안하고 BAN 논리와 AVISPA 정형화 검증 도구를 통해 검증하고 여러 보안 프로토콜과 성능 비교 및 분석하여 프로토콜의 우수성을 제시함.
- 참여학생 김영범은 “Optimized Implementation of PIPO Block Cipher on 32-bit ARM and RISC-V Processors” 논문을 통해 32-bit 환경인 ARM과 RISC-V 환경에서 블록암호 PIPO에 대한 최적화 구현 방안을 제안함.
- 참여학생 김영범은 “Signature Split Way for PQC-DSA Compliant with V2V Communication Standards” 논문을 통해 PQC-DSA를 분할하여 V2V 프로토콜에서 효율적으로 연산이 가능한 최적화 방안을 제안함.
- 참여학생 최호진은 “AVX512Crypto: Parallel Implementations of Korean Block Ciphers Using AVX-512” 논문을 통해 AVX512 환경에서 다양한 국내 블록암호 최적화 방안을 제안함.

▶ 국내 저널

- 참여학생 박종현은 “Skinny-128-384 와 Romulus-N 의 SITM 공격” 논문을 통해 Skinny-128-384 및 Romulus-N 블록 암호에 대한 새로운 SITM 공격을 제안함
- 참여학생 박귀은은 “iOS 환경에서의 협업 툴 아티팩트 분석 및 크리덴셜 활용 방안 연구” 논문을 통해 iOS 환경에서 사용되는 협업 툴의 아티팩트를 분석하고, 이러한 아티팩트를 크리덴셜 관점에서 활용하는 방안을 제시함
- 참여학생 박귀은은 “볼륨 암호화 및 백업 응용프로그램에 대한 복호화 방안 연구” 논문을 통해 볼륨 암호화 및 백업 기능을 제공하는 Cryptomator와 Norton Ghost를 분석하고, 데이터 복호화 방안을 제시함
- 참여학생 백승준은 “모바일 인스턴트 메신저에 대한 TMTO 및 GAN 모델을 활용한 안전성 분석” 논문을 통해 10종의 모바일 인스턴트 메신저에 대한 TMTO 및 GAN 모델을 활용한 안전성 분석을 제시함
- 참여학생 이민정은 “Dm-crypt류 기반 암호화 사용 흔적 조사 및 주요 데이터 수집 절차” 논문을 통해

Windows 환경에서 dm-crypt류 기반 암호화 도구의 사용 흔적 파악 방법과 이를 토대로 대상 암호화 도구를 특징짓는 방법을 제시함

- 참여학생 정서우는 “무선랜 환경에서 양자 엔트로피 칩 기반 암호모듈을 적용한 드론 피아식별과 안전한 정보 제공 기술 제안” 논문을 통해 드론 시스템 중 드론의 군집 비행 시스템과 이를 위한 이음 5G와 같은 이동통신 특화망에서 무선랜과 양자 엔트로피 기반 난수 발생기를 탑재한 암호모듈을 활용하여 군집 비행 드론 간 피아식별 및 안전한 정보 제공 기술 방법을 제안하고, 구현에 참고할 수 있는 테스트 벡터를 제공함
- 참여학생 황아리는 “수중 노이즈 상황에서의 기하학 기반 적외선 통신 채널 모델” 논문을 통해 Beer-Lambert의 감쇠 법칙과 기하학적 광학을 이용하여 기포에 대한 새로운 수학적 채널 모델링 기법을 도입하여 거리, 전력 및 물 유형에 따른 광통신의 성능을 시뮬레이션을 통해 분석함
- 참여학생 권수진, 박영재, 류지은은 “NTRU를 결합한 하이브리드 세션 보호 프로토콜을 이용한 금융 오픈 API 환경의 거래 세션 안전성 강화” 논문을 통해 NIST 양자내성암호 공모전 3라운드 후보 알고리즘이었던 NTRU를 사용하는 하이브리드 세션 키 교환 기법을 설계하고 성능을 분석함.
- 참여학생 최영락은 “블랙박스 암호모듈에 적용 가능한 CRYSTALS-Kyber의 은닉채널 공격과 IP카메라의 잠재적 보안 위협” 논문을 통해 내부 구조가 투명하게 공개되지 않은 완제품 형태의 카메라에 대한 은닉채널 존재 가능성을 제시하고 이에 대응하기 위한 기법을 제시함.
- 참여학생 김건우는 “5G 특화망의 성공적 정착을 위한 보안 고려사항 연구” 논문을 통해 이음5G 네트워크 내에 발생 가능한 위협에 대해 분석하였으며 그에 대응할 수 있는 보안 고려사항을 제안함
- 참여학생 문혜원은 “레이저 오류 주입 공격 성공률 향상을 위한 전자파 및 열 정보 활용 시스템” 논문을 게재하여 레이저 오류주입 공격의 성공률을 향상시키기 위해 분석 대상 장비가 동작하는 동안 발생하는 전자파 및 열 정보를 이용한 시스템을 제안함
- 참여학생 우지은은 “이종 디바이스 환경에 효과적인 신규 딥러닝 기반 프로파일링 부채널 분석” 논문을 게재 딥러닝 기반 비프로파일링 부채널 분석에서 효과적인 신경망 모델 설계방안을 제시함
- 참여학생 김동천은 “NIST PQC 공모전 동향 분석 및 표준화 대상 & Round 4 알고리즘 소개” 논문을 통해 NIST PQC 공모전 동향에 대해 분석하고 표준화 대상을 조사하였으며 각 알고리즘 프리미티브들을 분석함.

② 참여대학원생 학술대회 대표실적의 우수성

▶ 자체평가 대상 기간 내 국제 학회 20편, 국내 학회 50편 논문 등재의 성과를 냄

▶ 국제 학회

- 참여학생 허욱은 DFRWS USA 2023 Conference에서 “A study on cloud data access through browser credential migration in Windows environment” 논문을 발표함. 본 논문은 윈도우 환경의 다양한 브라우저에서 사용자 크리덴셜을 사용한 클라우드 데이터 획득 방법을 제시함.
- 참여학생 전용진은 International Conference on Platform Technology and Service (PlatCon) 2023에서 “Study on MC-Optimal S-Box Circuits” 논문을 발표함. 본 논문은 암호학적으로 안전한 S-box를 구성하기 위해 고려되어야 하는 MC (Multiplicative Complexity)를 주로 연구하며, 최적의 MC를 갖는 S-box를 찾는 방법을 제시하였음.
- 참여학생 신하 쉬르티카는 “Pros and Cons of Switching between LTE and Wi-Fi in Maritime” 논문을 통해 대량의 데이터를 수집하고 전송하기 어려운 열악한 수중 환경에서 데이터를 중앙 서버로 전송할 필요 없이 디바이스가 공유 머신러닝 모델을 학습할 수 있도록 지원하는 Federated learning(FL)을 이용하여 문제 해결 방안을 제시함
- 참여학생 신하 쉬르티카는 “A Survey of Deep/Machine Learning in Maritime Communications” 논문을 통해

다양한 해양 IoT 및 광대역 서비스 사용 사례를 제공하는 해양 네트워크 토폴로지에서의 머신/딥러닝 활용에 대해 기술하고 엣지 컴퓨팅, 빅 데이터 분석, 사물 인터넷(IoT)을 결합하여 이러한 시스템의 기능을 더욱 향상시킬 수 있는 방법에 대해서도 설명하였음

- 참여학생 박영재는 논문 “End-to-End PQC Encryption Protocol for GPKI Based Video Conferencing Systems”을 통해 화상 회의 시스템의 End-to-End 프로토콜에 양자내성암호를 적용하는 과정에 GPKI를 접목하는 방법을 제안함. 본 논문은 최우수 학회 논문으로 선정되어 ICEIB 2023 Best conference paper award를 수상함.
- 참여학생 김건우는 The 6th International Symposium on Mobile Internet Security (MobiSec 2022) 국제 학술대회에서 “Blockchain Applied 5G Authentication and Key Agreement Evaluation” 포스터를 발표함. 본 포스터는 5G 1차인증 과정에서 블록체인을 활용하여 코어망의 안전성을 올리는 연구를 분석하였음
- 참여학생 손대현은 The 6th International Symposium on Mobile Internet Security (MobiSec 2022) 국제 학술대회에서 “A study on machine learning-based false base station detection method in 5G“ 구두 발표를 통해 지도학습 알고리즘을 사용하여 허위 기지국을 탐지하는 연구를 수행하고, 허위 기지국을 탐지하는 5G Native 네트워크 기능을 제안함.
- 참여학생 오종민은 The 6th International Symposium on Mobile Internet Security (MobiSec 2022 국제 학술대회에서 “Formal Security Analysis for TLS 1.3 using AVISPA tool“ 포스터 발표를 통해 대표적인 인터넷 통신 프로토콜 TLS 1.3을 분석하고 AVISPA 정형화 검증 도구를 사용하여 프로토콜 검증을 수행하여 프로토콜의 취약점을 분석하고 검증함
- 참여학생 허재원은 ICISC 2022에서 “Differential Fault Attack on AES using Maximum Four Bytes Faulty Ciphertexts” 논문을 발표하여 AES 암호 알고리즘의 9라운드에서 최대 네 바이트에 오류가 주입되었을 때의 암호문을 통해 비밀키를 복구하는 차분 오류 공격을 제시함
- 참여학생 김영범은 MobiSec 2022에서 “Simulation of Vehicle-to-Vehicle Communication based on selected PQC-DSA” 논문을 발표함. 본 논문은 표준화를 위한 최적화된 PQC-DSA를 기반으로 V2Verifier의 서명 생성 및 검증방법을 제안함
- 참여학생 최호진은 MobiSec 2022에서 “AVX512Crypto : Parallel Implementation methods of Korean Block Cipher using AVX-512” 논문을 발표함. 본 논문은 AVX-512를 이용한 한국 블록 암호 병렬 구현 기법을 제안함
- 참여학생 김영범은 WISA 2023에서 “High-Performance Kyber implementation on ARMv7-based ARM Neon Technology” 주제를 발표함. ARMv7 기반 ARM Neon 기술에서의 고성능 Kyber 구현 기법을 제안함
- 참여학생 김동천은 WISA 2023에서 “Accelerating Key Derivation Function on GPU Architectures” 주제를 발표함. GPU Architectures에서의 Key Derivation Function 가속화 기법을 제안함
- 참여학생 김영범은 WISA 2023에서 “Efficient Implementation of Kyber on MSP430 Environment” 주제를 발표함. MSP430 환경에서의 Kyber 최적화 기법을 제안함
- 참여학생 김영범은 WISA 2023에서 “Implementation of Montgomery Reduction and Butterflies for CRYSTALS-Dilithium on RISC-V” 주제를 발표함. RISC-V 환경에서 CRYSTALS-Dilithium의 Montgomery Reduction 및 Butterflies 구현 기법을 제안함
- 참여학생 김영범은 WISA 2023에서 “V2V-MHT Accelerated V2V Authentication Framework using Merkle Hash Tree” 주제를 발표함. Merkle Hash Tree (MHT)를 활용한 V2V-MHT 프로토콜을 제안함
- 참여학생 김동천은 WISA 2023에서 “Optimization Study of Parallel Implementation” 주제를 발표함. 병렬 구현의 최적화 기법을 제안함
- 참여학생 김동천은 WISA 2023에서 “Tabling GHash in LEA-GCM and optimizing” 주제를 발표함. LEA-GCM에서의 GHash Tabling 최적화 기법을 제안함
- 참여학생 김영범은 WISA 2023에서 “Efficient implementation of multiplication reduction over NIST prime P-384 for 8-bit AVR Processor” 주제를 발표함. 8-비트 AVR 프로세서를 위한 NIST 소수 P-384에서의 multiplication reduction 최적화 기법을 제안함

▶ 국내 학회

- 참여학생 조세희는 2022 정보보호학회 동계 학술대회에서 “NIST LWC 최종 후보 Ascon-XOF에 대한 안전성 분석” 논문을 통해 미국 NIST LWC (LightWeight Cryptography)의 최종 후보 Ascon-XOF의 안전성 분석을 수행하였으며, MILP solver를 이용하여 실제 충돌쌍을 찾을 수 있는 효율적인 차분 경로를 제안함.
- 참여학생 박귀은은 2022 정보보호학회 동계 학술대회에서 “협업 툴 TeamUp과 Agit 데이터베이스 복호화 방안 및 아티팩트 분석 연구” 논문을 통해 데이터를 암호화하여 저장하는 협업 툴인 TeamUp과 Agit를 분석하여 데이터를 복호화하고 아티팩트 분석을 수행함.
- 참여 학생 윤혜진은 “드론 보안 시스템의 PQC 마이그레이션에 대한 연구” 논문을 통해 드론 기술에서 적용하고 있는 암호체계를 분석하고 양자컴퓨팅으로부터 위협을 받을 수 있는 암호 알고리즘을 PQC 알고리즘으로 적용하는 마이그레이션 연구를 제안함
- 참여 학생 김형엽은 “5G 상용망 연동을 위한 탈부착형 하드웨어 암호모듈 설계” 5G는 이동통신망 외의 구간에서 전송되는 데이터에 대한 보안은 보장하지 못하기에 5G 기반으로 제공되는 서비스를 사용할 때, 단말과 서비스를 제공하는 개체 간의 종단 간 보안을 확보하기 위해서는 직접 보호 조치를 수행해야 함. “5G 상용망 연동을 위한 탈부착형 하드웨어 암호모듈 설계” 논문을 통해 단말에 부착하여 종단 간 보안을 제공할 수 있는 탈부착형 하드웨어 암호모듈을 제안함
- 참여 학생 나태경은 “양자 키 분배 기술과 활용 동향” 논문을 통해 양자 암호의 기술 중 하나인 양자 키 분배 기술의 특징과 양자 키 분배를 사용한 사례를 소개함
- 참여 학생 윤혜진은 “AHS 프로토콜을 적용한 드론 인증 시스템” 논문을 통해 드론 운용 환경에서의 취약점을 분석하고 오프라인 환경에서의 인증 프로토콜인 AHS 프로토콜을 드론 운영환경에 적용한 인증시스템을 설명
- 참여 학생 김형엽은 “이동통신망과-국방광대역통합망 연동을 위한 qSIM 기반 인증의 필요성 연구” 논문을 통해 사용자 인증 에 대한 보안 요구사항을 정의하고, 이를 만족하는 양자 엔트로피 기반의 암호모듈인 qSIM과 qSIM 기반의 인증 활용 방안을 제안함
- 참여 학생 나태경은 “HMAC-SHA1 알고리즘을 사용하는 OTP 단말기의 평문과 키 추정 연구” 논문을 통해 OTP에서 출력되는 비밀번호의 생성 원리와 OTP 예측 가능성을 분석하고 OTP 단말기의 평문과 키 추정 연구를 진행함
- 참여 학생 윤혜진은 “양자암호통신장비를 활용한 광대역 네트워크 운영환경에 대한 암호학적 안전성 분석 및 활용방안” 논문을 통해 양자암호통신장비의 보안 요구사항을 분석하고, 양자암호통신장비의 도입시 고려해야하는 가용성을 분석함
- 참여학생 황아리는 “극한지 빅데이터를 위한 남극 IoT 네트워크 엔티티” 논문을 통해 극한지의 특징을 이해하고 대표적인 극한지인 남극 현장에서 활동하는 인구가 처한 문명권 대비 극심한정보격차의 원인을 이해하고 문제 극복을 위해 저자가 제시한 남극 IoT 네트워크 아키텍처 개발을 위해 선행한 네트워크참여 엔티티들의 정의 결과를 통해 극한지와 같은 인간 활동 제약 조건에서도 미래 추론이 가능한 ‘극한지 빅데이터’ 구축의실현 가능성에 대해 제시함
- 참여학생 신하 쉬르티카는 “Key factors for Maritime Communications: Challenges and Trends” 논문을 통해 주파수 및 채널 변경을 위해 많은 수동 절차에 의존하고 있는 해상 시스템에 대해아 주어진 전략적 전환의 장단점을 비교하고 머신러닝 기반 전환을 통하여 시스템 개선 방안을 제시함
- 참여학생 신하 쉬르티카는 “Federated Learning-Internet of Underwater Things” 논문을 통해 다양한 수중 디바이스에 의해 생성되는 데이터 양이 증가함에 따라 해상에서 효과적인 데이터 전송을 제공하고 있는 해상 통신의 다양한 동향과 연구에 대해 기술함
- 참여학생 유현도, 최영락은 “이미지센서 기반 진난수생성기에 적용 가능한 효율적인 엔트로피 축적 방법” 논문을 발표함. 본 논문은 이미지 센서 기반 양자난수생성기의 엔트로피 축적 방법을 설계하고 성능을 분석하여 후처리 알고리즘의 활용 가능성을 보임.

■ 참여학생 박영재, 유현도는 “Jetson nano 환경에서의 경량 암호학적 난수발생기 병렬 구현” 논문을 발표함. 본 논문은 경량 대칭 블록암호 CHAM을 활용한 난수발생기를 병렬화하여 GPU가 탑재된 임베디드 보드에서의 성능을 평가하고 표준 AES 알고리즘을 활용할 때보다 효율적임을 보임.

■ 참여학생 류지은, 유현도는 “병렬 잡음원 기반 난수발생기에 적합한 엔트로피 건전성 시험” 논문을 발표함. 본 논문은 병렬 잡음원에 적용 가능한 난수발생기 헬스 테스트 기법을 설계하고 효율성을 평가하여 단일 잡음원에 대한 건정성 시험만을 사용할 때보다 효율적임을 보임.

■ 참여학생 오종민은 2023 한국정보보호학회 하계학술대회 (CISC-S'23)에서 “자동화된 정형화 검증 도구를 사용한 완전 순방향 비밀성을 지원하는 TLS 1.2 프로토콜에 관한 PAL 3급의 보안성 검증 분석“ 논문을 통해 대표적인 암호화 프로토콜인 TLS 1.2에서 완전 순방향 비밀성을 지원하는 Diffie-Hellman 키 교환 방식을 분석하고 AVISPA 정형화 검증 도구를 사용하여 프로토콜의 보안성 검증을 수행함.

■ 참여학생 임아정은 2023 한국정보보안학회 하계학술대회 (CISC-S'23)에서 “블록체인과 머클해시트리를 이용한 데이터 무결성검증에 관한 연구 스마트 HACCP의 CCP 데이터를중심으로“ 논문을 통해 블록체인과 머클트리를 이용하여 HACCP인증에 사용되는 CCP데이터에 대한 무결성 검증 모델을 제시하였음.

■ 참여학생 손대현은 2023 한국 정보보호학회 하계학술대회에서 (CISC-S'23)에서 “이음 5G에서 연합 학습 시스템 연구“ 논문을 통해 이음 5G망에서 기계 학습을 이용하여 허위기지국을 탐지하고 여러 이음 5G망이 연합 학습을 통해 탐지 정확도를 향상시키는 시스템 모델을 제시하였음.

■ 참여학생 손대현은 2023 한국 스마트미디어학회 종합학술대회에서 (KISM-S'23)에서 “5G 초기 인증단계에서 Linkability 공격에 대응 가능한 5G-AKA' 프로토콜 취약점 분석“ 논문을 통해 개인정보보호에 있어 효과적인 방안을 제시한 5G-AKA' 프로토콜임에도 불구하고 해당 프로토콜에서 발생할 수 있는 취약점에 대해 분석하였음.

■ 참여학생 손대현은 2023 한국정보보호학회 하계학술대회 (CISC-S'23)에서 “설명 가능한 XGBOOST 기반의 허위기지국 탐지 기법“ 논문을 통해 XAI 기법 중 하나인 SHAP 알고리즘을 적용하여 모델의 예측 결과를 시각화하고 해석하였음.

■ 참여학생 김건우는 “5G 초기인증의 순방향 비밀성 지원을 위한 5G-IPAKA 보안 프로토콜 취약점 분석” 논문을 통해 5G-IPAKA 보안 프로토콜의 취약점 분석을 수행함. 취약점 분석 결과 해당 프로토콜이 안전하지 않음을 정형화 검증을 통해 분석하였으며, 발생 가능한 공격에 대해 제시함

■ 참여학생 김연재는 “경량 블록암호 PIPO에 대한 도메인 지향 마스킹 기법” 논문을 통해 경량 블록암호 PIPO에 대한 하드웨어 부채널 분석 대응기법으로 도메인 지향 마스킹 기법을 적용한 방법을 제시함

■ 참여학생 김수진은 “CRYSTALS-KYBER 다항식 곱셈의 하드웨어 병렬 구현에 대한 상관 전력 분석” 논문을 통해 NIST PQC KYBER의 하드웨어 병렬 구현된 다항식 곱셈에 대해 상관전력분석 기법을 제시하고 병렬 구현마다의 공격 성능 변화 추이를 분석함

■ 참여학생 김수진은 “하드웨어 구현 CRYSTALS-KYBER 암호문 비교 연산에 대한 부채널 분석” 논문을 통해 하드웨어 구현된 NIST PQC KYBER의 디캡슐레이션 과정에서 암호문 비교연산을 대상으로 전력분석을 통해 비밀키를 복구하는 방법을 제시함

■ 참여학생 허재원은 “DDR4 DRAM의 소프트웨어 기반 Rowhammer 기법과 전자파 오류주입 기반 Ehammer 기법에 관한 연구” 논문을 통해 DDR4 DRAM의 메모리를 변조하는 소프트웨어 기반 Rowhammer 공격과 전자파 오류주입 기반 Ehammer 공격을 비교 분석함

■ 참여학생 최건희는 “비교 연산 기반 상수시간 CDT 샘플링에 대한 단일 파형 분석” 논문을 통해 PQC 알고리즘에 많이 사용되는 상수시간 CDT 샘플링 중 비교 연산 기반의 코드에 대해 단일 파형 분석을 제시함.

■ 참여학생 한재승은 “KpqC 전자서명 후보 AIMer에 대한 부채널 및오류주입 공격” 논문을 통해 KpqC 전자서명 후보인 AIMer에 대한 상관전력분석과 오류주입공격을 제안하고 MCU 환경에서 실험을 수행함

■ 참여학생 최호진은 정보보호학회 동계학술대회 2022에서 “GPU 환경에서의 해시 기반 전자 서명 SPHINCS+ FORS 최적화 방안” 논문을 발표함. 본 논문은 GPU 환경에서의 SPHINCS+ FORS 병렬 연산 기법을 제안함

■ 참여학생 최호진은 정보보호학회 동계학술대회 2022에서 “MS office2013+ 다중 파일 크래킹 방안” 논문을 발표

함. 본 논문은 GPU 아키텍처 상에서의 MS office2013+ 다중 파일 패스워드 크래킹 방안과 Markov Password Table의 복사 과정을 최소화하여 다중 파일에 대한 크래킹 방안을 제안함

- 참여학생 최호진은 2022 한국정보호호학회 동계학술대회에서 “GPU 환경에서의 국산 해시 함수 LSH 벤치마킹” 논문을 통해 GPU의 아키텍처 특징을 이용하여 해시 함수 LSH에 대한 벤치마킹을 제시함
- 참여학생 최호진은 2022 한국정보호호학회 동계학술대회에서 “GPU 아키텍처 상에서의 격자 기반 양자 내성 암호 최적화 동향” 논문을 통해 병렬 연산이 가능한 GPU 아키텍처에서 격자 기반 양자내성암호에 대한 최적화 동향을 제시함
- 참여학생 김영범은 2022 한국정보보호학회 동계학술대회에서 “IoT 환경에서의 격자 기반 양자 내성 암호 최적 구현 동향” 논문을 통해 격자 기반 양자내성암호에 대해 IoT 환경에서 사용되는 저사양 기기들에서의 최적화 구현 동향을 제시함
- 참여 학생 김영범은 2022 한국정보보호학회 동계학술대회에서 “AVR 환경에서 표준화 대상 양자내성암호 Crystals Kyber 최적화 구현 연구” 논문을 통해 저사양 기기인 8-bit AVR 환경에서 표준화 대상 알고리즘인 Kyber의 최적화 구현 방안을 제시함
- 참여 학생 김영범은 2022 한국정보보호학회 동계학술대회에서 “8-bit AVR 환경에서의 PIPO, CHAM 최적화 구현” 논문을 통해 저사양 기기인 8-bit 환경에서 국내 블록암호 알고리즘인 PIPO와 CHAM에 대한 direct indexing 기법을 제안함
- 참여학생 김영범은 2023 한국정보보호학회 하계학술대회에서 “ARMv7 기반 Cortex-A에서의 Kyber 구현 최적화 연구“ 논문을 발표함. 본 논문은 ARM Coretx-A 시리즈에서 Kyber에 대한 주요 연산들의 최적화 방안을 제시함
- 참여학생 김동천은 정보보호학회 하계학술대회 2023에서 “GPU환경에서의 PBKDF2-HMAC-SHA2 최적화” 논문을 발표함. 본 논문은 비밀 키 생성 알고리즘에 대한 해독 기법을 적용하기 위해 파생 키 암호알고리즘인 PBKDF2에 대한 최적화 기법을 제안함
- 참여 학생 김영범은 2023 한국정보보호학회 하계학술대회에서 “16-bit MSP430환경에서 kyber 고속화 구현“ 논문을 통해 저사양 기기인 16-bit MSP430 환경에서 Kyber의 주 연산인 다항식곱셈 알고리즘 최적화 방안을 제시함
- 참여학생 김영범은 정보보호학회 하계학술대회 2023에서 “RISC-V 환경에서 CRYSTALS-Dilithium의 Montgomery Reduction 및 Butterfly 연산 최적 구현” 논문을 발표함. 본 논문은 CRYSTALS-Dilithium에서 사용하는 Montgomery Reduction과 Cooley-Tucky, Gentleman-Sande Butterfly 연산을 32비트 RISC-V 환경에서 최적화 기법을 제안함
- 참여학생 김영범은 정보보호학회 하계학술대회 2023에서 “V2V-MHT: Merkle Hash Tree를 활용한 IEEE 802.11p WAVE 프로토콜 V2V 서명 검증 가속화” 논문을 발표함. 본 논문은 차량 내 단말기인 OBU(On-Board-Unit)의 연산 부하를 줄이기 위해 ECDSA를 대신하여 MHT의 Root packet 값으로 V2V 인증 가속화 기법을 제안함
- 참여학생 김동천은 정보보호학회 하계학술대회 2023에서 “GPU 환경에서의 Scrypt 알고리즘 병렬 구현 최적화 연구” 논문을 발표함. 본 논문은 1 스레드 1 scryptROMix 구현을 기반으로 Scrypt의 성능 향 상을 위해 Scrypt의 내부 연산인 PBKDF2-HMAC-SHA256 함수에 대한 CPU와 GPU의 워크 스케줄러에 대한 방안을 제시함
- 참여학생 김동천은 정보보호학회 하계학술대회 2023에서 “LEA-GCM GPU상 동일 키에 따른 tabling, constant memory 사용 및 최적화“ 논문을 발표함. 본 논문에서는 GPU 상에서 병렬 로직을 이용하여 LEA-GCM 모드를 최적화하는 방안을 제시함
- 참여학생 김민기는 정보보호학회 하계학술대회 2023에서 “8-bit AVR 환경에서 P-384 곱셈 Reduction 연산 최적화” 논문을 발표함. 본 논문은 8-bit AVR 환경에서 Range Shifted Representation을 이용하여 NIST P-384 커브에서 효율적인 유한체 곱셈 최적화 기법을 제안함

③ 참여대학원생 특허, 기술이전, 창업 실적의 우수성

▶ 자체평가 대상 기간 내 국내특허 등록 7건/출원 32건, 국제특허 출원 2건, 기술이전 4건, 소프트웨어 등록 12건, 국내 표준 3건의 성과를 냄

▶ 국내특허

■ 양자보안 통신장치 통합형 원방감시 제어 시스템 및 방법 (등록)

✓ 양자보안 이동기록 데이터를 수신하여 기기 식별키를 추출하고 기기 식별키를 기초로 양자보안 키를 결정하여 이동기록 데이터를 검출하며, DIM에 대하여 사전에 양자 키 분배를 수행하여 양자보안 키 주입을 처리하는 중앙 이동기록처리 유닛 시스템을 제안함

■ 5G SIDF 암호처리장치 및 그 방법 (등록)

✓ 복수의 GPU(Graphic Processing Unit)를 병렬코어로 구성하여 각 단말에서의 ECIES(Elliptic Curve Integrated Encryption Scheme) 병렬 복호화를 수행함으로써 5G 이동통신망에 단말이 실시간으로 대량으로 접속할 시 SIDF 부하를 줄이고 처리시간을 줄일 수 있는 5G SIDF 암호처리장치 및 그 방법을 제공함

■ 인공신경망을 이용한 RSA 암호에 대한 부채널 분석 방법 및 장치 (등록)

✓ 인공 신경망을 이용해 RSA 암호의 비밀키를 분석하는 방법을 개발한 특허임

■ 스마트기기용 양자보안 통신 제공장치 및 방법 (출원)

✓ 스마트기기에 연결하여 암호보안 통신을 통해 기기 식별을 지원하고 안전하게 데이터를 송수신할 수 있는 스마트기기용 양자보안 통신 제공장치를 제안함

■ 양자암호 기반의 영상 식별 장치 및 방법 (출원)

✓ 영상 기기에서 생성되는 영상에 대한 식별 데이터를 양자암호의 보안을 통해 안전하게 저장하여 진위를 증명할 수 있는 양자암호 기반의 영상 식별 장치를 제안함

■ 양자암호 기반 수하물 식별 장치 (출원)

✓ 각각의 수하물에 대한 식별 데이터를 양자암호의 보안을 통해 안전하게 저장할 수 있는 양자암호 기반의 수하물 식별 장치 및 방법에 대해 제안함

■ 암호화된 데이터베이스의 암호화 모듈 식별 장치 및 방법 (출원)

✓ 데이터베이스 암호화에 취약한 암호화 모듈 사용 여부를 식별하고 식별된 암호화 모듈을 기초로 데이터 복호화 방안 제안한 특허임

■ 고 지연 네트워크에서 다중 통신 스펙트럼 기반 서비스 요청 추론 기법 (출원)

✓ 이기종 수중 네트워크 연동을 위해 주소 체계 상호 운용성을 제공하는 게이트웨이의 기능 및 동작을 개발한 특허임

■ 수중 무선 통신 시스템을 이용한 수중 무선 네트워크 구성 방법 (출원)

✓ 통신 인프라가 구축되지 않은 수중에서 한시적 네트워크 인프라 구축 기술을 개발한 특허임

■ 다중-모드 수중통신 장치 (출원)

✓ 단일 통신 시스템 내 물리적으로 성질이 다른 “다종의 수중 무선 신호 전송 장치”를 운용하는 기술. 다종의 수중 무선 신호와 수중 무선 전송 데이터를 수집하는 기술, 상기 수집 신호 및 데이터를 분석하는 기술, 다종의 수중 무선 신호 전송 장치를 탑재한 수중 장치들이 ‘인프라스트럭처 모드’, ‘애드혹 모드’로 수중 무선 네트워크를 구성하는 기술, 무선신호 전송을 위한 ‘링크 상태’ 관리 기술을 개발한 특허임

■ 이미지 센서 기반 엔트로피 축적 장치 및 방법, 이를 이용한 진난수생성기 (출원)

✓ 이미지 센서 기반 양자난수발생기에 적용했을 때 수학적으로 엔트로피 하한을 보장하는 양자난수발생기 엔트로피 축적 방법을 개발한 특허임

■ 모드버스 오류 처리 장치 및 방법 (출원)

✓ 모드버스 프로토콜에 TLS 중계 장치를 추가하여 모드버스 시스템에 대한 공격을 방어하고 오류를 처리

하는 방법을 개발한 특허임

■ 인퓨전 펌프에서 네트워크 기반 공격 감소 시도를 위한 MUD 적용 (출원)

✓ 인퓨전 펌프에 존재하는 다양한 보안 위협에 대하여 MUD(Manufacturer Usage Description)를 활용하여 방지하는 기술

■ 5G 환경에서의 허위 기지국으로부터 SON 기능 보호를 위한 그룹 키 기반의 보안 체계 (출원)

✓ BMANF을 활용하여 FBS로부터 수신되는 Broadcast 메시지 수신을 방지하며, SON 기능에 대하여 데이터 품질을 향상 시킨 후, SON Poison 공격으로부터 네트워크를 보호하는 기능에 대한 특허임

■ 군집화 알고리즘을 이용한 블록암호 CTR 운영모드 부채널 분석 방법 및 장치 (출원)

✓ 블록암호의 CTR 운영모드의 부채널 정보들에 군집화 알고리즘을 적용해 비밀키를 분석하는 방법을 개발한 특허임

■ 블록암호에 대한 4바이트 이하 오류 기반의 차분 오류 분석 방법 및 장치 (출원)

✓ 블록암호 특정 라운드에 4바이트 이하의 오류주입을 통해 비밀키를 복구하는 차분 오류 분석 방법을 개발한 특허임

■ 비지도 도메인 적응을 이용한 프로파일링 부채널 분석 방법 및 장치 (출원)

✓ 비지도 도메인 적응을 프로파일링 부채널 분석에 적용하여 공격 대상 장비와 프로파일링 장비가 다를 때도 분석 가능한 방법을 개발한 특허임

■ 경량 블록 암호 PIPO에 대한 Threshold Implementation 적용 방법 (출원)

✓ 경량 블록 암호 PIPO에 대해 Threshold Implementation을 적용하여 부채널 분석 안전성을 가지게 하는 방법을 개발한 특허임

■ 경량 블록 암호 PIPO에 대한 Domain-Oriented Masking 적용 방법 (출원)

✓ 경량 블록 암호 PIPO에 대해 Domain-Oriented Masking을 적용하여 부채널 분석 안전성을 가지게 하는 방법을 개발한 특허임

■ 부채널 공격을 방지하기 위한 암호문 비교 장치 및 방법 (출원)

✓ PQC에 사용되는 암호문 비교 연산에서 비교 결과가 부채널 정보로 누출되는 것을 막는 알고리즘을 제안하여 부채널 안전성을 가지게 하는 장치 및 방법을 개발한 특허임

■ 다항식 연산 기반의 보안 알고리즘의 연산 처리 방법, 그리고 이를 구현하기 위한 장치 (출원)

✓ 다항식 연산 기반의 보안 알고리즘에서 연산 처리 순서를 섞어 부채널 분석 복잡도를 증가시키는 방법을 개발한 특허임

■ 스마트폰 소리 재생 시 누설되는 전자기파를 이용한 은닉 채널 (출원)

✓ 스마트폰이 무음 상태일 때 소리 재생 시 누설되는 특성 전자기파를 통해 은닉 채널을 형성하는 방법을 개발한 특허임

■ 경량 블록 암호 PIPO에 대한 Re-Consolidating Masking 적용 방법 (출원)

✓ 경량 블록 암호 PIPO에 대해 Re-Consolidating Masking을 적용하여 부채널 분석 안전성을 가지게 하는 방법을 개발한 특허임

■ 인공 신경망의 오분류 유도 방법 및 파라미터 복원 방법과 이를 위한 장치 (출원)

✓ 인공 신경망이 수행되는 동안 오류를 주입하여 오분류 유도 및 신경망 파라미터를 복원하는 방법을 개발한 특허임

■ 가상메모리 할당 및 해제를 이용한 은닉채널 형성 방법 및 장치 (출원)

✓ 컴퓨터에서 가상메모리 할당 및 해제를 수행할 때 방출되는 특성 전자기파 신호를 이용해 은닉채널을 형성하는 방법을 개발한 특허임

■ 크리스탈 카이버 연산 장치에 대한 상관 전력 분석 방법 및 장치 (출원)

✓ 양자 내성 암호인 크리스탈 카이버 연산 장치에 대해 상관 전력 분석을 적용하는 방법을 개발한 특허임

■ 마르코프 패스워드 테이블을 이용한 다중 파일 패스워드 크래킹 장치 및 방법 (출원)

✓ 다중 파일에 대한 패스워드 크래킹의 고속화를 통해 빠른 디지털 포렌식 결과의 도출이 가능한 마르코프 패스워드 테이블을 이용한 다중 파일 패스워드 크래킹 장치 및 방법에 관한 특허임

▶ 국제특허

■ DPAPI 기반의 데이터 재생성을 통한 클라우드 데이터 획득 장치 및 방법 (출원)

✓ 클라우드 접속을 위한 크리덴셜 및 크리덴셜 보호를 위해 Windows의 데이터 보호 API인 DPAPI를 사용하는 소프트웨어에 대하여 크리덴셜 재생성을 통해 클라우드 데이터를 획득하는 방법을 제안한 특허임

■ 양자 엔트로피 기반 일회용 양자 비밀번호 생성 장치 및 방법 (출원)

✓ 암호화 시드에 기초하여 일회용 양자 비밀번호(QTP)를 생성하고 일회용 양자 비밀번호(QTP)의 발급 내역을 블록체인 상의 노드에 저장하는 QTP 생성부를 포함한 일회용 양자 비밀번호 생성 장치를 제안함

▶ 기술이전

■ 양자키 유도 함수를 활용한 암호키 생성 방법 및 이를 수행하는 암호키 생성 장치

✓ 난수를 생성하여 암호키로 사용할 때 양자키 유도 함수를 활용하여 암호키를 생성하는 방법에 대한 기술

■ 화이트박스 암호화 기술

✓ 데이터 암호화를 위한 키를 암복호화하기 위하여 사용하는 비밀키를 안전하게 배포하기 위한 화이트박스 암호화 프로그램에 대한 기술

■ 양자내성암호 알고리즘 Kyber의 고속구현 기술 이전

✓ 양자내성암호 표준으로 선정된 KYBER의 고속 구현을 위하여 알고리즘을 구성하는 각 함수를 분석하고 구현 병목 현상을 해결한 암호 모듈 개발을 위한 기술

▶ 소프트웨어 등록

■ 경량 데이터베이스(SQLite)에 대한 비밀번호 검증 및 복호화 프로그램 등록

✓ 경량 데이터베이스(SQLite)에 대한 비밀번호 검증 및 복호화 프로그램

■ 드론 제어 데이터 관리를 위한 Replaying(재생) FDR(비행데이터기록) 장치용 프로그램 등록

✓ 임무를 수행하는 드론과 GCS(지상제어시스템)간의 메시징 프로토콜인 MAVLink 데이터를 Replaying application을 이용하여 드론과 GCS간의 송수신 데이터를 직접 받아 데이터를 관리하는 프로그램임

■ 공간정보 기반 식별용 에이전트 모듈(리눅스) 등록

✓ 수집한 공간 정보를 이용하여 드론 식별 정보를 생성하고, 관리하는 응용 프로그램

■ 암호모듈 기반 식별 체계용 시험 프로그램(윈도우) 등록

✓ 개체의 식별을 위하여 암호모듈을 기반으로 식별 정보를 생성하고 관리하는 기능을 시험하는 응용 프로그램

■ Curve25519를 이용한 Kyber의 SETUP 프로그램 등록

✓ KBYER를 사용하여 키 생성 시스템을 구축하여도 은닉 채널이 존재할 수 있음을 보이기 위한 시연 소프트웨어임

■ NTRU(엔트루)가 적용된 모드버스 TLS(티엘에스) 통신 프로그램 등록

✓ 격자기반 양자내성암호 NTRU를 사용하여 키 교환을 진행하고 해당 키로 모드버스 패킷을 TLS 상에서 암호화하여 통신할 수 있도록 중계하는 소프트웨어임

■ 측정 보고서(Measurement Report) 학습 데이터 전처리기 프로그램

✓ 이동통신 네트워크에서 발생할 수 있는 Measurement Report(미저먼트 레포트)를 기계 학습에 사용하기 위해 정규화 처리하는 전처리기임

■ 허위기지국 비정상 데이터 생성기

✓ 이동통신네트워크에서 발생할 수 있는 Measurement Report(미저먼트 레포트)을 정규화 처리한

데이터로부터 비정상 데이터를 생성하는 프로그램임

■ 경량 블록암호 피포(PIPO)의 안전한 하드웨어 마스킹 코드
  ✓ 경량 블록암호 PIPO의 하드웨어 구현에서 부채널 분석 대응기법 마스킹을 적용한 소프트웨어를 등록하였음

■ 신경망 활성 함수 소프트맥스(Softmax) 입력 대상 오분류를 유도하기 위한 비트 반전 시뮬레이션 알고리즘
  ✓ 신경망 활성 함수 소프트맥스의 입력 대상 오분류를 유도하기 위한 비트 반전 시뮬레이션 소프트웨어를 등록하였음

■ CUDA C 기반 고정 길이 파라미터에 대한 PBKDF2-HMAC-SHA Family 고속 생성 방안
  - GPU 기기의 병렬 처리를 통하여 입력 인자에 대한 암호학적 파생 키를 고속으로 병렬처리하는 도구임

▶ 국내 표준

■ TTA 정보통신표준화위원회 신규 표준화 과제 “양자키분배 후처리에 대한 시험방법” 채택
  ✓ QKD 시스템의 후처리 과정에 대한 표준이 존재하지 않으므로 가이드라인 및 구현 평가 기준이 나타난 표준 제정이 필요함. QKD 후처리 알고리즘에 대한 국내 표준 제정을 위한 신규 표준화 과제를 제안하고 채택됨

■ 사물인터넷융합포럼 표준화 제안, “보안 강화된 블록암호에 대한 결합 상관 부채널 분석 기술 요구사항 및 절차”, IoTFS-0250.

■ 사물인터넷융합포럼 표준화 제안, “전압 전자파 이종 오류원 기반 오류 주입 분석 기술 요구사항 및 절차”, IoTFS-0251.

4. 신진연구인력 현황 및 실적

▶ 연구교수 윤승환의 연구 활동

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

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

■ 표준화 활동
  ✓ ISO/IEC JTC 1/SC 27/WG 3 국제 보안평가 분야 전문가 활동 (2022.10.~ 현재)
  ✓ ISO/IEC TS 20540 코에디터(2023.04.~현재)

■ 교육 활동
  ✓ 공군 암호기술 및 암호모듈 활용기술, 국민대학교(2022.09.19.~2022.09.23.)
  ✓ 국민대-공군 무인체계 전문과정/암호보안과정, 국민대학교(2023.07.24.~2023.07.28.)
  ✓ 정보보호 기초 및 암호모듈 설계에 관한 기술 교육, 국민대학교(2023.07.10.~2023.07.19.)

■ 자문 활동
  ✓ 무선 통신 기술에 적용될 수 있는 키 교환 프로토콜 제안에 대한 자문, 경기과학고등학교 (2022.05.01.~2022.12.31.)
  ✓ 타원곡선 암호를 이용한 이미지 암호화 알고리즘 연구에 대한 자문, 경기과학고등학교 (2022.05.01.~2022.12.31.)

■ 국내 논문
  ✓ “무선랜 환경에서 양자 엔트로피 칩 기반 암호모듈을 적용한 드론 피아식별과 안전한 정보 제공 기술 제안”, 정서우, 윤승환, 이옥연, 정보보호학회논문지, 32(5), 2022.10

▶ 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

■ 교육 활동

✓ 공군 암호기술 및 암호모듈 활용기술, 국민대학교(2022.09.19.~2022.09.23.)

✓ 국민대-공군 무인체계 전문과정/암호보안과정, 국민대학교(2023.07.24.~2023.07.28.)

✓ 정보보호 기초 및 암호모듈 설계에 관한 기술 교육, 국민대학교(2023.07.10.~2023.07.19.)

■ 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 장찬국의 연구 활동

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

✓ 검증필암호모듈 설계 및 구현 연구

✓ 검증필암호모듈 기반 가상사설망 설계 연구

■ 5G+/6G 이동통신 보안 플랫폼 설계 및 구현에 관한 연구

✓ 5G 코어 네트워크 암호기술 연구

✓ 6G 코어 네트워크 내 양자키분배기술 연동 모델링에 관한 연구

■ 무인이동체 보안 연구

✓ 양자내성암호 기반 드론 보안 시스템 연구

✓ 무인이동체 보안 통제항목 비교・분석 및 국방 체계 적용 방안 연구

■ 교육 활동

✓ 국민대-국군방첩사령부 상용암호모듈 설계 및 구현 교육, 국민대학교(2023.03.13.~2023.03.17.)

✓ 국민대-공군 무인체계 전문과정/암호보안과정, 국민대학교(2023.07.24.~2023.07.28.)

✓ 정보보호 기초 및 암호모듈 설계에 관한 기술 교육, 국민대학교(2023.07.10.~2023.07.19.)

✓ 국민대-펜타시큐리티 검증필암호모듈 설계 및 구현 교육, 국민대학교(2023.09.~2023.12.)

5. 참여교수의 교육역량 대표실적

▶ 인재 양성을 위한 노력

■ 산업 사물인터넷과 디지털전환 기반 기술 및 발전 방향에 관한 “사물지능망특론” 대학원 강좌 개설

✓ 북미와 유럽을 중심으로 로봇 기반 제조 기술의 유연성과 신뢰도 향상을 목표로 하는 산업 사물인터넷과 디지털전환 기술 개발이 선도적으로 수행됨에 따라, 기반 기술인 지능형 사물인터넷 네트워크 구축에 필요한 기술과 발전 방향에 대한 대학원 강좌를 개설

✓ 참여대학원생들은 강좌를 통해 로봇 중심의 미래 제조 산업에서 예상되는 정보 교환 방법의 실제와 사물지능망 정보보안 취약점 모델을 설계하는 데 활용할 수 있음

■ ‘인공지능과 보안이론’ 등 다양한 교육 내용을 통해 신경망 및 심층신경망 실습으로 보안 이론에 활용할 수 있는 방안에 대해 고찰할 수 있도록 하여 지식을 심어 주었음

■ 제지산업에서의 폐수처리 기술을 실현하기 위한 핵심 요소 ‘블록체인을 통한 제지산업의 폐수처리 구조’의 기술 설계 및 논문지도, 극한지에서 센서 장치들의 데이터의 신뢰성을 증대하기 위한 블록체인 융합 데이터 관리 매커니즘 논문지도를 위한 교육 일정을 수립, 권호석, 강나영 등 20인 연구원의 연구력 향상을 위한 세미나, 외부 도메인 전문가를 초빙 등을 진행하였음.

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

■ 김종성 교수는 ‘디지털 포렌식 개론’ 과목을 개설하여 디지털 포렌식 수사과정과 실제 현장에서 사용되는 포렌식 분석 기술들을 강의함으로써 본교 대학원생들의 연구역량 강화에 기여함

■ 김종성 교수는 ‘해시함수와데이터인증’ 과목을 개설하여 암호 분야의 핵심 프리미티브인 해시함수의 개념과 안전성 개념을 강의하였고, 대학원생들이 해시함수를 기반으로 블록암호와 같은 다른 종류의 암호 프리미티브를 생성하는 방식을 습득할 수 있도록 하였음

▶ 강연

■ 국정원 신입직원 대상 부채널분석 특강(2022.09.02.), 국가정보원

■ 양자시대와 정보보안, QIS(Quantum Information Science) (2022.09.02.) 전파통신법포럼

■ 보안 패러다임의 변화와 미래보안의 Keyword 제언 (2022.09.22.) 안랩 ISF 세미나

■ 랜섬웨어 대응 및 복호화 기술 (2022.10.01.), 국가보안기술연구소

✓ 랜섬웨어 대응과 복호화 기술을 소개하기 위한 강연

■ Crystals-Kyber와 Dilithium 최신 구현 동향 (2022.10.19., 2022.11.09.), 국가수리과학연구소.

✓ NIST PQC 알고리즘 중 Kyber와 Dilithium에 대한 최신 최적화 구현에 대한 강연

■ 스마트 공장 등 디지털 전환과정에서 겪는 보안 위협사례 및 보안 강화 전략 (2022.11.28.) KoiTa 한국산업기술진흥협회

■ 암호모듈 난수발생기 구현 및 엔트로피 테스트 (2022.12.02.), 건국대학교 SW 중심대학사업단.

✓ 암호모듈에서 사용되는 난수발생기 구현과 엔트로피 테스트에 대한 강연

■ KISA 암호팀 대상 부채널분석 교육 특강(2022.12.19.-20), 한국인터넷진흥원

■ 랜섬웨어 대응 및 복호화 기술 (2023.03.09.), 국가정보원

✓ 랜섬웨어 대응과 복호화 기술을 소개하기 위한 강연

■ 순천향대학교 정보보안학과 초청강연(2023.03.24.), 순천향대학교

■ 경량암호 (2023.04.11.), 삼성전자

✓ 경량암호의 전반적인 내용을 전달하고 Prince 블록암호 및 최신 NIST 표준 Ascon을 소개하기 위한 강연

■ 숭실대학교 AI보안연구센처 초청강연(2023.04.25.), 숭실대학교

■ 암호모듈 검증기준과 시험방법 (2023.05.15.), 건국대학교 SW 중심대학사업단

✓ 암호모듈의 검증기준과 시험방법 등에 대한 강연

■ 성신여자대학교 융합보안학과 초청강연(2023.05.24.), 성신여자대학교
■ NIST 격자기반암호 소개 (2023.07.03.), 한국전자통신연구원,
✓ NIST에서 선정한 표준화 대상 양자내성암호 알고리즘 중 격자 기반 암호에 대한 강연
■ 랜섬웨어 공격, 대응 및 복호화 기술 (2023.07.12.), 국가정보원
✓ 랜섬웨어 공격 방식, 대응 및 복호화 기술을 소개하기 위한 강연
■ 제 12호 정보보호의날 초청강연(2023.07.12.), 한국인터넷진흥원
■ 암호모듈 전문교육 기초과정 (암호모듈 검증 파트), (2023.07.20.~21.), 한국인터넷진흥원.
✓ 암호모듈이 무엇이며, 암호모듈의 검증이 어떻게 이루어 지는 가에 대한 강연
■ 랜섬웨어 대응 및 복호화 기술 (2023.08.04.), 국가보안기술연구소
✓ 랜섬웨어 대응과 복호화 기술을 소개하기 위한 강연

▶ 워크숍
■ 제5회 부채널정보분석 워크숍(2022.10.27.~2022.10.28.)
✓ 부채널정보분석 워크숍을 주관하여 개최함
■ 제6회 MobiSec 2022 워크숍 (2022.12.15.~2022.12.17.)
✓ MobiSec 2022 워크숍을 주관하여 개최함
■ 제 6회 5G보안 워크숍 (2023.4.6.~2023.4.7.)
✓ 5G보안 워크숍을 주관하여 개최함
■ 제 1회 랜섬웨어대응연구회 워크숍 (2023.5.4.)
✓ 랜섬웨어 대응 워크숍을 주관하여 개최함

6. 교육의 국제화 전략

① 교육 프로그램의 국제화 현황 및 계획

■ 유일선 교수팀은 필리핀의 최초 대학인 산카를로스 대학과 협력하여 국제 저널에 논문을 발표하였으며, 더 나아가 해당 주제를 통해 인슐린 펌프를 위한 경량의 비정상 행위탐지를 주제로 초청강연을 함
■ 유일선 교수팀은 전 세계 암호분야에서 최정상급에 위치하고 있는 오세아니아 월런공대학교와 국제 공동 연구를 수행중임
■ 유일선 교수팀은 일본의 최고 연구기관 AIST와 지속적인 연구협력을 수행해왔으며, AIST의 신성한 연구원과 국제 협력 멘토를 채결하여 지속적인 국제 협력을 수행해옴
■ 본 교육연구단은 국제적 경쟁력을 갖춘 정보보안 전문인력 양성을 위해 국제학회 참석 및 논문 발표를 독려하고 있음
■ 해당 기간 국제 저널 15건, 국제 학회 20건의 논문을 발표하였음

② 참여대학원생 국제공동연구 현황과 계획

▶ 유일선 교수팀의 참여학생 김건우는 차세대 네트워크 환경에 대응하기 위한 인증 프로토콜 설계 및 검증을 목표로 하는 국제 공동연구 '안전한 차세대 IoT 통신 환경 구축을 위한 양자내성암호 최적화 및 보안 프로토콜 적용 연구' 를 수행함
■ 본 공동연구는 국내 1개 대학(국민대학교)의 3개 연구실과, 해외 대학 (월런공대학교 Institute of Cybersecurity and Cryptology)이 참여함
■ 참여학생 김건우는 국제공동연구를 위해 2023년 2월 호주 월런공대학교에 방문하여 국제 협력 방안 논의 및 추후 연구방향에 대한 논의함

Ⅲ 연구역량 영역

□ 연구역량 대표 우수성과

▶ 자체평가 대상 기간 내 국제 저널 15건, 국내 저널 14건, 국제 학회 20건, 국내 학회 51건, 수상 24건, 강연 19건, 워크숍 4건, 국내특허(등록 7건, 출원 32건), 국제특허(출원 2건), 기술이전 4건, 소프트웨어 등록 12건, 국내 표준 3건 등의 성과를 냄

▶ 국제 저널

- “A method for decrypting data infected with Hive ransomware”, Giyoon Kim, Soram Kim, Soojin Kang, Jongsung Kim, Journal of Information Security and Applications (SCIE, I.F=5.6)
- “Quantum rebound attacks on reduced-round ARIA-based hash functions.”, Seungjun Baek, and Jongsung Kim, ETRI Journal (SCIE, I.F=1.4)
- “A study on cloud data access through browser credential migration in Windows environment”, Uk Hur, Soojin Kang, Giyoon Kim, Jongsung Kim, Forensic Science International: Digital Investigation (SCIE, I.F=2.0)
- “DIM-Based Random Number Generation Using Quantum Noise Resources”, Hansaem Wi, Seyoon Lee, and Okyeon Yi, Hindawi WCMC (SCIE, I.F=2.146)
- “Analysis of Distinguishable Security between the One-Time Password Extraction Function Family and Random Function Family”, Hyunki Kim and Okyeon Yi, MDPI Applied Science, (SCIE, I.F=2.838)
- “Rider Optimization with Deep Learning Based Image Encryption for Secure Drone Communication”, JN. Kannaiya Raja1, E. Laxmi Lydia, T Archana Acharya, K. Radhika, Eunmok Yang and Okyeon Yi, IEEE ACCESS. (SCIE, I.F=3.367)
- “Energy Optimization Techniques in Underwater Internet of Things: Issues, State-of-the-Art, and Future Directions” Delphin Raj Kesari Mary, Eunbi Ko, Dong Jin Yoon, Soo-Young Shin and Soo-Hyun Park, water 2022 (MDPI, I.F=3.4)
- “Practical Entropy Accumulation for Random Number Generators with Image Sensor-Based Quantum Noise Sources”, Youngrak Choi, Yongjin Yeom, and Ju-Sung Kang, MDPI Entropy. (SCIE, I.F=2.738)
- “End-to-End Post-Quantum Cryptography Encryption Protocol for Video Conferencing System Based on Government Public Key Infrastructure”, Yeongjae Park, Hyeondo Yoo, Jieun Ryu, Young-Rak Choi, Ju-Sung Kang, Yongjin Yeom, MDPI Applied System Innovation. (I.F=2.725)
- “APSec1.0: Innovative Security Protocol Design with Formal Security Analysis for the Artificial Pancreas System“, Jiyoon Kim, Jongmin Oh, Daehyeon Son, Hoseok Kwon, Philip Virgil Astillo and Ilsun You, Sensors (SCIE, I.F=6.3)
- “Chosen-Ciphertext Clustering Attack on CRYSTALS-KYBER Using the Side-Channel Leakage of Barrett Reduction”, Bo-Yeon Sim, Aesun Park, and Dong-Guk Han, IEEE Internet of Things Journal. (SCIE, I.F=10.238)
- “Deep-Learning Based Nonprofiling Side-Channel Attack on Mask Leakage-Free Environments Using Broadcast Operation”, Seonghyuck Lim, Hye-Won Mun, and Dong-Guk Han, IEEE ACCESS. (SCIE, I.F=3.476)
- “Optimized Implementation of PIPO Block Cipher on 32-bit ARM and RISC-V Processors “ by YoungBeom Kim and Seog Chung Seo, IEEE ACCESS (SCIE, IF=3.476)

■ “Signature Split Way for PQC-DSA Compliant with V2V Communication Standards“ by YoungBeom Kim and Seog Chung Seo, MDPI Applied Sciences (SCIE, IF=2.838)

■ “AVX512Crypto: Parallel Implementations of Korean Block Ciphers Using AVX-512“ by YongRhyel Choi, Hojin Choi, and Seog Chung Seo, IEEE ACCESS (SCIE, IF=3.476)

▶ 국내 저널

■ “Skinny-128-384 와 Romulus-N 의 SITM 공격.”, 박종현, 김종성, 정보보호학회논문지, 32권 5호

■ “iOS 환경에서의 협업 툴 아티팩트 분석 및 크리덴셜 활용 방안 연구”, 박귀은, 이민정, 강수진, 김소람, 김종성, 디지털포렌식연구 17권 2호

■ “볼륨 암호화 및 백업 응용프로그램에 대한 복호화 방안 연구”, 박귀은, 이민정, 강수진, 김기윤, 김종성, 정보보호학회논문지, 33권 3호

■ “Dm-crypt류 기반 암호화 사용 흔적 조사 및 주요 데이터 수집 절차”, 이민정, 박귀은, 강수진, 김기윤, 허욱, 김소람, 박수영, 이인수, 김종성, Contemporary Review of Forensic science 7호

■ “모바일 인스턴트 메신저에 대한 TMTO 및 GAN 모델을 활용한 안전성 분석”, 백승준, 전용진, 허욱, 김종성, 정보보호학회지 32권 6호

■ “무선랜 환경에서 양자 엔트로피 칩 기반 암호모듈을 적용한 드론 피아식별과 안전한 정보 제공 기술 제안”, 정서우, 윤승환, 이옥연, 정보보호학회논문지, 2022년 10월호

■ “수중 노이즈 상황에서의 기하학 기반 적외선 통신 채널 모델” 발카시나 스베틀라나, 황아리, 이진영, 염선호, 박수현, 전자공학회논문지 2022년 11월호

■ “NTRU를 결합한 하이브리드 세션 보호 프로토콜을 이용한 금융 오픈 API 환경의 거래 세션 안전성 강화”, 권수진, 김덕상, 박영재, 류지은, 강주성, 염용진, 정보보호학회논문지 2023년 2월호

■ “블랙박스 암호모듈에 적용 가능한 CRYSTALS-Kyber의 은닉채널 공격과 IP카메라의 잠재적 보안 위협”, 최영락, 강주성, 염용진, 한국통신학회논문지 2023년 6월호

■ “5G 특화망의 성공적 정착을 위한 보안 고려사항 연구“, 김건우, 손대현, 박훈용, 박성민, 김영수, 김환국, 김보남, 유일선, 정보기술융합공학논문지, 13권 1호, 2023

■ “레이저 오류 주입 공격 성공률 향상을 위한 전자파 및 열 정보 활용 시스템”, 문혜원, 지재덕, 한동국, 정보보호학회논문지, 32권, 5호

■ “이종 디바이스 환경에 효과적인 신규 딥러닝 기반 프로파일링 부채널 분석”, 우지은, 한동국, 정보보호학회논문지, 32권, 5호

■ “NIST PQC 공모전 동향 분석 및 표준화 대상 & Round 4 알고리즘 소개”, 김동천, 김영범, 서석충, 한국정보보호학회 학회지 2023년 4월호

■ “수중 센서 데이터의 SNS 포스팅 서비스 설계 및 구현“, 이정국, 염선호, 이진영, 박수현, 박철웅, 신수영, 한국통신학회논문지, 2023년 8월호

▶ 국제 학회

■ “A study on cloud data access through browser credential migration in Windows environment”, Uk Hur, Soojin Kang, Giyoon Kim, Jongsung Kim, DFRWS USA 2023 Conference

■ “Study on MC-Optimal S-Box Circuits”, Yongjin Jeon, Seungjun Baek, Jongsung Kim, International Conference on Platform Technology and Service (PlatCon) 2023

■ “Pros and Cons of Switching between LTE and Wi-Fi in Maritime” Shrutika Sinha, G. Pradeep Reddy, Soo-Hyun Park, International Conference on Green and Human Information Tech 2023 (ICGHIT 2023)

■ “A Survey of Deep/Machine Learning in Maritime Communications” Shrutika Sinha, Soo Yeon Kwon, Soo Hyun Park, 2023 International Conference on Ubiquitous and Future Networks (2023 ICUFN)

- “End-to-End PQC Encryption Protocol for GPKI Based Video Conferencing Systems”, Yeongjae Park, Hyeondo Yoo, Jieun Ryu, Young-Rak Choi, Ju-Sung Kang, Yongjin Yeom, 2023 IEEE 3rd International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB 2023)
- “Formal Security Analysis for TLS 1.3 using AVISPA tool“, Jongmin Oh, Daehyeon Son, Jiyoon Kim and Ilsun You, The 6th International Symposium on Mobile Internet Security (MobiSec 2022)
- “Blockchain Applied 5G Authentication and Key Agreement Evaluation“, Hoseok Kwon, Gunwoo Kim, Ajung Im, Bonam Kim and Ilsun You, The 6th International Symposium on Mobile Internet Security (MobiSec 2022)
- “A study on machine learning-based false base station detection method in 5G“, Hoonyong Park, Daehyeon Son, Gunwoo Kim and Ilsun You, The 6th International Symposium on Mobile Internet Security (MobiSec 2022)
- “Differential Fault Attack on AES using Maximum Four Bytes Faulty Ciphertexts”, Jae-Won Huh and Dong-Guk Han, The 25th Annual International Conference on Information Security and Cryptology (ICISC 2022)
- “Simulation of Vehicle-to-Vehicle Communication based on selected PQC-DSA“, YoungBeom Kim, Seog Chung Seo, The 6th International Symposium on Mobile Internet Security (MobiSec 2022)
- “AVX512Crypto : Parallel Implementation methods of Korean Block Cipher using AVX-512“, YongRyel Choi, Hojin Choi, Seog Chung Seo, The 6th International Symposium on Mobile Internet Security (MobiSec 2022)
- “High-Performance Kyber implementation on ARMv7-based ARM Neon Technology“, YoungBeom Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Accelerating Key Derivation Function on GPU Architectures“, DongCheon Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Accelerating Key Derivation Function on GPU Architectures“, DongCheon Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Efficient Implementation of Kyber on MSP430 Environment“, DongHyun Shin, YoungBeom Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Implementation of Montgomery Reduction and Butterflies for CRYSTALS-Dilithium on RISC-V“, YongRyeol Choi, YoungBeom Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “V2V-MHT Accelerated V2V Authentication Framework using Merkle Hash Tree“, YoonSun Han, YoungBeom Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Optimization Study of Parallel Implementation“, SeongJun Choi, DongCheon Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Tabling GHash in LEA-GCM and optimizing“, JaeSeok Lee, DongCheon Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)
- “Efficient implementation of multiplication reduction over NIST prime P-384 for 8-bit AVR Processor“, MinGi Kim, YoungBeom Kim and Seog Chung Seo, The 24th World Conference on Information Security Applications (WISA 2023 Poster)

▶ 국내 학회

- “NIST LWC 최종 후보 Ascon-XOF에 대한 안전성 분석”, 조세희, 백승준, 김종성, 2022 정보보호학회 동계 학술대회
- “협업 툴 TeamUp과 Agit 데이터베이스 복호화 방안 및 아티팩트 분석 연구”, 박세준, 이용진, 박지수, 박귀은, 김종성, 2022 정보보호학회 동계 학술대회
- “드론 보안 시스템의 PQC 마이그레이션에 대한 연구”, 윤혜진, 김태완, 장찬국, 이옥연, 2022 한국정보보호학회 동계학술대회
- “5G 상용망 연동을 위한 탈부착형 하드웨어 암호모듈 설계”, 김형엽, 정서우, 위한샘 이옥연, 2022 한국정보보호학회 동계학술대회
- “양자 키 분배 기술과 활용 동향”, 나태경, 이세윤, 김현기, 이옥연, 2022 한국정보보호호학회 동계학술대회
- “AHS 프로토콜을 적용한 드론 인증 시스템”, 윤혜진, 장찬국, 이재훈, 이옥연, JCCI 2023 (제 33회 통신정보 합동학술대회)
- “이동통신망과-국방광대역통합망 연동을 위한 qSIM 기반 인증의 필요성 연구”, 김형엽, 최지훈, 위한샘, 이옥연, 2023 한국정보보호호학회 하계학술대회
- “HMAC-SHA1 알고리즘을 사용하는 OTP 단말기의 평문과 키 추정 연구”, 나태경, 윤승환, 이옥연, 2023 한국정보보호호학회 하계학술대회
- “양자암호통신장비를 활용한 광대역 네트워크 운영환경에 대한 암호학적 안전성 분석 및 활용방안”, 윤혜진, 장찬국, 이재훈, 이옥연, 최지훈, 2023 한국정보보호학회 하계학술대회
- “극한지 빅데이터를 위한 남극 IoT 네트워크 엔티티”, 염선호, 윤동진, 황아리, 임용곤, 박수현, 2022 한국통신학회 추계종합학술대회
- “Key factors for Maritime Communications: Challenges and Trends”, Shrutika Sinha , ARi Hwang, Sun-Ho Yum, Jinyoung Lee, Soo-Hyun Park, The 33rd Joint Conference on Communications and Information (JCCI 2023)
- “Federated Learning-Internet of Underwater Things”, Shrutika Sinha, Soo-Hyun Park, Annual Conference of KIPS 2023 (ACK 2023)
- “이미지센서 기반 진난수생성기에 적용 가능한 효율적인 엔트로피 축적 방법”, 유현도, 최영락, 강주성, 염용진, 2022 한국통신학회 추계학술대회
- “Jetson nano 환경에서의 경량 암호학적 난수발생기 병렬 구현”, 박영재, 유현도, 강주성, 염용진, 2023 한국통신학회 동계학술대회
- “병렬 잡음원 기반 난수발생기에 적합한 엔트로피 건전성 시험”, 류지은, 유현도, 강주성, 염용진, 2023 한국통신학회 동계학술대회
- “자동화된 정형화 검증 도구를 사용한 완전 순방향 비밀성을 지원하는 TLS 1.2 프로토콜에 관한 PAL 3급의 보안성 검증 분석“, 오종민, 김지윤, 김보남, 유일선, 2023 한국정보보호학회 하계학술대회 (CISC-S’23)
- “블록체인과 머클해시트리를 이용한 데이터 무결성검증에 관한 연구 스마트 HACCP의 CCP 데이터를 중심으로“, 임아정, 김보남, 유일선, 2023 한국정보보호학회 하계학술대회 (CISC-S’23)
- “이음 5G에서 연합 학습 시스템 연구“, 박훈용, 손대현, 김건우, 유일선, 2023 한국정보보호학회 하계학술대회 (CISC-S’23)
- “5G 초기 인증단계에서 Linkability 공격에 대응 가능한 5G-AKA’ 프로토콜 취약점 분석“, 손대현, 오종민, 박영신, 유일선, 2023 한국 스마트미디어학회 종합학술대회에서 (KISM-S’23)
- “설명 가능한 XGBOOST 기반의 허위 기지국 탐지 기법“, 손대현, 박훈용, 유일선, 2023 한국정보보호학회 하계학술대회 (CISC-S’23)

- “5G 초기인증의 순방향 비밀성 지원을 위한 5G-IPAKA 보안 프로토콜 취약점 분석“, 김건우, 박훈용, 권호석, 김보남, 유일선, 2023 한국 스마트미디어학회 종합학술대회에서 (KISM-S’23)
- “경량 블록 암호 PIPO에 대한 도메인 지향 마스킹 기법”, 김연재, 한동국, 2022 한국정보보호학회 동계학술대회
- “CRYSTALS-KYBER 다항식 곱셈의 하드웨어 병렬 구현에 대한 상관 전력 분석”, 김수진, 한동국, 2022 한국정보보호학회 동계학술대회
- “SEED 마스킹의 일차 부채널 분석 취약점과 대응기법”, 김주환, 한재승, 한동국, 2022 한국정보보호학회 동계학술대회
- “하드웨어 구현 CRYSTALS-KYBER 암호문 비교 연산에 대한 부채널 분석”, 김수진, 한동국, 2022 한국정보보호학회 동계학술대회
- “DDR4 DRAM의 소프트웨어 기반 Rowhammer 기법과 전자파 오류주입 기반 Ehammer 기법에 관한 연구”, 허재원, 박형동, 여인국, 김다연, 권건우, 한동국, 2023 한국정보보호학회 하계학술대회
- “반복 학습을 통한 딥러닝 기반 비프로파일링 부채널 분석 성능을 향상 방안”, 김주환, 한동국, 2023 한국정보보호학회 하계학술대회
- “비교 연산 기반 상수시간 CDT 샘플링에 대한 단일 파형 분석”, 최건희, 허재원, 한재승, 한동국, 2023 한국정보보호학회 하계학술대회
- “노트북의 가상메모리 할당/해제를 통한 은닉 채널 형성”, 안현준, 한동국, 2023 한국정보보호학회 하계학술대회
- “Google 사 Project Vault AES-128 하드웨어 모듈에 대한 상관 전력 분석”, 기윤서, 한재승, 한동국, 2023 한국정보보호학회 하계학술대회
- “스마트폰 디스플레이 변화에 따른 은닉 채널 형성 방안”, 노혜빈, 김진웅, 한재승, 한동국, 2023 한국정보보호학회 하계학술대회
- “부채널 분석을 통한 USIM 복제 최신 동향 연구”, 최아록, 한재승, 한동국, 2023 한국정보보호학회 하계학술대회
- “KpqC 전자서명 후보 AIMer에 대한 부채널 및 오류주입 공격”, 한재승, 허재원, 이상엽, 권지훈, 한동국, 2023 한국정보보호학회 하계학술대회
- “GPU 환경에서의 해시 기반 전자 서명 SPHINCS+ FORS 최적화 방안”, 최호진, 서석충, 2022 한국정보호호학회 동계학술대회
- “MS office2013+ 다중 파일 크래킹 방안”, 최호진, 서석충, 2022 한국정보호호학회 동계학술대회
- “GPU 환경에서의 국산 해시 함수 LSH 벤치마킹”, 최성준, 최호진, 서석충, 2022 한국정보호호학회 동계학술대회
- “GPU 아키텍처 상에서의 격자 기반 양자 내성 암호 최적화 동향”, 김동천, 최호진, 서석충, 2022 한국정보호호학회 동계학술대회
- “IoT 환경에서의 격자 기반 양자 내성 암호 최적 구현 동향”, 최용렬, 김영범, 서석충, 2022 한국정보호호학회 동계학술대회
- “AVR 환경에서 표준화 대상 양자내성암호 Crystals Kyber 최적화 구현 연구”, 김영범, 서석충, 2022 한국정보호호학회 동계학술대회
- “8-bit AVR 환경에서의 PIPO, CHAM 최적화 구현”, 신동현, 김영범, 서석충, 2022 한국정보호호학회 동계학술대회
- “ARMv7 기반 Cortex-A에서의 Kyber 구현 최적화 연구“, 김영범, 서석충, 2023 한국정보보호학회 하계학술대회
- “GPU환경에서의 PBKDF2-HMAC-SHA2 최적화“, 김동천, 서석충, 2023 한국정보보호학회 하계학술대회
- “16-bit MSP430환경에서 kyber 고속화 구현“, 신동현, 김영범, 서석충, 2023 한국정보보호학회 하계학술대회

■ “RISC-V 환경에서 CRYSTALS-Dilithium의 Montgomery Reduction 및 Butterfly 연산 최적 구현“, 최용렬, 김영범, 서석충, 2023 한국정보보호학회 하계학술대회
■ “V2V-MHT: Merkle Hash Tree를 활용한 IEEE 802.11p WAVE 프로토콜 V2V 서명 검증 가속화“, 한윤선, 김영범, 서석충, 2023 한국정보보호학회 하계학술대회
■ “GPU 환경에서의 Scrypt 알고리즘 병렬 구현 최적화 연구“, 최성준, 김동천, 서석충, 2023 한국정보보호학회 하계학술대회
■ “LEA-GCM GPU상 동일 키에 따른 tabling, constant memory 사용 및 최적화“, 이재석, 김동천, 서석충, 2023 한국정보보호학회 하계학술대회
■ “8-bit AVR 환경에서 P-384 곱셈 Reduction 연산 최적화“, 김민기, 김영범, 서석충, 2023 한국정보보호학회 하계학술대회
■ 부호 기반 키체결 PALOMA의 섞음 연산 SHUFFLE에 관한 연구, 김민지, 박동현, 김동찬, 한국정보보호학회 하계학술대회, 2023 (6월)
■ Barrett Reduction과 Montgomery Reduction을 기반으로 한 RSA 비밀키 연산 고속화에 관한 연구, 김민지, 김동찬, 동계 통신학회 종합학술발표회, 2023 (2월)
■ “지능형 연안어선 운항안전 모듈 상위 설계” , 염선호, 임용곤, 이정국, 박수현, 2022 대한조선학회 추계학술대회

▶ 수상
■ 2022 국가암호 공모전 장려상 1건
■ 2022 한국정보보호학회 동계학술대회 정보보호학회장상 2건
■ 2022 한국정보호호학회 동계학술대회 우수논문상 1건
■ 2022 부채널분석연구회 한국정보보호학회장상 1건
■ 2022 MobiSec ETRI Best Student Paper 1건
■ 2022 국가 암호기술 전문인력 양성과정 최우수상 1건, 우수상 2건
■ 2022 부채널분석경진대회 부채널분석연구회 회장상 1건
■ 2022 부채널분석경진대회 한국전자통신연구원 원장상 1건
■ 2022 Mobisec ETRI Best Poster Award 1건
■ 2023 한국정보보호학회 하계학술대회 정보보호학회장상 2건
■ 2023 한국정보보호학회 하계학술대회 차세대 우수 여성과학자상 1건
■ 2023 한국정보보호학회 하계학술대회 정보보호학회장상 1건
■ 2023 한국정보호호학회 하계학술대회 우수논문상 1건
■ 2023 부채널분석경진대회 부채널분석연구회 회장상 1건
■ 2023 부채널분석경진대회 국가보안기술연구소 소장상 1건
■ 2023 한국정보보호학회 충청지부 학술대회 국가보안기술연구소장상 1건, 정보보호학회장상 1건 수상
■ 2023 부채널분석연구회 부채널분석연구회장상 1건
■ 2023 ICEIB 2023 Best conference paper award 1건
■ 2023 제6회 부채널정보분석 워크숍 차세대 정보보호 여성 과학기술인상 1건

▶ 참여교수 교육대표실적
■ 보안 강연
✓ 국정원 신입직원 대상 부채널분석 특강(2022.09.02.), 국가정보원
✓ 양자시대와 정보보안, QIS(Quantum Information Science) (2022.09.02.) 전파통신법포럼
✓ 보안 패러다임의 변화와 미래보안의 Keyword 제언 (2022.09.22.) 안랩 ISF 세미나

✓ 랜섬웨어 대응 및 복호화 기술(2022.10.01.), 국가보안기술연구소
✓ Crystals-Kyber와 Dilithium 최신 구현 동향, 국가수리과학연구소, 2022.10.19., 2022.11.09.
✓ 스마트 공장 등 디지털 전환과정에서 겪는 보안 위협사례 및 보안 강화 전략 (2022.11.28.) KoiTa 한국산업기술진흥협회
✓ 암호모듈 난수발생기 구현 및 엔트로피 테스트, 건국대학교 SW 중심대학사업단, 2022.12.02.
✓ KISA 암호팀 대상 부채널분석 교육 특강(2022.12.19.-20), 한국인터넷진흥원
✓ 랜섬웨어 대응 및 복호화 기술(2023.03.09.), 국가정보원
✓ 순천향대학교 정보보안학과 초청강연(2023.03.24.), 순천향대학교
✓ 경량암호(2023.04.11.), 삼성전자
✓ 숭실대학교 AI보안연구센처 초청강연(2023.04.25.), 숭실대학교
✓ 암호모듈 검증기준과 시험방법, 건국대학교 SW 중심대학사업단, 2023.05.15.
✓ 성신여자대학교 융합보안학과 초청강연(2023.05.24.), 성신여자대학교
✓ NIST 격자기반암호 소개, 한국전자통신연구원, 2023.07.03.
✓ 랜섬웨어 공격, 대응 및 복호화 기술(2023.07.12.), 국가정보원
✓ 제 12호 정보보호의날 초청강연(2023.07.12.), 한국인터넷진흥원
✓ 암호모듈 전문교육 기초과정 (암호모듈 검증 파트), 한국인터넷진흥원, 2023.07.20.~21
✓ 랜섬웨어 대응 및 복호화 기술(2023.08.04.) 국가보안기술연구소

■ 워크숍
✓ 제 5회 부채널정보분석 워크숍 (2022.10.27.~2022.10.28.)
• 부채널정보분석 워크숍을 주관하여 개최함
✓ 제 6회 MobiSec 2022 워크숍 (2022.12.15.~2022.12.17.)
• MobiSec 2022 워크숍을 주관하여 개최함
✓ 제 6회 5G보안 워크숍 (2023.4.6.~2023.4.7.)
• 5G보안 워크숍을 주관하여 개최함
✓ 제 1회 랜섬웨어대응연구회 워크숍 (2023.5.4.)
• 랜섬웨어 대응 워크숍을 주관하여 개최함

▶ 국내특허
[등록]
■ 양자보안 통신장치 통합형 원방감시 제어 시스템 및 방법 (등록)
■ 5G SIDF 암호처리장치 및 그 방법 (등록)
■ 인공신경망을 이용한 RSA 암호에 대한 부채널 분석 방법 및 장치 (등록)
■ 무선통신 기기 및 이의 동작방법 (등록)
■ 수중 사물 인터넷의 온톨로지 기반 통신 매체 선택 방법 및 이를 수행하는 수중 통신 장치(등록)
■ 수중 네트워크 관리 시스템 및 그의 동작 방법(등록)
■ 부채널 공격에 안전한 행렬 곱 연산을 수행하기 위한 장치 및 방법(등록)
[출원]
■ 스마트기기용 양자보안 통신 제공장치 및 방법
■ 양자암호 기반의 수하물 식별 장치 및 방법
■ 양자암호 기반의 영상 식별 장치 및 방법
■ 무인 비행체 및 이의 비행 경로 설정 방법
■ 무인 비행체 및 이의 센서 장치 구동 제어 방법, 및 통신 시스템

■ 무인 비행체를 통한 센서 상태 확인 방법
■ 지상 네트워크 및 수중 네트워크 간 주소 상호 운용성을 위한 게이트웨이 장치 및 그 동작 방법
■ 고 지연의 Tum-IoT 네트워크에서 다중 통신 스펙트럼 기반 서비스 요청 추론 기법
■ 수중 네트워크에서의 트랜잭션 동작
■ 수중 무선 통신 시스템을 이용한 수중 무선 네트워크 구성 방법
■ 다중-모드 수중통신 장치
■ 수중 네트워크 관리 시스템 및 그의 동작 방법
■ 이미지 센서 기반 엔트로피 축적 장치 및 방법, 이를 이용한 진난수생성기
■ 모드버스 오류 처리 장치 및 방법
■ 군집화 알고리즘을 이용한 블록암호 CTR 운영모드 부채널 분석 방법 및 장치
■ 비지도 도메인 적응을 이용한 프로파일링 부채널 분석 방법 및 장치
■ 블록암호에 대한 4바이트 이하 오류 기반의 차분 오류 분석 방법 및 장치
■ 경량 블록 암호 PIPO에 대한 Domain-Oriented Masking 적용 방법
■ 스마트폰 소리 재생 시 누설되는 전자기파를 이용한 은닉 채널
■ 가상메모리 할당 및 해제를 이용한 은닉채널 형성 방법 및 장치
■ 경량 블록 암호 PIPO에 대한 Threshold Implementation 적용 방법
■ 크리스탈 카이버 연산 장치에 대한 상관 전력 분석 방법 및 장치
■ 경량 블록 암호 PIPO에 대한 Re-Consolidating Masking 적용 방법
■ 인공 신경망의 오분류 유도 방법 및 파라미터 복원 방법과 이를 위한 장치
■ 부채널 공격을 방지하기 위한 암호문 비교 장치 및 방법
■ 다항식 연산 기반의 보안 알고리즘의 연산 처리 방법, 그리고 이를 구현하기 위한 장치
■ 부채널 공격을 방지하기 위한 암호문 비교 장치 및 방법
■ 이미지 센서 기반 엔트로피 축적 장치 및 방법, 이를 이용한 진난수생성기
■ 모드버스 오류 처리 장치 및 방법
■ 마르코프 패스워드 테이블을 이용한 다중 파일 패스워드 크래킹 장치 및 방법
■ 인퓨전 펌프를 위한 머드 기반의 네트워크 관리 방법 및 장치
■ BMANF를 활용한 그룹 키 기반 프로토콜 수행 방법 및 BMANF 노드

▶ 국제특허
■ DPAPI 기반의 데이터 재생성을 통한 클라우드 데이터 획득 장치 및 방법 (출원)
■ 양자 엔트로피 기반 일회용 양자 비밀번호 생성 장치 및 방법 (출원)

▶ 기술이전
■ 양자키 유도 함수를 활용한 암호키 생성 방법 및 이를 수행하는 암호키 생성 장치
■ 화이트박스 암호화 기술
■ 양자내성암호 알고리즘 Kyber의 고속구현 기술 이전
■ 심리스 DTN 프로토콜을 사용한 수중통신 장치 및 그 통신방법

▶ 소프트웨어 등록
■ 경량 데이터베이스(SQLite)에 대한 비밀번호 검증 및 복호화 프로그램 등록
■ 드론 제어 데이터 관리를 위한 Replaying(재생) FDR(비행데이터기록) 장치용 프로그램 등록
■ 공간정보 기반 식별용 에이전트 모듈(리눅스) 등록
■ 암호모듈 기반 식별 체계용 시험 프로그램(윈도우) 등록

■ Curve25519를 이용한 Kyber의 SETUP 프로그램 등록
■ NTRU(엔트루)가 적용된 모드버스 TLS(티엘에스) 통신 프로그램 등록
■ 측정 보고서(Measurement Report) 학습 데이터 전처리기 프로그램
■ 허위기지국 비정상 데이터 생성기
■ 경량 블록암호 피포(PIPO)의 안전한 하드웨어 마스킹 코드
■ 신경망 활성 함수 소프트맥스(Softmax) 입력 대상 오분류를 유도하기 위한 비트 반전 시뮬레이션 알고리즘
■ CUDA C 기반 고정 길이 파라미터에 대한 PBKDF2-HMAC-SHA Family 고속 생성 방안
■ 수중 SNS(소셜 네트워크 서비스)를 위한 S-DTN(심리스 전공지연 감내 네트워크) 기반 이종망 데이터 전송 중계 프로그램

▶ 국제 표준(해당없음)

▶ 국내 표준
■ TTA 정보통신표준화위원회 신규 표준화 과제 “양자키분배 후처리에 대한 시험방법” 채택
■ 사물인터넷융합포럼 표준화 제안, “보안 강화된 블록암호에 대한 결합 상관 부채널 분석 기술 요구사항 및 절차”, IoTFS-0250.
■ 사물인터넷융합포럼 표준화 제안, “전압 전자파 이종 오류원 기반 오류 주입 분석 기술 요구사항 및 절차”, IoTFS-0251.

▶ 연구비 수주실적 표(자체평가 대상 기간 2022.9.1.~2023.8.31. 연구비 입금일 기준) (단위: 원)

총 58건			합계	9,556,860,800	5,942,281,771
연번	과제번호	연구과제명	과제기간	총연구비	수입금액
1	A2021-0578	딥러닝을 이용한 RISC-V 기반 하드웨어 보안성 검증 도구 개발(2차년도)	2021-12-01~2022-11-30	100,000,000	28,812,966
2	A2021-0586	(MC24) 비침입·준침입 공격 및 분석기법 연구	2021-08-27~2024-05-31	670,251,000	280,828,545
3	A2021-0587	(MC31) 의사난수 생성기술 및 암호 알고리즘 식별기술 연구	2021-08-27~2024-05-31	456,163,800	104,749,680
4	A2021-0588	(MC33) 블록암호/해쉬함수 분석기술 연구 및 분석도구 개발	2021-08-27~2024-05-31	549,723,000	141,836,352
5	A2022-0172	“국방 KCMVP 검증필 OO모듈“을 납품 용역	2022-03-11~2023-12-31	250,000,000	125,000,000
6	A2022-0196	dm-crypt류 기반 암호화 기법 연구	2022-03-17~2022-11-25	130,000,000	48,619,540
7	A2022-0255	랜섬웨어 동향 및 암호기능 상세분석 용역	2022-04-06~2022-11-30	85,500,000	17,100,000
8	A2022-0258	AM-01장치 전압 및 전자파 글리칭 기반 보안성 분석 도구 제작	2022-03-14~2022-08-31	47,500,000	23,750,000
9	A2022-0309	JRF	2022-05-16~2022-12-15	158,775,000	85,595,000

10	A2022-0467	드론용 암호장비 연동 시험 자문 용역	2022-06-01~ 2022-08-31	55,000,000	16,500,000
11	A2022-0469	eSIM 플랫폼용 암호 알고리즘 포팅 및 개발환경 구축	2022-08-01~ 2022-11-30	51,600,000	25,800,000
12	A2022-0474	다중매체 다중대역 수중 네트워크 기술 표준개발	2022-07-01~ 2022-12-31	60,000,000	80,846,567
13	A2022-0525	공군본부 강의 용역	2022-09-19~ 2022-09-23	10,100,000	10,100,000
14	A2022-0547	양자암호통신 시범인프라 구축운영시범망 구축을 위한 5G 기반 KCMVP적용 IoT암호화	2022-09-05~ 2022-12-15	55,000,000	44,000,000
15	A2022-0552	V 어플리케이션 보안 강도 검증 도구 제작	2022-10-11~ 2022-11-30	38,000,000	38,000,000
16	A2022-0617	안전한 차세대 IoT 통신 환경 구축을 위한 양자내성암호 최적화 및 보안 프로토콜 적용 연구	2022-11-01~ 2023-04-30	250,000,000	250,000,000
17	A2023-0029	GPU/ASIC 기반 암호알고리즘 고속화 설계 및 구현 기술개발(3차년도)	2023-01-01~ 2023-12-31	330,000,000	264,000,000
18	A2023-0044	국방정보통신망-상용망(5G) 연동을 위한 보안 기술개발(2/4)	2023-01-01~ 2023-12-31	250,000,000	250,000,000
19	A2023-0060	양자컴퓨팅 환경에 대비한 분산자원 플랫폼 관리용 암호 기술 연구(1/1-2단계)	2023-02-24~ 2024-02-23	90,000,000	90,000,000
20	A2023-0072	무기체계 코드 안티탬퍼링 기술 개발 용역(1/4)	2023-01-19~ 2023-12-31	660,000,000	660,000,000
21	A2023-0077	제1형 당뇨환자의 안전하고 신뢰성 있는 치료를 위한 인슐린 펌프 보안 내재화 연구: 비정상행위 탐지 기술 및 보안 프로토콜을 중심으로(5/5)	2023-03-01~ 2023-05-31	32,500,000	32,500,000
22	A2023-0087	(2단계)고신뢰 온-디바이스 딥러닝 가속기 설계를 위한물리채널 기반 취약점 검증 및 대응기술 개발(1/2)	2023-01-01~ 2023-12-31	139,000,000	81,000,000
23	A2023-0090	부호기반 암호의 안전성 및 효율성에 관한 연구(3/3)	2023-03-01~ 2024-02-29	67,791,000	67,791,000
24	A2023-0109	(2단계)국가공공 정보시스템 안전성 및 활용성 제고를 위한 차세대 암호체계 개발(1/2)	2023-01-01~ 2023-12-31	210,000,000	165,600,000
25	A2023-0115	차세대 양자내성 공개키 암호알고리즘에 대한 SW/HW 구현최적화 및 구현적합성 연구(2/5)	2023-03-01~ 2024-02-29	131,246,000	131,246,000
26	A2023-0142	단안 영상 기반 사용자 중심 3차원 인터랙션을 위한 경량 비전 기술 연구(3/3)	2023-03-01~ 2024-02-29	95,818,000	95,818,000
27	A2023-0162	5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발	2023-01-01~ 2023-12-31	100,000,000	72,000,000
28	A2023-0164	상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구(3/4)	2023-01-01~ 2023-12-31	150,000,000	108,000,000
29	A2023-0166	(ICT 전문연구실) SCR-Friendly 대칭키 암	2023-01-01~	340,000,000	100,000,000

		호 및 응용 모드 개발(2단계-3차년도)	2023-12-31		
30	A2023-0167	5G+ 기반 6G 이동통신 정보보안 기술 연구(4/4)	2023-01-01~ 2023-12-31	363,000,000	280,000,000
31	A2023-0170	다중매체 다중대역 수중 네트워크 기술 표준개발	2023-01-01~ 2023-12-31	120,000,000	65,450,121
32	A2023-0195	양자기반 암호학적 난수 생성 기술 개발	2023-01-01~ 2023-12-31	80,000,000	80,000,000
33	A2023-0294	PC기반 인스턴트 메신저 데이터 획득, 분석, 복호화 기법 연구	2023-04-21~ 2023-11-24	100,000,000	78,574,000
34	A2023-0297	다종 플랫폼 대상 안티포렌식 소프트웨어 정보 은닉 방식 연구	2023-04-01~ 2023-10-31	70,000,000	70,000,000
35	A2023-0298	하드웨어 기반 양자내성 표준 서명 알고리즘의 안전성 분석 및 대응기술 연구	2023-04-01~ 2023-10-31	50,000,000	50,000,000
36	A2023-0299	국외 표준 양자내성암호 구현적절성 검증 기법 연구	2023-04-01~ 2023-12-31	90,000,000	90,000,000
37	A2023-0310	랜섬웨어 동향 및 암호기능 상세분석	2023-04-28~ 2023-11-30	85,500,000	68,400,000
38	A2023-0331	사이버폭력 해결을 위한 모바일 포렌식 기술 및 피해 감지·대응 기술 개발	2023-04-01~ 2023-12-31	75,000,000	75,000,000
39	A2023-0332	메모리 접근에 의해 발생하는 전자파를 이용한 은닉채널 기능 검증 및 시험	2023-05-12~ 2023-09-15	50,050,000	25,025,000
40	A2023-0348	안전한 차세대 IoT 통신 환경 구축을 위한 양자내성암호 최적화 및 보안 프로토콜 적용 연구	2023-05-01~ 2024-04-30	500,000,000	242,000,000
41	A2023-0356	농산물 산지 유통센터(APC) 내 이음5G망 구축을 위한 보안 기술 연구	2023-05-25~ 2023-11-25	36,000,000	28,800,000
42	A2023-0373	코드 역공학 방지 기술 시험 개발환경 구축	2023-06-08~ 2023-11-30	318,500,000	159,250,000
43	B2022-0005	안전한 초연결사회를 위한 문제해결형 정보보안 교육연구단(3/8)	2022-03-01~ 2023-02-28	566,160,000	173,577,000
44	B2023-0005	안전한 초연결사회를 위한 문제해결형 정보보안 교육연구단(4/8)	2023-03-01~ 2024-02-29	700,783,000	514,542,000
45	G2022-0020	국방 IoT용 양자난수 암호모듈 상용화 자문 용역	2022-09-01~ 2023-08-31	44,000,000	33,000,000
46	S2022-0051	선박입출항실적통계 데이터 분석을 통한 미래 선박 이동량 예측 분석 모델	2022-06-01~ 2023-03-31	26,400,000	7,920,000
47	S2022-0052	화이트박스암호 기반 키보호 메커니즘 개발	2022-05-16~ 2022-08-15	22,000,000	11,000,000
48	S2022-0091	DRAM Security 기술 연구 클러스트 산학	2022-07-01~ 2023-06-30	88,000,000	26,400,000
49	S2022-0099	DSTA대상 PQC 부채널내성기술 시연	2022-08-09~ 2022-11-30	33,000,000	33,000,000
50	S2022-0100	PQC 부채널내성 암호기술 확보	2022-08-01~ 2023-05-31	88,000,000	88,000,000

51	S2022-0113	PQC 부채널분석 기술 확보	2022-10-17~ 2022-11-18	35,000,000	35,000,000
52	S2023-0016	화이트박스 암호 설계/분석 기술 공동연구	2023-03-01~ 2024-02-28	16,500,000	8,250,000
53	S2023-0019	경량 PQC 최적 구현	2023-01-26~ 2023-07-31	88,000,000	88,000,000
54	S2023-0029	암호모듈검증시험(K-CMVP)인증 용역	2023-03-15~ 2023-11-30	50,000,000	22,000,000
55	S2023-0037	PQC 대상 NTT HW 구현 최적화	2023-03-01~ 2023-12-31	77,000,000	23,100,000
56	S2023-0042	2023년 국민대학교-펜타시큐리티시스템 정보보안 산학협력 프로그램	2023-04-01~ 2024-02-29	165,000,000	82,500,000
57	S2023-0048	모바일 환경에서 적용 가능한 화이트박스 암호 설계/분석 기술 공동연구	2023-05-01~ 2023-08-31	22,000,000	11,000,000
58	S2023-0068	사이버보안 및 정보보호 기술 교육 용역	2023-06-01~ 2023-12-31	33,000,000	33,000,000

1. 참여교수 연구역량

1.1 국내 및 해외기관 연구비 수주 실적

<표 3-1> 최근 1년간(2022.9.1.-2023.8.31.) 이공계열 참여교수 1인당 정부, 산업체, 해외기관 등 연구비 수주 실적

항 목	수주액(단위: 천원)		
	3년간(2017.1.1.-2019.12.31.) 실적 (선정평가 보고서 작성내용)	최근 1년간(2022.9.1.～2023.8.31.) 실적	비고
정부 연구비 수주 총 입금액	9,858,736	5,440,112	
산업체(국내) 연구비 수주 총 입금액	763,070	502,170	
해외기관 연구비 수주 총 (환산)입금액	0	0	
이공사회계열 참여교수 수	10	11	
1인당 총 연구비 수주액	1,062,180	540,207	

1.2 연구업적물

① 참여교수 연구업적물의 우수성

▶ 국제 저널

■ A method for decrypting data infected with Hive ransomware

✓ 국내·외에 다수의 피해를 입힌 Hive 랜섬웨어에 대한 복호화 방법을 개발하여 복호화 도구를 제작함

■ Quantum rebound attacks on reduced-round ARIA-based hash functions

✓ ARIA 블록암호를 기반으로 하는 해시함수의 양자 보안성을 분석하고, 이전 관련 연구의 오류를 제시함

■ A study on cloud data access through browser credential migration in Windows environment
  ✓ Windows 환경의 다양한 브라우저에서 사용자 크리덴셜을 사용한 클라우드 데이터 획득 방법을 제시함
■ DIM-based Random Number Generation Using Quantum Noise Resources
  ✓ 기존의 UAS 트래픽 관리(UTM)에 사용되는 DIM의 난수 생성의 한계를 도출하고, 양자 잡음 자원을 이용하여 DIM에서 난수를 생성하는 방법을 제안하였음
■ Analysis of Distinguishable Security between the One-Time Password Extraction Function Family and Random Function Family
  ✓ OTP 비트열 추출 과정에서 사용되는 함수를 구별 가능한 보안성 측면에서 포함하는 함수 패밀리를 분석함으로써 OTP 추출 함수 패밀리는 랜덤 함수 패밀리에 비해 구별 가능한 보안성 측면에서 취약하다는 결론을 내림
■ Rider Optimization with Deep Learning Based Image Encryption for Secure Drone Communication
  ✓ 긴급 모니터링 시나리오에서 효과적인 보안 통신 및 분류 프로세스를 위해 이미지 암호화 기반 보안 드론 통신(ODLE-SDC) 기법을 통한 최적의 딥러닝을 제안하였음
■ "Energy Optimization Techniques in Underwater Internet of Things: Issues, State-of-the-Art, and Future Directions"
  ✓ 해양에서의 수중 사물 인터넷(UIoT)은 다양한 응용 분야에서 중요하며, 통신에는 음향, IR, VL, RF, M.I 등이 사용됩니다. 그러나 각 통신 매체는 한계가 있고, UIoT 디바이스의 에너지 소비 문제를 해결하기 위한 연구와 에너지 최적화 기술이 중요하기 때문에 UIoT 네트워크의 에너지 최적화 이슈와 향후 개선 방향에 대해 제시함
■ Practical Entropy Accumulation for Random Number Generators with Image Sensor-Based Quantum Noise Sources
  ✓ 암호 시스템의 기반이 되는 난수에 관한 연구로 이미지 센서 기반 양자 난수 발생기에 대한 엔트로피 축적 방법을 제안함
■ End-to-End Post-Quantum Cryptography Encryption Protocol for Video Conferencing System Based on Government Public Key Infrastructure
  ✓ End-to-End 통신에서 GPKI를 활용하는 화상회의 보안 시스템 구축 방식을 제안함
■ Session Management for Security Systems in 5G Standalone Network
  ✓ 기존 NFGW에서는 저렴하지 않지만 5G SA의 보안 시스템에는 반드시 유용한 사용자를 위한 효율적인 세션 관리 기법
■ Towards Intelligent Attack Detection Using DNA Computing
  ✓ DNA 컴퓨팅(ADDC) 기반 지능형 공격 탐지를 제안함
■ Smart Collaborative Evolvement for Virtual Group Creation in Customized Industrial IoT
  ✓ VGC(Virtual Group Creation)를 위한 SCE(Smart Collaborative Evolvement) 방식을 제안함
■ Blockchain-Based Privacy Preservation Scheme for Misbehavior Detection in Lightweight IoMT Devices
  ✓ 최근 블록체인과 연합 학습(FL)의 강력한 통합을 기반으로 경량 IoMT 장치, 특히 인공 췌장 시스템(APS)에서 안전한 오작동 감지를 위한 효율적인 개인정보 보호 프레임워크를 제안
■ A Smart Retransmission Mechanism for Ultra-Reliable Applications in Industrial Wireless Networks
  ✓ 신뢰성 요구 사항을 지능적으로 충족하기 위해 적시에 데이터를 재전송할 수 있는 주문형 서비스 보호(OSP) 메커니즘을 제안
■ APSec1.0: Innovative Security Protocol Design with Formal Security Analysis for the Artificial Pancreas System
  ✓ 컨텍스트 협상이 리소스 친화적이며 프로토콜이 긴급 상황에 탄력적인 APS 환경을 위한 보안 프

로토콜을 제안

- Towards secure asynchronous messaging with forward secrecy and mutual authentication
  - ✓ 블룸 필터 암호화와 신원 기반 매치메이킹 암호화를 결합하여 천공 가능한 신원 기반 매치메이킹 키 캡슐화 메커니즘이라는 새로운 암호화 기본 요소를 제시하고 구체적인 구성도 제안
- An Enhanced Deep Learning Neural Network for the Detection and Identification of Android Malware
  - ✓ AMDI-Droid라는 악성 앱으로부터 Android 장치를 보호하기 위해 효과적으로 개선된 심층 신경망을 제시함
- Exploring Reliable Decentralized Networks with Smart Collaborative Theory
  - ✓ 스마트 협업 이론을 기반으로 콘텐츠 개인 정보 보호 기능을 향상시키기 위해 RDN(Reliable Decentralized Networks) 시스템을 제안함
- Chosen-Ciphertext Clustering Attack on CRYSTALS-KYBER Using the Side-Channel Leakage of Barrett Reduction
  - ✓ NIST PQC KYBER의 Barrett reduction에서 발생하는 부채널 누출을 이용하여 공격하는 선택 암호문 기반 클러스터링 공격을 제안함
- Deep-Learning Based Nonprofiling Side-Channel Attack on Mask Leakage-Free Environments Using Broadcast Operation
  - ✓ 딥러닝 및 broadcast 연산을 기반으로 키 분석 성공률이 높은 비프로파일링 부채널 분석을 제안함
- Optimized Implementation of PIPO Block Cipher on 32-bit ARM and RISC-V
  - ✓ 32-bit 환경인 ARM과 RISC-V 환경에서 블록암호 PIPO에 대한 최적화 구현 방안을 제안하였음.
- ignature Split Way for PQC-DSA Compliant with V2V Communication Standards
  - ✓ PQC-DSA를 분할하여 V2V 프로토콜에서 효율적으로 연산이 가능한 최적화 방안을 제안하였음.
- AVX512Crypto: Parallel Implementations of Korean Block Ciphers Using AVX-512
  - ✓ AVX512 환경에서 다양한 국내 블록암호 최적화 방안을 제안하였음.

▶ 국내 저널

- Skinny-128-384 와 Romulus-N 의 SITM 공격
  - ✓ 부채널 정보를 이용하여 Skinny128-384와 Romulus-N 블록암호에 대한 새로운 SITM 공격을 제안함
- iOS 환경에서의 협업 툴 아티팩트 분석 및 크리덴셜 활용 방안 연구
  - ✓ iOS 환경에서 사용되는 협업 툴의 아티팩트를 분석하고, 이러한 아티팩트를 크리덴셜 관점에서 활용하는 방안을 제시함
- 볼륨 암호화 및 백업 응용프로그램에 대한 복호화 방안 연구
  - ✓ 볼륨 암호화 및 백업 기능을 제공하는 Cryptomator와 Norton Ghost를 분석하고, 데이터 복호화 방안을 제시함
- Dm-crypt류 기반 암호화 사용 흔적 조사 및 주요 데이터 수집 절차
  - ✓ Windows 환경에서 dm-crypt류 기반 암호화 도구의 사용 흔적 파악 방법과 이를 토대로 대상 암호화 도구를 특징짓는 방법을 제시함
- 모바일 인스턴트 메신저에 대한 TMTO 및 GAN 모델을 활용한 안전성 분석
  - ✓ 10종의 모바일 인스턴트 메신저에 대한 TMTO 및 GAN 모델을 활용한 안전성 분석을 제시함
- 무선랜 환경에서 양자 엔트로피 칩 기반 암호모듈을 적용한 드론 피아식별과 안전한 정보 제공 기술 제안
  - ✓ 드론 시스템중드론의군집 비행 시스템과 이를 위한 이음 5G와 같은 이동통신 특화망에서 무선랜과 양자 엔트로피 기반 난수발생기를 탑재한 암호모듈을 활용하여 군집 비행 드론 간 피아식별 및 안전한 정보 제공 기술 방법을 제안하고, 구현에 참고할수 있는 테스트 벡터를 제공함
- 수중 노이즈 상황에서의 기하학 기반 적외선 통신 채널 모델

- ✓ Beer-Lambert의 감쇠 법칙과 기하학적 광학을 이용하여 수중 bubble에 대한 수리적 채널 모델링 기법으로 거리, 전력 및 수중 유형에 따른 광통신의 성능을 시뮬레이션으로 분석함

■ NTRU를 결합한 하이브리드 세션 보호 프로토콜을 이용한 금융 오픈 API 환경의 거래 세션 안전성 강화

- ✓ NIST 양자내성암호 공모전 3라운드 후보 알고리즘이었던 NTRU를 사용하는 하이브리드 세션 키 교환 기법을 설계하고 성능을 분석함

■ 블랙박스 암호모듈에 적용 가능한 CRYSTALS-Kyber의 은닉채널 공격과 IP카메라의 잠재적 보안 위협

- ✓ 내부 구조가 투명하게 공개되지 않은 완제품 형태의 카메라에 대한 은닉채널 존재 가능성을 제시하고 이에 대응하기 위한 기법을 제시함

■ 레이저 오류 주입 공격 성공률 향상을 위한 전자파 및 열 정보 활용 시스템

- ✓ 레이저 오류주입 공격의 성공률을 향상시키기 위해 분석 대상 장비가 동작하는 동안 발생하는 전자파 및 열 정보를 이용한 시스템을 제안함

■ 이종 디바이스 환경에 효과적인 신규 딥러닝 기반 프로파일링 부채널 분석

- ✓ 학습 대상 장치와 공격 대상 장치가 다른 종류인 환경에서 효과적인 딥러닝 기반 프로파일링 부채널 분석 기법을 제안함

■ “수중 센서 데이터의 SNS 포스팅 서비스 설계 및 구현“

- ✓ 수중 통신을 사용하여 스쿠버 다이빙 중 얻은 센서 데이터를 서버에 전달 후 원하는 데이터만 선택하여 SNS 환경에 업로드할 수 있는 시스템을 설계 및 구현함. 본 시스템을 구현하기 위해 수중 통신 시스템과 이를 운용하기 위한 하드웨어를 구현하였으며 수면 게이트웨이를 구현하여 수중과 지상의 이종망 통신 시스템을 구축함

▶ 국제 학회

■ A study on cloud data access through browser credential migration in Windows environment

- ✓ 사용자 크리덴셜을 활용하여 클라우드 데이터 획득 방법을 Windows 환경의 다양한 브라우저에서 실험하고 연구 결과를 소개함

■ Study on MC-Optimal S-Box Circuits

- ✓ 암호학적으로 안전한 S-box를 구성하기 위해 고려해야 하는 MC를 분석하고, 최적의 MC를 갖는 S-box를 찾는 방법을 제안함

■ Pros and Cons of Switching between LTE and Wi-Fi in Maritime

- ✓ 열악한 수중 환경에서 대량의 데이터를 수집하고 중앙 서버로 전송하기 어려울 때, Federated Learning(FL)은 디바이스 자체에서 학습을 진행하고 중앙 서버로 데이터를 전송하지 않고 모델을 업데이트할 수 있는 효과적인 방법을 제시함

■ A Survey of Deep/Machine Learning in Maritime Communications

- ✓ 해양 네트워크 토폴로지에서 머신/딥러닝을 활용한 다양한 해양 IoT 및 광대역 서비스 사용 사례에 대해 살펴보았습니다. 또한, 엣지 컴퓨팅, 빅 데이터 분석, 그리고 사물인터넷(IoT)을 융합하여 이러한 시스템의 성능을 향상시키는 방법에 대해 기술함

■ End-to-End PQC Encryption Protocol for GPKI Based Video Conferencing Systems

- ✓ 화상 회의 시스템의 End-to-End 프로토콜에 양자내성암호를 적용하는 과정에 GPKI를 접목하는 방법을 제안함

■ Differential Fault Attack on AES using Maximum Four Bytes Faulty Ciphertexts

- ✓ AES 암호 알고리즘의 9라운드에서 최대 네 바이트에 오류가 주입되었을 때의 암호문을 통해 비밀키를 복구하는 차분 오류 공격을 제시함

■ Simulation of Vehicle-to-Vehicle Communication based on selected PQC-DSA

✓ 표준화를 위한 최적화된 PQC-DSA를 기반으로 V2Verifier의 서명 생성 및 검증방법을 제안하였음.

■ AVX512Crypto : Parallel Implementation methods of Korean Block Cipher using AVX-512
✓ AVX512 환경에서 다양한 국내 블록암호 최적화 방안을 제안하였음.

■ AVX512Crypto: Parallel Implementations of Korean Block Ciphers Using AVX-512
✓ AVX-512를 이용한 한국 블록 암호 병렬 구현 기법을 제안하였음.

■ High-Performance Kyber implementation on ARMv7-based ARM Neon Technology
✓ ARMv7 기반 ARM Neon 기술에서의 고성능 Kyber 구현 기법을 제안하였음.

■ Accelerating Key Derivation Function on GPU Architectures
✓ GPU Architectures에서의 Key Derivation Function 가속화 기법을 제안하였음.

■ Efficient Implementation of Kyber on MSP430 Environment
✓ MSP430 환경에서의 Kyber 주요 컴포넌트에 대한 최적화 기법을 제안하였음.

■ Implementation of Montgomery Reduction and Butterflies for CRYSTALS-Dilithium on RISC-V
✓ RISC-V 환경에서 CRYSTALS-Dilithium의 Montgomery Reduction 및 Butterflies 구현 기법을 제안하였음.

■ V2V-MHT Accelerated V2V Authentication Framework using Merkle Hash Tree
✓ Merkle Hash Tree (MHT)를 활용한 V2V-MHT 프로토콜을 제안하였음.

■ Optimization Study of Parallel Implementation
✓ 병렬 구현 아키텍처 들과 최적화 기법을 제안하였음.

■ Tabling GHash in LEA-GCM and optimizing
✓ LEA-GCM에서의 GHash Tabling 최적화 기법을 제안하였음.

■ Efficient implementation of multiplication reduction over NIST prime P-384 for 8-bit AVR Processor
✓ 8-비트 AVR 프로세서를 위한 NIST 소수 P-384에서의 multiplication reduction 최적화 기법을 제안하였음.

▶ 국내 학회

■ NIST LWC 최종 후보 Ascon-XOF에 대한 안전성 분석
✓ 미국 NIST LWC의 최종후보 Ascon-XOF에 대한 충돌쌍 공격을 분석하고, MILP solver를 이용하여 공격에 효율적으로 적용할 수 있는 차분 경로를 제안함

■ 협업 툴 TeamUp과 Agit 데이터베이스 복호화 방안 및 아티팩트 분석 연구
✓ 사용자 데이터를 암호화하여 저장하는 협업 툴인 TeamUp과 Agit를 분석하여 데이터를 복호화하고 아티팩트 분석을 수행함

■ 극한지 빅데이터를 위한 남극 IoT 네트워크 엔티티
✓ 남극에서 활동하는 인구가 겪는 극심한 정보격차 문제를 극복하기 위해 남극 IoT 네트워크 아키텍처를 개발하여 '극한지 빅데이터' 구축의 실현 가능성을 제시함

■ Key factors for Maritime Communications: Challenges and Trends
✓ 해상 시스템에서 주파수 및 채널 변경을 위해 수동 절차에 의존하는 전통적인 방식과 머신러닝 기반 전환의 장단점을 비교하며, 머신러닝을 활용하여 시스템을 개선 방안을 제시함

■ Federated Learning-Internet of Underwater Things
✓ 해상에서 생성되는 다양한 수중 디바이스의 데이터 양이 증가함에 따라, 효과적인 데이터 전송을 제공하는 해상 통신의 최신 동향과 연구에 대해 기술함

■ 이미지센서 기반 진난수생성기에 적용 가능한 효율적인 엔트로피 축적 방법
✓ 이미지 센서 기반 양자난수생성기의 엔트로피 축적 방법을 설계하고 성능을 분석하여 후처리 알고리즘의 활용 가능성을 보임

■ Jetson nano 환경에서의 경량 암호학적 난수발생기 병렬 구현
✓ 경량 대칭 블록암호 CHAM을 활용한 난수발생기를 병렬화하여 GPU가 탑재된 임베디드 보드에서의 성능

을 평가하고 표준 AES 알고리즘을 활용할 때보다 효율적임을 보임

■ 병렬 잡음원 기반 난수발생기에 적합한 엔트로피 건전성 시험
  ✓ 병렬 잡음원에 적용 가능한 난수발생기 헬스 테스트 기법을 설계하고 효율성을 평가하여 단일 잡음원에 대한 건정성 시험만을 사용할 때보다 효율적임을 보임

■ 경량 블록 암호 PIPO에 대한 도메인 지향 마스킹 기법
  ✓ 경량 블록 암호 PIPO에 대한 하드웨어 부채널 분석 대응기법으로 도메인 지향 마스킹 기법을 적용한 방법을 제시함.

■ CRYSTALS-KYBER 다항식 곱셈의 하드웨어 병렬 구현에 대한 상관 전력 분석
  ✓ NIST PQC KYBER의 하드웨어 병렬 구현된 다항식 곱셈에 대해 상관전력분석 기법을 제시하고 병렬 구현 마다의 공격 성능 변화 추이를 분석함.

■ SEED 마스킹의 일차 부채널 분석 취약점과 대응기법
  ✓ 블록암호 SEED의 마스킹 구현에 대해 1차 부채널 분석 잔여 취약점을 보이고 이에 대한 대응기법을 제시함.

■ 하드웨어 구현 CRYSTALS-KYBER 암호문 비교 연산에 대한 부채널 분석
  ✓ 하드웨어 구현된 NIST PQC KYBER의 디캡슐레이션 과정에서 암호문 비교연산을 대상으로 전력분석을 통해 비밀키를 복구하는 방법을 제시함.

■ DDR4 DRAM의 소프트웨어 기반 Rowhammer 기법과 전자파 오류주입 기반 Ehammer 기법에 관한 연구
  ✓ DDR4 DRAM의 메모리를 변조하는 소프트웨어 기반 Rowhammer 공격과 전자파 오류주입 기반 Ehammer 공격을 비교 분석함.

■ 비교 연산 기반 상수시간 CDT 샘플링에 대한 단일 파형 분석
  ✓ PQC 알고리즘에 많이 사용되는 상수시간 CDT 샘플링 중 비교 연산 기반의 코드에 대해 단일 파형 분석을 제시함.

■ 노트북의 가상메모리 할당/해제를 통한 은닉 채널 형성
  ✓ 노트북의 가상메모리 할당 및 해제시 누설되는 전자파를 이용해 은닉 채널을 형성하는 방법을 제안함.

■ Google 사 Project Vault AES-128 하드웨어 모듈에 대한 상관 전력 분석
  ✓ Google 사의 AES 하드웨어 구현 모듈인 project vault에 대한 상관전력분석을 제안하고 실제 FPGA 환경에서 실험하여 비밀키를 분석함.

■ 스마트폰 디스플레이 변화에 따른 은닉 채널 형성 방안
  ✓ 스마트폰의 디스플레이 변화에 따른 누설 전자파 차이를 이용해서 은닉채널을 형성하는 방법을 제안함.

■ 부채널 분석을 통한 USIM 복제 최신 동향 연구
  ✓ USIM에 대한 부채널 분석 동향을 연구하고 향후 연구 방향을 제시함.

■ KpqC 전자서명 후보 AIMer에 대한 부채널 및 오류주입 공격
  ✓ KpqC 전자서명 후보인 AIMer에 대한 상관전력분석과 오류주입공격을 제안하고 MCU 환경에서 실험을 수행함.

■ “지능형 연안어선 운항안전 모듈 상위 설계”
  ✓ 국내 어선 안전 문제에 대한 해결책으로, 연안어선 안전법과 어민들의 우선순위를 고려한 어선용품 갭분석을 통해 안전하고 효율적인 어선 운항을 도출함. 이를 기반으로 한 ’실시간 운항 안전 유스케이스’와 연안어선의 운항상태를 모니터링하는 기술 및 위험요소 수집 알고리즘을 결합한 ’지능형 연안어선 운항안전 모듈’ 상위 설계함

▶ 연구 업적물(기타)

■ 김동찬 교수 연구팀에서 개발한 부호기반 양자내성암호 PALOMA가 한국 양자내성암호 KpqC 공모전 2라운드 암호로 선정됨 (2023.12)

② 이공계열 참여교수 특허, 기술이전, 창업 실적의 우수성

▶ 국내특허

■ 양자보안 통신장치 통합형 원방감시 제어 시스템 및 방법 (등록)

✓ 양자보안 이동기록 데이터를 수신하여 기기 식별키를 추출하고 기기 식별키를 기초로 양자보안 키를 결정하여 이동기록 데이터를 검출하며, DIM에 대하여 사전에 양자 키 분배를 수행하여 양자보안 키 주입을 처리하는 중앙 이동기록처리 유닛 시스템을 제안함

■ 5G SIDF 암호처리장치 및 그 방법 (등록)

✓ 복수의 GPU(Graphic Processing Unit)를 병렬코어로 구성하여 각 단말에서의 ECIES(Elliptic Curve Integrated Encryption Scheme) 병렬 복호화를 수행함으로써 5G 이동통신망에 단말이 실시간으로 대량으로 접속할 시 SIDF 부하를 줄이고 처리시간을 줄일 수 있는 5G SIDF 암호처리장치 및 그 방법을 제공함

■ 인공신경망을 이용한 RSA 암호에 대한 부채널 분석 방법 및 장치 (등록)

✓ 인공 신경망을 이용해 RSA 암호의 비밀키를 분석하는 방법을 개발한 특허임

■ 무선통신 기기 및 이의 동작방법(등록)

✓ 무선 통신 기기는, 복수의 수광 소자, 상기 복수의 수광 소자와 대응하도록 상기 복수의 수광 소자의 전방에 배치되고, 서로 다른 광 차단율을 갖는 복수의 필터, 및 상기 복수의 수광 소자로 광이 방출되면, 상기 복수의 수광 소자 중 광을 수신한 수광 소자의 개수를 확인하고, 확인된 개수에 기초하여, 상기 무선 통신 기기가 위치한 환경의 탁도를 측정하는 제어부를 포함함

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

✓ 다중통신 시스템 및 통신 방법에 관한 것으로, 더욱 상세하게는 수중 센서 네트워크와 지상 네트워크를 결합하여 수중 및 지상에서 통신을 수행하는 다중통신 시스템임. 수중과 지상이 연결된 다중통신 시스템은 수중 센서 네트워크를 형성하는 수중 센서 노드, 지상 네트워크를 형성하는 지상 노드 및 수중 센서 노드의 신호와 지상 노드의 신호를 상호 변환하여 수중 센서 네트워크와 지상 네트워크를 연결하는 게이트웨이를 포함함

■ 암호화된 데이터베이스의 암호화 모듈 식별 장치 및 방법 (출원)

✓ 데이터베이스 암호화에 취약한 암호화 모듈 사용 여부를 식별하고 식별된 암호화 모듈을 기초로 데이터 복호화 방안 제안한 특허임

■ 스마트기기용 양자보안 통신 제공장치 및 방법 (출원)

✓ 스마트기기에 연결하여 암호보안 통신을 통해 기기 식별을 지원하고 안전하게 데이터를 송수신할 수 있는 스마트기기용 양자보안 통신 제공장치를 제안함

■ 양자암호 기반의 영상 식별 장치 및 방법 (출원)

✓ 영상 기기에서 생성되는 영상에 대한 식별 데이터를 양자암호의 보안을 통해 안전하게 저장하여 진위를 증명할 수 있는 양자암호 기반의 영상 식별 장치를 제안함

■ 양자암호 기반 수하물 식별 장치 (출원)

✓ 각각의 수하물에 대한 식별 데이터를 양자암호의 보안을 통해 안전하게 저장할 수 있는 양자암호 기반의 수하물 식별 장치 및 방법에 대해 제안함

■ 고 지연 네트워크에서 다중 통신 스펙트럼 기반 서비스 요청 추론 기법 (출원)

✓ 이기종 수중 네트워크 연동을 위해 주소 체계 상호 운용성을 제공하는 게이트웨이의 기능 및 동작을 개발한 특허임

■ 수중 무선 통신 시스템을 이용한 수중 무선 네트워크 구성 방법 (출원)

✓ 통신 인프라가 구축되지 않은 수중에서 한시적 네트워크 인프라 구축 기술을 개발한 특허임

■ 다중-모드 수중통신 장치 (출원)

✓ 서로 다른 물리적 특성을 가진 “수중 무선 신호 전송 장치“를 하나의 통신 시스템에서 운용하는 기술과 다양한 수중 무선 신호를 수집하고 해당 데이터를 분석하며, 수중 장치들이 ’인프라스트럭처 모드’ 및 ’애드혹 모드’로 수중 무선 네트워크를 형성하도록 지원합니다. 뿐만 아니라, 무선 신호 전송을 위한 ’링크 상태’ 관리 기술을 개발한 특허임

■ 이미지 센서 기반 엔트로피 축적 장치 및 방법, 이를 이용한 진난수생성기 (출원)

✓ 이미지 센서 기반 양자난수발생기에 적용했을 때 수학적으로 엔트로피 하한을 보장하는 양자난수발생기 엔트로피 축적 방법을 개발한 특허임

■ 모드버스 오류 처리 장치 및 방법 (출원)

✓ 모드버스 프로토콜에 TLS 중계 장치를 추가하여 모드버스 시스템에 대한 공격을 방어하고 오류를 처리하는 방법을 개발한 특허임

■ 인퓨전 펌프에서 네트워크 기반 공격 감소 시도를 위한 MUD 적용 (출원)

✓ 인퓨전 펌프에 존재하는 다양한 보안 위협에 대하여 MUD(Manufacturer Usage Description)를 활용하여 방지하는 기술

■ 5G 환경에서의 허위 기지국으로부터 SON 기능 보호를 위한 그룹 키 기반의 보안 체계 (출원)

✓ BMANF을 활용하여 FBS로부터 수신되는 Broadcast 메시지 수신을 방지하며, SON 기능에 대하여 데이터 품질을 향상 시킨 후, SON Poison 공격으로부터 네트워크를 보호하는 기능에 대한 특허임

■ 군집화 알고리즘을 이용한 블록암호 CTR 운영모드 부채널 분석 방법 및 장치 (출원)

✓ 블록암호의 CTR 운영모드의 부채널 정보들에 군집화 알고리즘을 적용해 비밀키를 분석하는 방법을 개발한 특허임

■ 블록암호에 대한 4바이트 이하 오류 기반의 차분 오류 분석 방법 및 장치 (출원)

✓ 블록암호 특정 라운드에 4바이트 이하의 오류주입을 통해 비밀키를 복구하는 차분 오류 분석 방법을 개발한 특허임

■ 비지도 도메인 적응을 이용한 프로파일링 부채널 분석 방법 및 장치 (출원)

✓ 비지도 도메인 적응을 프로파일링 부채널 분석에 적용하여 공격 대상 장비와 프로파일링 장비가 다를 때도 분석 가능한 방법을 개발한 특허임

■ 경량 블록 암호 PIPO에 대한 Threshold Implementation 적용 방법 (출원)

✓ 경량 블록 암호 PIPO에 대해 Threshold Implementation을 적용하여 부채널 분석 안전성을 가지게 하는 방법을 개발한 특허임

■ 경량 블록 암호 PIPO에 대한 Domain-Oriented Masking 적용 방법 (출원)

✓ 경량 블록 암호 PIPO에 대해 Domain-Oriented Masking을 적용하여 부채널 분석 안전성을 가지게 하는 방법을 개발한 특허임

■ 부채널 공격을 방지하기 위한 암호문 비교 장치 및 방법 (출원)

✓ PQC에 사용되는 암호문 비교 연산에서 비교 결과가 부채널 정보로 누출되는 것을 막는 알고리즘을 제안하여 부채널 안전성을 가지게 하는 장치 및 방법을 개발한 특허임

■ 다항식 연산 기반의 보안 알고리즘의 연산 처리 방법, 그리고 이를 구현하기 위한 장치 (출원)

✓ 다항식 연산 기반의 보안 알고리즘에서 연산 처리 순서를 섞어 부채널 분석 복잡도를 증가시키는 방법을 개발한 특허임

■ 스마트폰 소리 재생 시 누설되는 전자기파를 이용한 은닉 채널 (출원)

✓ 스마트폰이 무음 상태일 때 소리 재생 시 누설되는 특성 전자기파를 통해 은닉 채널을 형성하는 방법을 개발한 특허임

■ 경량 블록 암호 PIPO에 대한 Re-Consolidating Masking 적용 방법 (출원)

✓ 경량 블록 암호 PIPO에 대해 Re-Consolidating Masking을 적용하여 부채널 분석 안전성을 가지게 하는

방법을 개발한 특허임

■ 인공 신경망의 오분류 유도 방법 및 파라미터 복원 방법과 이를 위한 장치 (출원)

✓ 인공 신경망이 수행되는 동안 오류를 주입하여 오분류 유도 및 신경망 파라미터를 복원하는 방법을 개발한 특허임

■ 가상메모리 할당 및 해제를 이용한 은닉채널 형성 방법 및 장치 (출원)

✓ 컴퓨터에서 가상메모리 할당 및 해제를 수행할 때 방출되는 특성 전자기파 신호를 이용해 은닉채널을 형성하는 방법을 개발한 특허임

■ 크리스탈 카이버 연산 장치에 대한 상관 전력 분석 방법 및 장치 (출원)

✓ 양자 내성 암호인 크리스탈 카이버 연산 장치에 대해 상관 전력 분석을 적용하는 방법을 개발한 특허임

■ 마르코프 패스워드 테이블을 이용한 다중 파일 패스워드 크래킹 장치 및 방법 (출원)

✓ 다중 파일에 대한 패스워드 크래킹의 고속화를 통해 빠른 디지털 포렌식 결과의 도출이 가능한 마르코프 패스워드 테이블을 이용한 다중 파일 패스워드 크래킹 장치 및 방법에 관한 특허임

▶ 국제특허

■ DPAPI 기반의 데이터 재생성을 통한 클라우드 데이터 획득 장치 및 방법 (출원)

✓ 클라우드 접속을 위한 크리덴셜 및 크리덴셜 보호를 위해 Windows의 데이터 보호 API인 DPAPI를 사용하는 소프트웨어에 대하여 크리덴셜 재생성을 통해 클라우드 데이터를 획득하는 방법을 제안한 특허임

■ 양자 엔트로피 기반 일회용 양자 비밀번호 생성 장치 및 방법 (출원)

✓ 암호화 시드에 기초하여 일회용 양자 비밀번호(QTP)를 생성하고 일회용 양자 비밀번호(QTP)의 발급 내역을 블록체인 상의 노드에 저장하는 QTP 생성부를 포함한 일회용 양자 비밀번호 생성 장치를 제안함

▶ 기술이전

■ 양자키 유도 함수를 활용한 암호키 생성 방법 및 이를 수행하는 암호키 생성 장치

✓ 난수를 생성하여 암호키로 사용할 때 양자키 유도 함수를 활용하여 암호키를 생성하는 방법에 대한 기술임

■ 화이트박스 암호화 기술

✓ 데이터 암호화를 위한 키를 암복호화하기 위하여 사용하는 비밀키를 안전하게 배포하기 위한 화이트박스 암호화 프로그램에 대한 기술임

■ 양자내성암호 알고리즘 Kyber의 고속구현 기술 이전

✓ 양자내성암호 표준으로 선정된 KYBER의 고속 구현을 위하여 알고리즘을 구성하는 각 함수를 분석하고 구현 병목 현상을 해결한 암호 모듈 개발을 위한 기술임

■ 심리스 DTN 프로토콜을 사용한 수중통신 장치 및 그 통신방법

✓ 수중에서 외부 장치와 광통신을 수행하는 수중 통신 장치에 있어서, 외부 장치로 송신할 제 1 데이터를 제 1 전류로 변조하는 전류 제어부; 및 변조된 제 1 전류에 대응하는 450 내지 500nm의 파장의 광을 외부 장치로 송신하는 광 송신부를 포함하는 것을 특징을 가진 장치 및 기술임

▶ 소프트웨어 등록

■ 경량 데이터베이스(SQLite)에 대한 비밀번호 검증 및 복호화 프로그램 등록

✓ 경량 데이터베이스(SQLite)에 대한 비밀번호 검증 및 복호화 프로그램임

■ 드론 제어 데이터 관리를 위한 Replaying(재생) FDR(비행데이터기록) 장치용 프로그램 등록

✓ 임무를 수행하는 드론과 GCS(지상제어시스템)간의 메시징 프로토콜인 MAVLink 데이터를 Replaying application을 이용하여 드론과 GCS간의 송수신 데이터를 직접 받아 데이터를 관리하는 프로그램임

■ 공간정보 기반 식별용 에이전트 모듈(리눅스) 등록

✓ 수집한 공간 정보를 이용하여 드론 식별 정보를 생성하고, 관리하는 응용 프로그램임

■ 암호모듈 기반 식별 체계용 시험 프로그램(윈도우) 등록

✓ 개체의 식별을 위하여 암호모듈을 기반으로 식별 정보를 생성하고 관리하는 기능을 시험하는 응용 프로그램임

■ Curve25519를 이용한 Kyber의 SETUP 프로그램 등록

■ NTRU(엔트루)가 적용된 모드버스 TLS(티엘에스) 통신 프로그램 등록

■ 측정 보고서(Measurement Report) 학습 데이터 전처리기 프로그램

✓ 이동통신 네트워크에서 발생할 수 있는 Measurement Report(미저먼트 레포트)를 기계 학습에 사용하기 위해 정규화 처리하는 전처리기임

■ 허위기지국 비정상 데이터 생성기

✓ 이동통신네트워크에서 발생할 수 있는 Measurement Report(미저먼트 레포트)을 정규화 처리한 데이터로부터 비정상 데이터를 생성하는 프로그램임

■ 경량 블록암호 피포(PIPO)의 안전한 하드웨어 마스킹 코드

✓ 경량 블록암호 PIPO의 하드웨어 구현에서 부채널 분석 대응기법 마스킹을 적용한 소프트웨어를 등록하였음

■ 신경망 활성 함수 소프트맥스(Softmax) 입력 대상 오분류를 유도하기 위한 비트 반전 시뮬레이션 알고리즘

✓ 신경망 활성 함수 소프트맥스의 입력 대상 오분류를 유도하기 위한 비트 반전 시뮬레이션 소프트웨어를 등록하였음

■ CUDA C 기반 고정 길이 파라미터에 대한 PBKDF2-HMAC-SHA Family 고속 생성 방안

✓ GPU 기기의 병렬 처리를 통하여 입력 인자에 대한 암호학적 파생 키를 고속으로 병렬처리하는 도구임

■ 수중 SNS(소셜 네트워크 서비스)를 위한 S-DTN(심리스 전공지연 감내 네트워크) 기반 이종망 데이터 전송 중계 프로그램

✓ 본 프로그램은 수중 SNS 포스팅 서비스를 위한 게이트웨이(GW)용 응용 소프트웨어임. 수중 통신 장치 UHSDM(Underwater Hybrid Software Defined Modem, 자체개발)’ 을 이용하여 수신된 ‘수중 데이터’ 를 ‘목표 SNS(다이브메모리(*자체 다이버 커뮤니티))’ 에 직접적으로 포스팅을 수행함. 수중통신망과 지상망 간의 원활한 데이터 전송 중계 수행을 위해서 S-DTN(Seamless Delay Tolerant Network, 심리스 지연 감내 네트워크) 기반 통신 상황 인식 기술을 적용함.

③ 연구의 수월성을 대표하는 연구업적물 (최근 1년(2022.9.1.～2023.8.31.))

연번	대표연구업적물 설명
1	▶ A method for decrypting data infected with Hive ransomware [Giyoon Kim, Soram Kim, Soojin Kang, Jongsung Kim, Journal of Information Security and Applications] 2021년 6월에 등장한 Hive 랜섬웨어를 분석하였으며, Hive 랜섬웨어는 막대한 피해를 입혀 FBI가 경고를 발령한 바 있다. Hive 랜섬웨어로 인한 피해를 최소화하고 피해자의 파일 복구를 돕기 위해 Hive 랜섬웨어를 분석하고 복구 방법을 연구했다. Hive 랜섬웨어의 암호화 과정을 분석하여 자체 암호화 알고리즘에 취약점이 존재함을 확인하였다. Hive 랜섬웨어로 암호화된 데이터를 복호화할 수 있도록 파일 암호화 키 생성을 위한 키 테이블을 부분적으로 복구했다. 공격자의 RSA 개인키 없이 키 테이블의 95%를 복구하고 실제 감염된 데이터를 복호화했다.
2	▶ Quantum rebound attacks on reduced-round ARIA-based hash functions [Baek, Seungjun, and Jongsung Kim, ETRI Journal]

	ARIA는 2003년 제안된 국내/외 표준 블록암호이며, TLS 프로토콜에서도 지원하는 잘 알려진 블록암호이다. 블록암호를 기반으로 해시함수를 구성하는 것은 널리 사용되는 해시함수 구성 방식으로, 대표적인 방법은 Davies-Meyer, Matyas-Meyer-Oseas, Miyaguchi-Preneel, Hirose와 MJH 등이 존재한다. 본 연구에서는 언급한 5가지 해시함수 생성 방식에 ARIA 블록암호를 사용할 경우 확보할 수 있는 양자 안전성을 다룬다. 미래의 공격자가 양자 컴퓨터를 사용할 수 있다면, 그로버 알고리즘을 이용하여 암호 공격량을 현저히 낮출 수 있음이 알려져 있으므로, 해당 공격자를 가정하고 ARIA 기반 해시함수들을 분석한다. 이에 대한 상세한 분석과 동시에 관련하여 제시됐던 이전 결과들의 오류를 지적한다. 결론적으로, ARIA를 기반으로 한 해시함수는 양자 컴퓨팅 환경을 고려하더라도 안전성을 침해당하지 않는다.
3	▶ A study on cloud data access through browser credential migration in Windows environment [Uk Hur, Soojin Kang, Giyoon Kim, Jongsung Kim, Forensic Science International: Digital Investigation] 로컬 크리덴셜을 사용하는 포렌식 방식과 달리, 웹 브라우저에 저장된 크리덴셜을 다른 디바이스로 마이그레이션하여 효과적으로 활용하는 새로운 방법을 제안하였다. 분석 결과 대부분의 브라우저가 자격 증명을 암호화하고 저장하는 것으로 나타났으므로 자격 증명 암호 해독 방법을 연구하였다. 해독된 자격 증명을 조사자의 장치로 이동 및 암호화하거나 암호화되지 않은 자격 증명을 간단히 이동하는 마이그레이션 실험을 수행하였다. 총 28개 브라우저에 대한 크리덴셜 마이그레이션 실험을 진행했으며, 그 중 Tor와 같이 데이터를 저장하지 않는 3개 브라우저를 제외한 모든 브라우저에서 마이그레이션이 가능함을 밝혔다. 마이그레이션된 자격증명을 이용하여 자주 사용하는 20종의 웹 서비스에 대한 로그인 및 데이터 수집이 가능한 것을 확인하였다.
4	▶ DIM-based Random Number Generation Using Quantum Noise Resources [Hansaem Wi, Seyoon Lee, Okyeon Yi, “DIM-based Random Number Generation Using Quantum Noise Resources“, Hindawi WCMC, 2022.] 현재 다양한 산업 분야에서 무인 항공기 시스템(UAS) 또는 드론이 서비스되고 있으며, 각 UAS 운영자는 자체적으로 독립적인 드론 시스템을 구축하여 운영하고 있다. 이러한 개별 드론 시스템은 통합적인 관리 없이 자체 구성요소만으로 상호 작용한다. 드론 산업의 확대로 UAS의 수가 증가하고 있어 표준화된 운영이 요구되고 있다. 따라서 기존 드론 시스템을 통합하여 관리하기 위해 연방항공청과 미국항공우주국은 UAS 교통관리(UTM)를 고안하였다. 드론 식별 장치로 개발 중인 드론 식별 모듈(DIM)은 각 드론의 원격 식별(RID)을 안전하게 저장하고 드론과 UTM 인프라 간의 정보를 확보하기 위해 암호화 작업을 수행한다. DIM은 UTM 인프라와 암호화 식별 및 인증을 달성하기 위해 암호화 인증 프로토콜을 수행하며, 이는 난수가 필요하다. 현대의 암호화 시스템은 어려운 계산에 의존하며, 안전한 암호 난수를 생성할 수 있는 환경을 구성해야 공격자에게 높은 계산 비용을 제공할 수 있다.
5	▶ Analysis of Distinguishable Security between the One-Time Password Extraction Function Family and Random Function Family [Hyunki Kim, and Okyeon Yi, “Analysis of Distinguishable Security between the One-Time Password Extraction Function Family and Random Function Family”, MDPI Appl. Sci. 2023, 13, 8761.] 일회용 비밀번호는 인증 시 한 번만 사용하는 비밀번호를 사용하는 보안 시스템으로 다요소 인증 시스템에서 일반적으로 사용된다. OTP를 생성하는 과정은 암호학에서 의사난수열을 생성하는 것과 매우 유사하다. 하지만 OTP에서는 비트열의 일부만 사용하기 때문에 그 일부를 추출하는 알고리즘이 필요하다. 또한 OTP 과정에서는 사람의 인지를 위해 비트열의 값을 십진법 형태로 변환하는 과정도 포함된다. 본 논문에서는 16진수가 십진법 형태로 재가공되기 전 단계인 추출 함수를 분석하는 데 중점을 둔다. 비트열 추출

	과정에서 사용되는 함수를 구별 가능한 보안성 측면에서 포함하는 함수 패밀리를 분석한다. 따라서 OTP 추출 함수 패밀리는 랜덤 함수 패밀리에 비해 구별 가능한 보안성 측면에서 취약하다는 결론을 내렸다
6	▶ Rider Optimization with Deep Learning Based Image Encryption for Secure Drone Communication [N. Kannaiya Raja, E. Laxmi Lydia, T Archana Acharya, K. Radhika, Eunmok Yang and Okyeon Yi, “Rider Optimization with Deep Learning Based Image Encryption for Secure Drone Communication”, IEEE ACCESS. 2023] 최근 드론 또는 무인항공기(UAV)는 상업적 응용, 국경 감시 등에 광범위하게 적용되어 연구자들 사이에서 큰 주목을 받았다. 기존의 지상 통신 시스템이 홍수, 산사태, 사이클론, 지진 등과 같은 대규모 재해에 효과적으로 작동하지 않기 때문에 UAV는 저렴하고 신속하며 무선 통신을 위한 잠재적인 솔루션을 제공할 수 있다. 긴급 모니터링에서 드론의 이점에도 불구하고 전송을 위한 무선 연결이 존재하기 때문에 보안이 주요 요인이었다. 따라서 본 논문에서는 이미지 암호화 기반 보안 드론 통신(ODLE-SDC) 기법을 통한 최적의 딥 러닝을 소개한다. ODLE-SDC 기법의 주요 의도는 긴급 모니터링 시나리오에서 효과적인 보안 통신 및 분류 프로세스에 있다. 이를 위해 제시된 ODLE-SDC 기법은 하이퍼차오틱 맵 기반 이미지 암호화 기법을 설계하고 라이더 최적화 알고리즘(ROA)을 사용하여 최적의 키를 생성한다. 이미지 분류 프로세스는 EfficientNet-B4-CBAM 특징 추출 및 ESAE(Enhanced Stacked AutoEncoder) 분류를 포함하여 수행된다. 마지막으로 이미지 분류 프로세스는 EfficientNet-B4-CBAM 특징 추출 및 ESAE(Enhanced Stacked AutoEncoder) 분류를 포함하여 수행된다. EfficientNet-B4-CBAM 기법의 하이퍼파라미터 튜닝은 베이지안 최적화(BO) 알고리즘을 사용하여 이루어진다. ODLE-SDC 기법의 실험적 검증은 AIDER 데이터셋을 대상으로 실험한다. 종합비교분석에서는 기존의 다른 접근법에 비해 ODLEDC 기법의 성능이 향상된 것으로 보고하였다.
7	▶ Energy Optimization Techniques in Underwater Internet of Things: Issues, State-of-the-Art, and Future Directions [Delphin Raj Kesari Mary, Eunbi Ko, Dong Jin Yoon, Soo-Young Shin and Soo-Hyun Park, water 2022] 해양에서의 수중 사물 인터넷(UIoT)은 해양 탐사, 심해 모니터링, 수중 감시 등 다양한 분야에서 중요한 역할을 하며, 음향, 적외선, 가시광선, 무선주파수, 자기유도 등 다양한 통신 매체를 활용함 각 통신 매체는 특정 문제를 가지며, UIoT 디바이스의 높은 에너지 소비는 에너지 효율 문제로 작용하므로 최신 연구와 문제점을 분석하여 향후 UIoT 네트워크의 에너지 효율 개선 방향을 제시함
8	▶ 수중 노이즈 상황에서의 기하학 기반 적외선 통신 채널 모델 [발카시나 스베틀라나, 황아리, 이진영, 염선호, 박수현, 전자공학회논문지 2022년 11월호] 수중 통신에 대한 관심도 증가는 감시부터 기후변화 모니터링까지 수중 및 해안 지역을 탐사하는데 있어 중요한 역할에 의해 결정된다. 극한 환경으로 인해 수중 통신의 구현은 감쇠, 산란, 난류 등과 같은 수중 노이즈에 대한 심각한 문제에 직면한다. 그리고 이 문제에 대한 몇 가지 연구가 진행 중이다. 그러나 수중 노이즈 중에서 난류 감쇠의 한 형태인 수중 기포는 특히 수중광통신(UWOC)에 미치는 영향에 대해 충분히 연구되지 않았다. 본 논문에서는 Beer-Lambert의 감쇠 법칙과 기하학적 광학을 이용하여 기포에 대한 새로운 수학적 채널 모델링 기법을 도입하여 거리, 전력 및 물 유형에 따른 광통신의 성능을 보여준다. 시뮬레이션 결과는 난류 환경에서 적외선 채널의 성능이 수중 가시광선 통신보다 강력하다는 것을 보여주었다.
9	▶ Practical Entropy Accumulation for Random Number Generators with Image Sensor-Based Quantum Noise Sources

	[Choi, Youngrak, Yongjin Yeom, and Ju-Sung Kang. 2023. “Practical Entropy Accumulation for Random Number Generators with Image Sensor-Based Quantum Noise Sources“ Entropy 25, no. 7: 1056.] 암호화 모듈의 작동에 있어 고품질의 난수를 효율적으로 생성하는 것은 필수적이다. 난수생성기의 품질은 엔트로피 소스의 최소 엔트로피(min-entropy)로 평가할 수 있다. 일반적으로는 최소 엔트로피를 높이기 위해 Leftover Hash Lemma에 기반한 해시 함수를 통해 엔트로피를 축적한다. 그러나 이 방법은 엔트로피 축적 속도가 느리다는 한계가 있다. 본 연구실에서는 출력 수열의 최소 엔트로피에 대한 이론적 배경을 가진 새로운 효율적인 엔트로피 축적 기법을 제시한다. 엔트로피 소스로부터 얻는 난수열이 독립적일 때, 제시한 엔트로피 축적 기법은 비트 단위 XOR 연산만을 사용하여 매우 효율적으로 출력 난수열에 대한 이론적 최소 엔트로피를 제시할 수 있도록 한다.
10	▶ End-to-End Post-Quantum Cryptography Encryption Protocol for Video Conferencing System Based on Government Public Key Infrastructure [Park, Yeongjae, Hyeondo Yoo, Jieun Ryu, Young-Rak Choi, Ju-Sung Kang, and Yongjin Yeom. 2023. “End-to-End Post-Quantum Cryptography Encryption Protocol for Video Conferencing System Based on Government Public Key Infrastructure“ Applied System Innovation 6, no. 4: 66.] 암호화 모듈의 작동에 있어 고품질의 난수를 효율적으로 생성하는 것은 필수적이다. 난수생성기의 품질은 엔트로피 소스의 최소 엔트로피(min-entropy)로 평가할 수 있다. 일반적으로는 최소 엔트로피를 높이기 위해 Leftover Hash Lemma에 기반한 해시 함수를 통해 엔트로피를 축적한다. 그러나 이 방법은 엔트로피 축적 속도가 느리다는 한계가 있다. 본 연구실에서는 출력 수열의 최소 엔트로피에 대한 이론적 배경을 가진 새로운 효율적인 엔트로피 축적 기법을 제시한다. 엔트로피 소스로부터 얻는 난수열이 독립적일 때, 제시한 엔트로피 축적 기법은 비트 단위 XOR 연산만을 사용하여 매우 효율적으로 출력 난수열에 대한 이론적 최소 엔트로피를 제시할 수 있도록 한다. 재택근무 및 비대면 회의의 증가에 따라 화상 회의 시스템 보안에 대한 수요가 증가하고 있다. 본 연구실에서는 화상 회의 시스템의 보안 서비스 중 End-to-End Encryption(E2EE) 기능을 연구하기 위하여 주요 화상 회의 시스템인 Zoom과 Secure Frame (SFrame)의 E2EE 프로토콜을 비교 및 분석하고, 이들과 달리 행정전자서명 인프라(Government Public Key Infrastructure, GPKI)에 기반하는 화상 회의 시스템의 E2EE 프로토콜을 제시한다. 또한 사용자 키 교환 과정에 양자내성암호(Post-Quantum Cryptography, PQC) 키 캡슐화 메커니즘(Key Encapsulation Mechanism, KEM)을 적용하는 방법을 제안함으로써, GPKI 기반 프로토콜이 차세대 화상 회의 시스템의 보안 수준을 양자 컴퓨터에 내성을 가지는 수준까지 향상될 것을 전망함.
11	▶ “APSec1.0: Innovative Security Protocol Design with Formal Security Analysis for the Artificial Pancreas System“, Jiyoon Kim, Jongmin Oh, Daehyeon Son, Hoseok Kwon, Philip Virgil Astillo and Ilsun You, Sensors (SCIE, I.F=6.3) 의료사물인터넷 (MIoT) 중 대표적인 인공 췌장 시스템의 보안 취약점을 보완하고 보안 요구사항을 고려한 새로운 보안 프로토콜을 제안하고 BAN 논리와 AVISPA 정형화 검증 도구를 통해 검증하고 여러 보안 프로토콜과 성능 비교 및 분석하여 프로토콜의 우수성을 제시함.
12	▶ Chosen-Ciphertext Clustering Attack on CRYSTALS-KYBER Using the Side-Channel Leakage of Barrett Reduction [Bo-Yeon Sim, Aesun Park, Dong-Guk Han, “Chosen-Ciphertext Clustering Attack on CRYSTALS-KYBER Using the Side-Channel Leakage of Barrett Reduction “, IEEE IoT journal 9 (2022): 21382-21397]

	NIST PQC CRYSTALS-KYBER 대상으로 선택 암호문 부채널 공격을 제안했다. 역 NTT나 메시지 인코딩/디코딩과 같은 연산을 대상으로 하는 기존 부채널 공격과 달리, 비밀 키를 얻기 위해 CRYSTALS-KYBER의 복호화 단계에서 Barrett reduction을 공격 대상으로 한다. 변수 종속적인 Barrett reduction의 누출이 전체 비밀 키를 노출시킨다는 것을 보여주고 ARM Cortex-M4 MCU에서 실험을 수행한 결과 100%의 공격 성공률을 달성했다. KYBER512와 KYBER768의 경우 6개의 암호문이 필요했고, KYBER1024의 경우 8개의 암호문이 필요했다. 또한 ARM Cortex-M4 특정 최적화 레벨로 구현된 pqm4 라이브러리가 제안된 공격에 취약하다는 것을 보였다.
13	▶ Deep-Learning Based Nonprofiling Side-Channel Attack on Mask Leakage-Free Environments Using Broadcast Operation [SeongHyuck Lim, Hye-Won Mun, Dong-Guk Han, “Deep-Learning Based Nonprofiling Side-Channel Attack on Mask Leakage-Free Environments Using Broadcast Operation “, IEEE ACCESS 11 (2023): 94335-94345] 부채널 대응기법인 마스킹이 적용된 암호 대상으로 딥러닝을 활용한 부채널 분석을 통해 효과적으로 비밀키를 복구할 수 있는 방법론을 제시했다. 마스킹 정보뿐만 아니라 마스킹된 2바이트 정보를 결합한 경우의 분석을 시도했으며 보다 효과적인 공격을 수행하기 위한 신경망 설계 기법을 제안했다. 기존에는 공격 대상 8비트 값의 일부 비트, 8비트 값의 이진 인코딩 값을 딥러닝 신경망의 라벨 값으로 사용했으나 제안하는 방법에서는 8비트 값을 해밍웨이트를 기준으로 하여 2가지로 나누는 방식을 채택했고, 이를 broadcast 연산을 통해 설계했다. 제안한 기법의 효과를 보이기 위해 오픈 데이터셋, 시뮬레이션 및 실제 보드에서 기존 공격 기법과 비교했다.
14	▶ AVX512Crypto: Parallel Implementations of Korean Block Ciphers Using AVX-512 [“AVX512Crypto: Parallel Implementations of Korean Block Ciphers Using AVX-512“ by YongRhyel Choi, Hojin Choi, and Seog Chung Seo, IEEE ACCESS (SCIE, IF=3.476)] 암호알고리즘은 다양한 보안시스템의 기초로 널리 사용되고 있으며, 애플리케이션(예: 보안 통신, 블록체인 시스템, 클라우드 서비스) 블록 암호는 기밀성을 확보하기 위한 필수 암호화 알고리즘이다. 이 논문에서는 병렬 구현을 제안한다. 새로운 Single 명령어인 AVX(Advanced Vector eXtension)-512를 이용한 한국어 블록 암호, 최근 여러 고급 Intel 중앙 시스템에 통합된 다중 데이터(SIMD) 명령어 세트 처리 장치(CPU)이다. 대상 알고리즘은 LEA, HIGHT 및 CHAM 블록 암호이다. 추가적으로, 본 논문에서는 또한 각 알고리즘에 맞게 설계된 적용 가능한 구현 기법을 제안한다. 이를 통해 각 알고리즘에 맞게 AVX-512의 병렬 처리 명령을 사용할 수 있다. 제안된 LEA-128(192, 256 resp.) 구현은 다음과 같은 성능 향상을 보여준다. 참조 코드 및 HIGHT 구현과 비교하여 506.09%(323.31%, 386.76% resp.) 레퍼런스 코드 대비 520.88%의 성능 향상을 보여준다. 또한 CHAM64/128(128/256 resp.) 구현에서는 1,325.81%(833.61% resp.)의 성능 향상을 보여준다.
15	▶ Optimized Implementation of PIPO Block Cipher on 32-bit ARM and RISC-V [“Optimized Implementation of PIPO Block Cipher on 32-bit ARM and RISC-V Processors “ by YoungBeom Kim and Seog Chung Seo, IEEE ACCESS (SCIE, IF=3.476)] ICISC’2020에서는 경량 블록 암호 PIPO-64/128이 발표되었다. 8비트의 PIPO 불균형 브리지 S-box를 사용하는 장치는 다른 경량 블록 암호보다 더 나은 성능을 보였다. 8비트 AVR 환경의 알고리즘. 지금까지 PIPO 구현을 위한 최적화 방법은 다양한 환경에서 제안되었다. 그러나 두 가지에 대한 최적화 연구는 수행되지 않았다. 널리 사용되는 32비트 기반 프로세서: ARM Cortex-M4 및 RISC-V. RISC-V 및 ARM

	Cortex-M 이후 시리즈 플랫폼은 비트 기반 SIMD(Single Instruction Multiple Data) 명령어를 지원하지 않는다. 강제 병렬화 전략을 적용하려면 측면을 고려해야 한다. 본 논문에서는 32비트 RISC-V 및 ARM Cortex-M4 환경을 위한 PIPO 구현 최적화 방법론에 대해 논의한다. 제안된 레지스터 스케줄링 및 마스킹 기술을 통해 S-Layer의 성능을 유지하는 동시에 R-Layer 구현과의 병렬성. 또한, 온더플라이(on-the-fly) 키 스케줄링 기법을 제안한다. 마지막으로 기존 참조 구현과 비교하면 다음과 같다. RISC-V 및 ARM Cortex-M4 플랫폼에서 4개의 일반 텍스트가 동시에 암호화되면 소프트웨어 각각 229%, 370%의 성과를 달성한다.
16	▶ Signature Split Way for PQC-DSA Compliant with V2V Communication Standards ["Signature Split Way for PQC-DSA Compliant with V2V Communication Standards" by YoungBeom Kim and Seog Chung Seo, MDPI Applied Sciences (SCIE, IF=2.838)] 양자컴퓨팅 시스템의 발전은 보안에 큰 위협이 되고 있다. 기존 공개 키 기반 시스템. 이에 따라 국립표준기술원은 NIST(NIST)는 2015년부터 PQC(Post-Quantum Cryptography) 표준화 프로젝트를 시작했으며 현재 다양한 암호화 프로토콜에 PQC를 적용하기 위한 연구가 활발히 진행되고 있다. 곡선 암호화(ECC) 기반 체계와 달리, PQC에는 큰 메모리 공간과 키/서명이 필요하다. 따라서 PQC를 프로토콜로 마이그레이션할 때 PQC 및 프로토콜 사양에 따라 PQC를 마이그레이션하는 것은 어려울 수 있다. 특정 PQC 알고리즘의 경우 전송 중에 서명 분할이 발생하기 때문에 WAVE 프로토콜의 경우 정확도를 만족시키기 어렵다. 따라서 본 논문에서는 두 가지 방법론을 제시한다. 이전 마이그레이션 연구는 하이브리드 모드 설계에 중점을 두었다. 프로토콜과 관련하여 이 문서에서는 프로토콜의 애플리케이션 계층에서 보다 직관적으로 솔루션을 탐색한다. 우리는 두 가지 PQC 디지털 서명 알고리즘(Crystals-Dilithium 및 Falcon)을 분석했으며 크기 측면에서 V2V 프로토콜의 기본 안전 메시지(BSM) 구조. 이를 통해 우리는 기다리지 않고 독립적인 서명 검증 프로세스를 수행할 수 있는 방법을 제안한다. V2Verifier를 사용하여 방법론을 시뮬레이션했으며, 정확한 지연 시간을 측정했다. V2V 통신 네트워크에서 주로 OBU로 사용되는 Jetson Xavier에서의 시뮬레이션이다.
17	▶ 수중 센서 데이터의 SNS 포스팅 서비스 설계 및 구현" 이정국, 염선호, 이진영, 박수현, 박철웅, 신수영, 한국통신학회논문지, 2023년 8월호 수중 통신을 사용하여 스쿠버 다이빙 중 얻은 센서 데이터를 서버에 전달 후 원하는 데이터만선택하여 SNS환경에 업로드 할 수 있는 시스템을 설계 및 구현하였다. 본 시스템을 구현하기 위해 수중 통신 시스템과 이를 운용하기 위한 하드웨어를 구현하였으며 수면 게이트웨이를 구현하여 수중과 지상의 이종망 통신 시스템을 구축하였다. 마지막으로 사용자 어플리케이션을 구현하여 수중에서 얻은 센서 데이터를 관리하고 원하는SNS에 업로드 할 수 있도록 하였다.

2. 산업・사회에 대한 기여도

▶ 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. 이를 논문으로 발표하고 한국 인터넷 진흥원 및 과기정통부와 협업하여 복호화 도구 제작 및 배포 작업을 통해 랜섬웨어 피해를 완화하는데 도움이 될 것으로 기대됨
▶ 김종성 교수는 양자컴퓨팅 환경에서의 블록암호와 해시함수 분석 및 설계에 관한 연구를 진행하여 자체 평가기간 동안 국제학회 1편, 국제저널 1편과 국내학술대회 1편의 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, 블록암호와 해시함수의 양자 저항성에 관한 연구가 필요하고 양자 저항성을 갖는 블록암호와 해시함수의 설계가 필요함. 그러므로 현재 연구 중인 분야는 앞으로 국내 미래 암호기술 발전에 도움이 될 것으로 기대됨

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

▶ 이옥연 교수는 군용 드론 보안과 이동통신 보안 연구를 꾸준히 진행하고 있으며, 이를 양자 엔트로피 기반 난수발생기 등의 양자보안과 융합시키는 연구 또한 진행 중임. 2022년에는 한국정보보호학회 회장을 맡아 국내 정보보호 학계를 대표하는 역할을 수행하였으며, 국방암호기술특화연구센터 제3실장, 대검찰청디지털수사자문위원, 5G 보안협의회 의원 등 다양한 국내 산업 및 사회를 위한 정보보안 전문가로써 우리 사회를 위협하는 정보보안 문제해결을 위한 정책자문과 기술발전에 기여하고 있음.

▶ 강주성, 염용진 교수는 양자내성암호에 사용되는 난수의 분포에 대한 안전성 분석을 연구하고 기반 문제들을 파악하기 위한 연구를 지속하고 있음. NIST 양자내성암호 공모전을 통해 국제 표준으로 선정된 KYBER의 구성과 수학적 구조를 분석함으로써 국내 기업 및 시스템에 양자내성암호를 도입하기 위한 방향성을 분석함. 한국에서 진행 중인 KpqC 공모전은 한국형 양자내성암호의 저변 확대 및 알고리즘 제안을 통한 표준화 움직임 독려를 목표하며, 강주성, 염용진 교수는 해당 공모전에 기존에는 제안되지 않았던 조합론 기반 암호를 제시함으로써 암호 분야의 다양성에 기여할 것으로 기대됨.

▶ 강주성, 염용진 교수는 난수발생기의 잡음원 분포, 엔트로피 축적 기법, 보안 프로토콜 안전성 분석, 경량 환경에서의 암호 알고리즘 적용 등의 연구를 진행하여 자체 평가기간동안 특허 출원 2건, 국제 논문지 2편, 국내 논문지 1편, 국제 학술대회 1편, 국내 학술대회 3편의 성과를 냄. 특히 정보보안시스템에서 난수발생기는 암호키와 보안 매개변수, 암호 프로토콜에서 사용하는 각종 파라미터 등의 생성 시에 반드시 사용되어야 하는 핵심 요소임. 안전하지 않은 난수발생기의 사용이나 잘못된 사용 때문에 암호시스템과 암호 프로토콜의 취약점이 발견된 사례가 빈번하게 보고되고 있음. 따라서 암호학적 난수발생기의 안전성은 입력되는 잡음원의 엔트로피에 의존하기 때문에 사용되는 잡음원에 대한 엔트로피를 최대한 정확하게 추정할 수 있는 기술은 필수적으로 필요함. 그러므로 본 연구 결과들은 안전한 난수발생기 사용에 대한 토대를 마련하여 난수발생기의 취약성으로 발생할 수 있는 산업・사회적 피해를 최소화하는 데 이바지할 수 있을 것으로 기대됨

▶ 유일선 교수는 5G 보안연구회 위원장으로 2018년부터 매년 5G보안 워크숍을 주관하여 2023년 기준 6회째 개최하였음. 특히 2023년 급변하는 사이버 보안 상황에 대응하기 위한 제로트러스트, 암호화 트래픽 관제 등과 같은 미래 기술을 논의하고, 안전한 5G 환경을 위해 사이버보안기술이 나아가야 하는 방향성에 대한 논의를 진행함

▶ 유일선 교수는 현재 과학기술정보통신부 5G 보안협의회 기술분과장으로 분과 회의를 통해 주요 선진국의 5G 보안 정책, 5G 핵심 네트워크 보안 위협 및 대응기술, 5G 보안 국제 표준화 동향 등 측정 주제별로 심층 논의하고 이에 대한 정책 방향 및 제도적 개선 방안 모색에 기여함

▶ 한동국 교수는 부채널 분석 연구회 회장을 맡아 2018년 10월부터 매년 부채널정보분석 워크숍을 주관하여 현재 5회째 개최하였고, 특히 5회에서는 코드 안티탬퍼링 기술, 양자 내성 암호 안전성 및 최적화 등의 다양한 분야에서 부채널 보안기술의 중요성을 알리고 있음. 또한 부채널정보분석 경진대회를 개최하여 학생들의 부채널 분석 연구를 장려하고, 연구소, 기업, 학계 사이에 부채널 보안에 대한 지식 공유의 장을 생성하는데 기여하고 있음.

▶ 한동국 교수는 부채널 분석과 오류주입 분석 기법 총 2건에 대한 국내 표준화를 진행하여 정보보호제품 시험, 인증 기관 및 민간 기업들에게 부채널 분석 안전성 검증 기준을 제시했음. 해당 표준을 통해 부채널 분석 기술 적

용 기준을 명확히 했고 이는 제품의 부채널 분석 안전성 검증 과정에 기여함. 따라서, 실생활에 사용될 제품들의 부채널 분석 안전성 검증 및 안전성 강화에 활용되어 향후 발생할 수 있는 산업·사회적 피해를 사전에 예방할 수 있을 것으로 기대됨

▶ 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 것으로 기대됨

▶

3. 연구의 국제화 현황

① 참여교수의 국제적 학술활동 참여 실적 및 현황

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

▶ 김종성 교수는 The 24th World Conference on Information Security and Applications (WISA) 국제 학술대회의 Program committee로 활동함

▶ 김종성 교수는 2023 International Conference on Platform Technology and Service (PlatCon-23) 국제 학술대회의 Steering Committee 및 Banquet Chair로 활동함

▶ 이옥연 교수는 SCIE 저널 Hindawi WCMC(IF: 2.146)의 Associate Editor로 활동함

▶ 이옥연 교수는 SCIE 저널 MDPI Applied Sciences(IF: 2.838)의 Associate Editor로 활동함

▶ 이옥연 교수는 SCIE 저널 IEEE ACCESS(IF: 3.367)의 Associate Editor로 활동함

▶ 유일선 교수는 세계 Elsevier-Stanford University의 세계 상위 2% 과학자에 선정됨

▶ 유일선 교수는 국제 컨퍼런스 Mobile Internet Security의 General Chair로 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

▶ 유일선 교수는 Information Science Associate Editor로 활동함

▶ 유일선 교수는 국제 저널인 IEEE Access의 Associate Editor로 활동함

▶ 유일선 교수는 Springer의 국제 저널인 Soft Comouting의 Associate Editor로 활동함

▶ 유일선 교수는 국제 저널인 Information Sciences의 Associate Editor로 활동함

▶ 한동국 교수는 Fault Diagnosis and Tolerance in Cryptography (FDTC) 국제 학술대회의 Program committee로 활동함

▶ 한동국 교수는 The 26th Annual International Conference on information Security and Cryptology (ICISC) 국제 학술대회의 Program committee로 활동함

▶ 한동국 교수는 한국정보보호학회 제 24회 정보보호응용 국제 컨퍼런스 (WISA 2023) Organizing committee으로 활동함
▶ 박수현 교수는 한국멀티미어학회 편집운영위원으로 활동함
▶ 박수현 교수는 대한전자공학회 컴퓨터소사이어티 부회장으로 활동함
▶ 박수현 교수는 한국시뮬레이션학회 논문지편집위원회 자문위원으로 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	Laxmi Lydia	India / Vignan's Institute of Information Technology	3.367의 IF를 갖는 Hindawi WCMC에 "Rider Optimization with Deep Learning Based Image Encryption for Secure Drone Communication" 논문을 게재함. 본 논문은 긴급 모니터링 시나리오에서 효과적인 보안 통신 및 분류 프로세스를 위해 이미지 암호화 기반 보안 드론 통신(ODLE-SDC) 기법을 통한 최적의 딥러닝을 제안함	10.1109/ACCESS.2023.3324068

③ 외국 대학 및 연구기관과의 연구자 교류 실적 및 계획

▶ 유일선 교수팀은 전 세계 암호분야에서 최정상급에 위치하고 있는 오세아니아 월런공대학교와 '22.11.01부터 현재까지 국제 공동 연구를 수행중임