2023년 국가 암호기술 전문인력 양성과정(9기)

지 원 서

▣ 기본 인적사항

성 명	(한글) 심 민 주 (영문) Sim Min Joo		
성 별	여	생년월일	97. 6. 4.
휴대전화	010-7248-0087	Email	minjoos9797@gmail.com
소속(학교)	한성대학교	학과/전공	컴퓨터공학/정보보호
과정(년차)	박사(1년차)	지도교수	서 화 정

▣ 학력

학교명	기간 (월 단위까지)	평점	학과	전공	과정
한성대학교	2017.03~2021.02	3.66/4.5	융합공학	it융합공학	학사
한성대학교 대학원	2021.03~2023.02	4.06/4.5	it융합공학	it융합공학	석사
	(논문명) ARMv8 프로세서 상에서의 해시 함수 LSH 최적 구현				
	(소속Lab 및 지도교수명) CryptoCraftLab / 서화정 교수님				
한성대학교 대학원	2023.02~	/4.5	정 보 컴 퓨 터공학	정보시스템 공학	박사
	(논문명)				
	(소속Lab 및 지도교수명) CryptoCraftLab / 서화정 교수님				

* 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 구간의 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
	0편	1편	0편	1편	1편	18편	21편

※ 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	5건	5건

	대회/학회명 및 수상내용	공동수상자	당시 소속기관	수상 연월일
연구결과물 관련 수상실적	2022 국가암호공모전 특별상	엄시우, 송경주	한성대	22.10.20
	2022 정보보호학회 호남지부 학술대회 우수논문 수상	권혁동, 오유진, 송민호, 서화정	한성대	22.09.30
	2021년 경량 PIPO 대칭키 암호 경진대회 SCA 부문 부채널분석연구회 회장상	김현준, 엄시우	한성대	21.10.29
	2021 국가암호공모전 우수상	권혁동,김현준, 웨이 콩 리, 서화정	한성대	21.10.14
	2021 한국정보처리학회 충청지부 학술대회 우수논문상 2건	엄시우, 장경배, 송경주, 서화정	한성대	21.08.27
	2021 한국정보처리학회 춘계학술대회 우수논문상	엄시우,권혁동, 김현준,장경배, 김현지,박재훈, 송경주,서화정	힌성대	21.05.14
	제3회 부채널분석 경진대회 부채널분석연구회장상	엄시우, 송경주	힌성대	20.10.29
	2020 한국정보보호학회 호남지부 학술대회 우수논문	김현지,송경주, 임세진,서화정	한성대	20.10.23
	2020 국가암호공모전 장려상	김현지, 권용빈, 임세진	한성대	20.10.22
	2020 한국정보처리학회 춘계학술대회 우수논문	장경배, 서화정	한성대	20.05.29

[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 (0편)	"해당없음"				
SCIE (1편)	Optimized Implementation of Simpira on Microcontrollers for Secure Massive Learning	Symmetry	13page	22.12.10	엄시우, 권혁동, 장경배, 김현준, 김현지, 송경주
국제저널 논문집 (0편)	"해당없음"				
국내저널 논문집 (1편)	사물인터넷 상에서의 블록체인 기술 동향	정보보호학회 논문지	pp 5-16	22.04.30	강예준, 김원웅
국제 학술대회 (1편)	K-XMSS and K-SPHINCS+: Hash based Signatures with Korean Cryptography Algorithms	MobiSec'22	5page	22.12.15	엄시우, 송경주, 양유진, 김원웅
국내 학술대회 (18편)	경량 블록 암호 SIMON 최적 구현 연구 동향	정보보호학회 동계학술대회	4page	22.11.26	권혁동, 송민호, 김동현

국내 학술대회 (18편)	저사양 프로세서 상에서의 경량 블록암호 SIMECK 최적 구현 동향	정보처리학회 추계학술대회	3page	22.11.05	이민우, 김동현, 운세영
	Intel SIMD를 활용한 해시 함수 LSH 최적 구현 연구 동향	정보보호학회 충청지부 학술대회	4page	22.10.14	권혁동, 김현준
	ARMv8 상에서의 Fault Attack에 안전한 블록 암호 최적 구현 연구 동향	정보보호학회 영남지부 학술대회	4page	22.10.06	권혁동, 엄시우
	32-bit RISC-V 프로세서 상에서의 경량 블록 암호 SIMECK-CTR 최적 구현	정보보호학회 호남지부 학술대회	4page	22.09.22	권혁동, 오유진, 송민호
	32-bit RISC-V 프로세서 상에서의 경량 블록암호 SIMECK 최적 병렬 구현	정보보호학회 하계학술대회	4page	22.06.17	엄시우, 권혁동
	ARMv8 상에서의 블록 암호 최적 구현 동향	정보처리학회 춘계학술대회	4page	22.05.21	권혁동, 김현준
	32-bit RISC-V 프로세서 상에서의 경량 블록암호 Revised CHAM 최적 병렬 구현	정보보호학회 동계학술대회	4page	21.11.27	장경배, 엄시우
	32-bit RISC-V 프로세서 상에서의 초경량 블록암호 알고리즘 Revised CHAM 구현	정보처리학회 추계학술대회	4page	21.11.04	엄시우
	32-bit RISC-V processor 상에서의 블록 암호 구현 동향	정보보호학회 호남지부 학술대회	4page	21.11.05	권혁동
	Simple PQ-Fabric : 블록체인 상에서 양자내성 암호로 안전하게 전이하는 프로토콜 설계	정보보호학회 충청지부 학술대회	4page	21.08.27	장경배
	딥러닝 기반 논프로파일링 부채널 분석 기술 연구 동향	정보보호학회 하계학술대회	4page	21.06.24	김현준, 송경주
	국산 경량 암호 PIPO에 대한 부채널 분석과 마스킹 기법 제안	정보처리학회 춘계학술대회	4page	21.05.17	김현준
	경량 블록 암호 PIPO에 대한 상관관계 전력분석 공격	정보보호학회 영남지부학술대회	3page	21.02.22.	김현준
	딥러닝 기반의 부채널 분석 기술 연구 동향	정보보호학회 동계학술발표대회	4page	20.11.30	김현지
	블록체인을 활용한 공유 전동킥보드 시스템 제안	정보보호학회 호남지부학술대회	3page	20.10.23	김현지

국내 학술대회 (18편)	스마트폰과 스마트워치를 활용한 2차 사용자 인증 방식 제안	한국정보보호학회 하계학술발표대회	4page	20.07.15.	엄시우, 김현지
	블록체인을 통한 키오스크 스마트 체크인 방식 제안	한국정보처리학회 춘계학술발표대회	3page	20.05.30	최승주
기타	32-bit RISC-V 프로세서 상에서의 경량 블록 암호 SIMECK, SIMON 카운터 운용 모드 최적 구현	정보보호학회 논문지	10page	게재예정	권혁동, 오유진, 송민호

▣ 특 허

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

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

▣ 연구과제(프로젝트) 수행실적

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

발주처	연구과제명	참여형태 (참여율)	수행기간	당시 소속기관
국가보안기술연구소	KpqC 공모전 알고리즘 구현을 통한 성능 비교 분석 기술 연구	참여연구원 (11%)	23.04.01~현재	한성대학교
IITP	저사양 디바이스 지원을 위한 경량 사물 블록체인 네트워크 기술개발	참여연구원 (15%)	2022.04~2024.12	한성대학교
IITP	GPU/ASIC 기반 암호 알고리즘 고속화 설계 및 구현 기술 개발	참여연구원 (30%)	2021.04~현재	한성대학교
IITP	IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구	참여연구원 (30%)	2020.01~현재	한성대학교
IITP	미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술 개발	참여연구원 (25%)	2020.01~현재	한성대학교

자 기 소 개 서

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

저는 학부 4학년이었을 때, 부채널 분석에 처음 접하였습니다. 학부 연구생을 하면서 부채널 분석에 대한 이론 공부를 하였고, 부채널 분석 경진대회가 있다는 것을 알게 되어 팀원들과 경진대회에 참가하게 되었습니다. 참가 당시 팀원들과 수집된 파형의 어느 부분에 대해 분석하는 것이 적합한지에 대해 계속 의견을 공유를 하면서 파형에 대해 분석을 하는 기회를 얻게 되었습니다. 결과적으로, 팀원들과 학부생 부문에서 부채널분석연구회장상을 수상할 수 있었습니다. 이론적으로 공부만 하고 있었던 분야인 부채널 분석을 해당 대회를 통해 직접 파형을 분석해 보면서 흥미가 생겼습니다. 그 후 대학원에 입학하여 석사 1학기까지 국산 암호에 대한 부채널 분석 연구를 하였습니다. ChipWhisperer Lite를 사용하여 국산 블록 암호 알고리즘(AES, PIPO 등)에 대해 파형을 수집하고 수집된 파형에 대해 CPA(Correlation Power Analysis) 공격을 수행하여 비밀키 값을 유추하는 과정과 그 비밀키를 유추하지 못하게 키값을 마스킹하는 기법을 적용하는 연구를 진행하였습니다. 계속 연구를 진행하면서 팀원들과 2021년 경량 PIPO 대칭키 암호 경진대회 SCA 부문 부채널분석연구회 회장상을 수상하는 좋은 결과도 얻을 수 있었습니다.

하지만, 부채널 분석 연구를 진행하면서 암호 고속 구현에 더욱 관심이 생겨 연구 분야를 석사 2학기부터 암호 구현으로 연구 분야를 변경하여 박사 1학기인 현재까지 암호 구현 연구를 하고 있습니다.

저의 첫 암호 고속 구현 연구는 32-bit RISC-V 상에서의 CHAM 암호 고속 구현이었습니다. CHAM 암호 알고리즘은 사물인터넷에 사용하기 효율적인 국산 경량 블록 암호 중 하나입니다. 저사양 프로세서 중 하나인 32-bit RISC-V 프로세서 상에서 Revised CHAM에 대해 CHAM 암호 알고리즘의 구조적 특징에 따라 1~4 라운드에 대해 (1, 3) 라운드와 (2, 4) 라운드를 병렬하여 암호화하는 라운드 동시성 기법을 제안하였습니다. 이를 단순하게 표현하면 CHAM의 라운드를 절반으로 줄인 단일 평문 병렬 구현 기법을 제안하였습니다. 연속된 라운드에 대해 값이 서로 의존적이지 않아, 짝수 라운드와 홀수 라운드 별로 동일 연산을 진행하는 CHAM의 구조적 특징을 활용하였습니다. 그리고 16-bit 단위의 블록으로 연산이 진행되기 때문에 32-bit의 레지스터를 갖고 있는 RISC-V 프로세서에서 레지스터 하나에 16-bit 단위의 블록 하나만 동작되게 구현되는 것은 비효율적이기 때문에 2개의 평문에 대한 병렬 구현 기법을 제안하였습니다. 서로 섞이지 않아야하는 16-bit 값 두 개가 한 개의 32-bit 레지스터에 저장되어 있기 때문에 두 개의 기법에 대해 올바른 로테이션 연산과 덧셈 연산을 구현하였습니다. 이러한 기법들을 활용하여 경량 블록 암호인 SIMECK, SIMON, SPECK 등에 해당하는 경량 블록 암호에 대한 고속 최적 병렬 구현 연구를 하였고, 해당 결과 국내 학술대회에서 수상할 수 있었습니다.

두 번째 진행한 연구는 Simpira permutation을 AVR과 RISC-V 상에서 고속 구현을 진행하였습니다.

Simpira permuation은 AES 라운드 함수를 활용하는 특징을 가지고 있기 때문에 AVR과 32-bit RISC-V상에서의 AES 선행 연구들을 활용하여 Simpira permutation을 최적 구현하였으며, 해당 결과를 SCIE 논문으로 게재할 수 있었습니다.

그다음으로는 국내에서 진행한 KpqC 공모전에 해시함수인 XMSS와 SPHINCS+ 내부에 사용되는 해시함수를 국산 해시함수로 변경하는 K-XMSS/K-SPHINCS를 제안을 하였습니다. 비록 결과는 좋지 않았지만, 그 공모전을 계기로 해시 함수에 관심이 생겨 64-bit ARMv8 상에서 국산 해시함수 LSH를 최적화하는 연구를 진행하여 석사 졸업 논문으로 발표하였습니다. 64-bit ARMv8 프로세서에는 효율적으로 병렬 구현이 가능하게 하는 벡터 레지스터가 존재합니다. 벡터 레지스터를 활용하여 LSH-256과 LSH-512에 대한 싱글 메시지 최적화 구현과 LSH-256에 대한 멀티 메시지 최적화 병렬 구현 연구를 하였습니다. LSH의 ARX 연산에 대한 병렬 구현을 하였고, Wordperm 함수와 메시지 확장 함수에서 수행되는 순열을 구현하기 위해서는 많은 벡터 명령어가 필요하여 싱글 메시지 최적화 구현에서 Wordperm과 메시지 확장함수에 대해 최적화하였습니다. 멀티 메시지에 대한 최적화 병렬 구현은 레지스터 내부 정렬을 통해 서로 다른 2개의 메시지에 대해 LSH-256을 병렬 구현하였습니다. 이 과정에서 메시지 확장 함수에서 수행되는 덧셈 연산을 기존의 절반으로 생략하는 최적화 연구를 하였습니다.

그리고 64-bit ARMv8 프로세서 상에서의 LSH 구현 연구를 수행하면서, 64-bit ARMv8 프로세서 상에서 NIST PQC 4라운드 후보군 암호 중 코드 기반 암호인 Classic McEliece에 대해 Encapsulation과 Decapsulation 과정의 일부에 대해 최적 구현 연구를 수행하였고, 2022 국가암호공모전 특별상 수상을 할 수 있었습니다. 현재, Classic McEliece Decapsulation의 BM 알고리즘에 대한 최적 구현 연구를 수행 진행하고 있고 있습니다. 그리고 향후, ARMv8 상에서 PQC에서 주로 사용되고 있는 곱셈기(몽고메리 곱셈, NTT 곱셈 등)에 대해 연구하여 기존 알고리즘들에 사용되고 있는 곱셈기를 좀 더 빠른 곱셈기로 변경하는 최적 구현 연구를 수행하려고 합니다.

제가 전문 인력 양성 과정에 참여하게 된다면, 암호기술 전문 인력 양성과정을 통해 다른 연구실분들과의 교류와 암호기술 분야의 최고 전문가분들에게 배움을 받고 싶습니다. 다른 연구실분들과 교류를 가질 기회가 원래도 적었지만 코로나로 인해 학술대회와 여러 워크숍들도 온라인으로 변경되어 제가 대학원 입학을 한 후에는 더욱 그러한 기회가 없어졌습니다. 따라서, 저는 암호기술 전문 인력 양성과정을 통해 다른 연구실 분들과의 교류를 통해 많은 소통하고, 암호 기술 분야의 전문가분들에게 배움을 받으면서 함께 성장해 나가고 싶습니다. 그리고 인력 양성과정을 참여하셨던 연구실 선배님들의 후기를 통해 제가 열심히 노력을 한다면, 그만큼의 많은 것을 인력 양성과정을 통해 배울 수 있다는 것을 알 수 있었습니다. 만약 제가 양성 과정에 참여할 수 있는 기회가 주어진다면, 다양한 사람들과의 교류를 통해 인력 양성과정이 끝난 이후에도 그분들과 다른 연구를 같이 하게 된다면 좋은 시너지가 있을 것으로 생각됩니다.

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

양자컴퓨터의 급격한 발전으로 기존에 사용되고 있는 암호가 취약하기 때문에 이에 대한 대응책은 필수적입니다. 따라서, 국내에서 KpqC 공모전이 진행되고 있습니다. 양자컴퓨터를 실생활에서 사용할 수 있을 미래에 주로 사용될 암호는 현재 2라운드가 진행 중인 KpqC 공모전을 통해 선발된 암호가 사용될 것으로 생각됩니다.
하지만, 아직 PQC보다 KpqC 2라운드에 진출한 암호 알고리즘에 대해서는 많은 관심이 더욱 필요하다고 생각됩니다. 따라서, 국내 대학, 연구소, 산업계에서 KpqC 2라운드에 진출한 암호 알고리즘에 대해 많은 관심을 갖고 이에 대해 연구를 하여 해당 연구를 발표하여 교류하는 세미나가 많이 진행되면 좋을 것 같습니다. 해당 세미나를 통해 KpqC에 대한 관심이 NIST PQC를 통해 선발된 암호 알고리즘만큼 높아지고 중요성이 더욱 부각될 것 같다고 생각됩니다. 감사합니다.