2023년 국가 암호기술 전문인력 양성과정(9기)

지 원 서

▣ 기본 인적사항

성 명	(한글) 엄 시 우 (영문) Eum Si Woo		
성 별	남	생년월일	94. 2. 8.
휴대전화	010-4415-1448	Email	shuraatum@gmail.com
소속(학교)	한성대학교	학과/전공	정보컴퓨터공학/정보시스템공학
과정(년차)	박사(1년차)	지도교수	서 화 정

▣ 학력

학교명	기간 (월 단위까지)	평점	학과	전공	과정
한성대학교	2013.03~2021.02	3.7/4.5	IT융합공학	사이버보안	학사
한성대학교 대학원	2021.03~2023.02	4/4.5	IT융합공학	IT융합공학	석사
	(논문명) RISC-V상에서의 Fixslicing AES CTR 운용 모드 최적화 구현				
	(소속Lab 및 지도교수명) CryptoCraft / 서화정				
한성대학교 대학원	2023.03~	/4.5	정보컴퓨터공학	정보시스템공학	박사
	(논문명)				
	(소속Lab 및 지도교수명) CryptoCraft / 서화정				

* 석사/박사/통합과정 중의 평점은 현재까지 평균 학점으로 기록
* 학점 만점 기준이 4.5가 아닌 경우 환산방법
  ① 성적증명서에 4.5만점 기준의 환산 점수가 기재되어 있는 경우 해당 점수를 기입
  ② 4.5만점 기준의 환산점수가 기재되어 있지 않은 경우에는 아래의 산식을 이용하여 기입
  (예1) 4.0만점 기준에 평점 3.0 획득 시 기입 평점: (3.0 * 4.5) / 4.0 = 3.375
  (예2) 100점만점 기준에 평점 60점 획득 시 기입 평점: (60 * 4.5) / 100 = 2.7
  (예3) 일부 외국대학에서 등급으로만 성적이 표기된 경우는 성적표 내의 등급별 점수 환산표를 이용하여 기재하되, 등급이 일정 구간의 점수를 의미하는 경우에는 해당 구

간의 최고•최저점의 평균값을 기재 (예: A: 90~80인 경우 85로 기재)

* 평점은 소수 둘째자리까지 기재하며, 셋째 자리에서 반올림

▣ 연구실적물 등 현황(최근 3년 이내)

논문 실적	SCI	SCIE	국제 저널·논문	국내 저널·논문	국제 학술대회	국내 학술대회	계
	1편	0편	0편	4편	1편	8편	14편

※ 제1저자로 게재 완료 및 게재수락된 건만 기재하며, 모두 증빙자료 첨부가능해야 함

특허실적	국제특허등록	국내특허등록	계
	0건	0건	0건

※ 제1발명자로서 등록완료 및 증빙자료 첨부 가능한 건만 기재

연구과제 수행실적	연구책임자	연구참여자	계
	0건	0건	0건

연구결과물 관련 수상실적	대회/학회명 및 수상내용	공동수상자	당시 소속기관	수상 연월일
	제 3 회 부채널분석 경진대회, 부채널 분석연구회장상 수상	송경주, 심민주	한성대학교	20.10.15
	SCR-Friendly 경량 블록암호 PIPO 고속구현, SCA, 활용사례 경진대회	김현준, 심민주	한성대학교	21.10.15
	AI+Security 아이디어 최우수상	김현준, 장경배	한성대학교	21.12.15
	2022 국가암호공모전 특별상	심민주	한성대학교	22.10.20
	2022 부채널 분석 경진대회 KISA 원장상		한성대학교	22.10.28

[연구실적물 목록]

* 지원서의 '연구실적물 등 현황'과 일치해야함

▣ 논 문

※ 최근 3년 이내(2020년 부터) "제1저자"로 게재완료 및 게재수락된 논문에 한하며, 지원서 상의 실적내역과 일치하도록 작성

구분	논문명	게재지 발표대회	수록 page	게재/발표 년월일	공동 저자
SCI (1편)	Parallel Implementations of ARIA on ARM Processors and Graphics Processing Unit	Applied Sciences	12/34/11246	22.01	김현준 권혁동 심민주 송경주 서화정
국제 학술대회 (1편)	Implementation of SM4 block cipher on CUDA GPU and its analysis	2022 PlatCon	71-74	22.08.22	김현준 권혁동 장경배 김현지 서화정
국내저널 논문집 (4편)	64-bit ARM 프로세서 상에서의 블록암호 PIPO 병렬 최적 구현	정보처리학회	10, 8, 223-230	2021. 5	권혁동 김현준 장경배 김현지 박재훈 심민주 송경주 서화정
	32-bit RISC-V 상에서의 사전 연산을 활용한 Fixslicing AES-CTR 속도 최적화 구현	정보보호학회	32, 1, 1-9	2022. 2	김현준 심민주 송경주 서화정
	32-bit RISC-V 상에서의 PIPO 경량 블록암호 최적화 구현	정보처리학회	11, 6, 167-174	2022	장경배 송경주 이민우 서화정
	32-bit RISC-V상에서의 LEA 경량 블록 암호 GCM 운용 모드 구현	정보보호학회	32, 2, 163-170	2022. 04. 30	권혁동 김현지 양유진 서화정

▣ 특 허

※ 최근 3년 이내(2020년 부터) "제1발명자"로 "등록 완료"된 특허에 한하며, 지원서 상의 실적내역과 일치하도록 작성

구분	특허명	등록 번호	등록 국가	등록 연월일	공동 발명자
국제 특허					
국내 특허					

▣ 연구과제(프로젝트) 수행실적

※ 최근 3년 이내(2020년 부터) 참여율이 포함된 연구과제에 한하며, 지원서 상의 실적내역과 일치하도록 작성

발주처	연구과제명	참여형태 (참여율)	수행기간	당시 소속기관
IITP	IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구	참여연구원 (50%)	2020-08-01 ~ 2020-12-31	한성대학교
IITP	미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술 개발	참여연구원 (10.8%)	2021-01-01 ~ 2021-12-31	한성대학교
IITP	IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구	참여연구원 (32.5%)	2021-01-01 ~ 2021-12-31	한성대학교
IITP	GPU/ASIC 기반 암호알고리즘 고속화 설계 및 구현 기술개발	참여연구원 (30%)	2021-04-01 ~ 2021-12-31	한성대학교
IITP	미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발	참여연구원 (10%)	2022-01-01 ~ 2022-12-31	한성대학교
IITP	GPU/ASIC 기반 암호알고리즘 고속화 설계 및 구현 기술개발	참여연구원 (25%)	2022-01-01 ~ 2022-12-31	한성대학교
IITP	저사양 디바이스 지원을 위한 경량 사물 블록체인 네트워크 기술개발	참여연구원 (10%)	2022-04-01 ~ 2022-12-31	한성대학교
IITP	저사양 디바이스 지원을 위한 경량 사물 블록체인 네트워크 기술개발	참여연구원 (17%)	2023-01-01 ~ 2023-12-31	한성대학교
IITP	미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발	참여연구원 (13%)	2023-01-01 ~ 2023-12-31	한성대학교
IITP	IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구	참여연구원 (15%)	2023-01-01 ~ 2023-12-31	한성대학교
IITP	GPU/ASIC 기반 암호알고리즘 고속화 설계 및 구현 기술개발	참여연구원 (15%)	2023-01-01 ~ 2023-12-31	한성대학교

자 기 소 개 서

1. 관심 연구 주제 / 지원 동기 / 바라는 점에 대해 기재해 주십시오.

안녕하세요. 한성대학교 서화정 교수님 연구실에서 박사과정을 하고 있는 엄시우라고 합니다. 대학원에 진학하여 암호를 처음 접하게 되었고, 암호 구현에 관심이 생겨 현재 암호 구현을 연구 분야로 공부하고 있습니다. 석사 1년차 동안 RISC-V 프로세서를 활용하여 최적화 암호 구현을 공부하였습니다. 석사 2년차에는 ARM 프로세서를 활용하여 최적화 구현을 공부하였습니다. 석사과정을 통해서 많은 공부를 하면서 많은 것을 알았다고 생각했지만 졸업할 때가 되니 모르는게 더 많아지는 기분이 들었습니다. 그래서 저는 박사과정을 진학하였고, 박사과정 동안에는 GPU를 활용한 암호구현 연구에 집중해볼 예정입니다.

암호기술 전문인력 양성과정을 통해서 새로운 분야와 이론들을 전문가분들에서 직접 배우고 실습을 통해서 배울 수 있다는 것이 굉장히 좋은 기회라고 생각하여 지원하게 되었습니다. 대학원 진학하여 새로운 이론을 공부하고 적용하기 위해서 혼자 찾아보고 실습해보며 공부를 하는 경우가 많은데, 스스로 공부하는 것이 바람직 할 수 있으나 잘못된 이론을 공부하고 있을 수도 있고, 많은 시간을 필요로 하게 됩니다. 양성과정을 통해서 새로운 기초 이론을 전문가분에게 배우고 실습을 통해 흥미를 얻을 수 있는 기회라고 생각합니다.

현재 시대의 흐름은 하나의 분야만 공부하는 것이 아니라 다양한 분야를 공부하여 융합하는 것이 중요하다고 생각합니다. 이번 양성과정의 커리큘럼은 구현된 암호 모듈을 분석하고 검증하는 과정, 암호 하드웨어 분석과 부채널 분석까지 포함되어 있는 것으로 알고 있습니다. 또한 암호가 적용되어 사용되는 제품에 원리나 응용을 배우고, 취약점을 분석하는 과정이 있습니다. 저는 암호 구현을 공부하고 있지만 구현된 암호가 어떻게 사용되거나, 또는 구현된 암호가 안전한지 분석하는 것에는 부족함이 있습니다. 이번 양성과정이 제가 공부하고 있는 분야의 연장선이라고 생각하기 때문에 더욱이 좋은 배움을 얻을 수 있을 것이라고 생각합니다.

마지막으로 양성과정을 통해서 같은 분야를 공부하고 있는 여러 사람들을 새롭게 만날 수 있는 좋은 자리라고 생각합니다. 대학원에서 공부하면서 혼자서 공부하는 것보다 여럿이서 공유하면서 공부할 수 있는 것이 굉장히 도움이 되는 것을 배웠습니다. 저와 다른 환경에서 같은 분야를 공부하고 계시는 다른 분들을 양성과정을 통해서 만나게 되면 서로에서 좋은 시너지가 될 거라고 생각하기 때문에 다양한 분들을 만나 즐거운 배움의 시간을 가질 수 있을 것이라고 생각합니다. 감사합니다.

2. 국내 암호 관련 대학/연구소/기관/산업계에 암호기술과 관련하여 바라는 점이 있으면 자유롭게 서술해 주십시오.

암호라는 분야가 인터넷이 굉장히 발달되고 주가 되는 현대에 굉장히 중요한 분야라고 생각합니다. 하지만 일반인들에게는 굉장히 생소하고 관심을 받지 못하는 분야라고 생각합니다. 보안이 굉장히 다양한 분야가 있지만 단순하게 '해킹'이라는 개념으로 보안을 생각하고 있는 분들이 많을 거라고 생각합니다. 보안에 다양한 분야와 중요성, 정확한 개념에 대해서 많은 분들이 알 수 있는 다양한 기회나 홍보가 있으면 좋겠다고 생각합니다. 암호 분야는 소수의 분들의 노력으로 지금까지 이어오고 우리나라의 암호 분야가 발전할 수 있었다고 생각합니다. 이런 소수의 분들이 좀 더 대우를 받고, 인정을 받을 수 있었으면 좋겠습니다. 감사합니다.