//hyu.wiki/%EC%98%A4%ED%98%84%EC%98%A5

오현옥

오현옥은 서울캠퍼스 공과대학 정보시스템학과 교수이자, 보안 및 프라이버시 연구실장을 겸임하고 있다.

2020년 영지식증명(Zero-Knowledge Proof, ZKP) 기술을 활용한 블록체인 프라이버시 보장과 확장성을 제공하는 응용 서비스 사업 회사인 '지크립토(Zkrypto)'를 창업했다.

- 02-2220-2395
- hoh@hanyang.ac.kr
- ITBT관 807호

정보시스템학과 홈페이지 참고(2020.10)

□

목차

학력

- Ph.D. in Computer Engineering, Seoul National University, Korea, 2003
- M.S. in Computer Engineering, Seoul National University, Korea, 1998
- B.S. in Computer Engineering, Seoul National University, Korea, 1996
- Seoul Science High School, Korea, 1992

경력

- Sep. 2008 Present : Professor, Hanyang University, Korea
- Jul. 2014 - Jun. 2015 : Visiting scholar, ASU, AZ, USA
- Dec. 2005 Aug. 2008 : Staff Software Engineer, ARM Inc. Irvine CA,USA
- Sept. 2003 Nov. 2005 :Post Doctoral Researcher, UC Irvine, CA, USA
- Mar. 2003 Sept. 2003 :Post Doctoral Researcher, Research Institute of Advanced Computer Technology, Seoul, Korea

연구

관심 분야: 암호학,보안, 내장형 시스템, 비휘발성 메모리, 컴파일러, 실시간 시스템; Cryptography, security, embedded system, nonvolatile memory , compiler, real-time system

검증형 인공지능(Verifiable AI) 기술 ‘vCNN’ 개발[1]

- 영지식증명(zk-SNARKs)을 활용해 입력과 모델을 공개하지 않은 채 ‘AI가 규정 절차대로 정확히 계산했다’는 사실만을 짧고 간결한 증명으로 제공. 특히 CNN의 핵심 연산인 합성곱(convolution) 증명 방식을 새롭게 설계해 기존 O(l · n)(커널 크기 l, 데이터 크기 n)이던 복잡도를 O(l + n)으로 줄임. 그 결과 MNIST 모델에서 약 20배, VGG16 모델에서 약 1만8,000배의 증명 속도 향상을 달성했으며, 보안성 또한 수학적으로 입증
- 과학기술정보통신부 및 정보통신기획평가원(IITP) 사업의 지원을 받아 수행됐으며, 논문 「vCNN: Verifiable Convolutional Neural Network Based on zk-SNARKs」에는 국민대 이승화 박사가 제1저자, 한양대 고한경 박사가 참여자, 한양대 오현옥 교수와 국민대 김지혜 교수가 공동 교신저자로 참여
- 과학기술정보통신부 및 정보통신기획평가원(IITP) 사업의 지원을 받아 수행됐으며, 논문 「vCNN: Verifiable Convolutional Neural Network Based on zk-SNARKs」에는 국민대 이승화 박사가 제1저자, 한양대 고한경 박사가 참여자, 한양대 오현옥 교수와 국민대 김지혜 교수가 공동 교신저자로 참여

수상

- 2025:『IEEE Transactions on Dependable and Secure Computing(이하 TDSC)』의 2024년 Best Paper Award (최우수논문상)
- 2023: 창업기업 '지크립토' CES 최고 혁신상
- 2019: 국가암호공모전 특별상: 이지원, 김지혜, 오현옥, "QAP-based Simulation-Extractable SNARK with a Single Verification"
- 2018: 한국정보과학회 동계학술대회 우수논문상: 김동혁, 김지혜, 오현옥, "전방향 안전 서명을 보장하는 Proof of Elapsed Time"
- 2018: 국가암호공모전 장려상: 이승화, 김지혜, 오현옥, "E cient Zero-Knowledge Succinct Non-interactive Argument of Knowledge for Convolution operations"
- 2018: 국가암호공모전 특별상: 이지원, 김지혜, 오현옥, "BESTIE: Broadcast Encryption Scheme for Tyny IoT Equipments"
- 2018: KCC2018 라인X한국정보과학회 블록체인 경진대회 장려상: 이정혁, 김예지, 오현옥, "비밀선거를 보장하는 블록체인 기반 전자투표 시스템"
- 2018: 한국컴퓨터종합학술대회 우수논문상: 이정혁, 김예지, 조수연, 오현옥, 김지혜, "전방향 안전서명을 사용하는 빠른 블록체인"
- 2017: 국가암호공모전 특별상: 이지원, 오현옥, 이승화, 김지혜, "Wildcard Based Identity Based Encryption with Constant Size Ciphertext"
- 2017: 고한경, 오현옥, KSC 2017 SW 구현/데모 경진대회 대학원생 부문 장려상
- 2017: 고한경, 박사로, 윤정준, 유영천, 오현옥, 김지혜, EDA Summer Workshop Student Poster Presentation 3rd Place
- 2017: 고한경, 박사로, 윤정준, 유영천, 오현옥, 김지혜, Embedded System Design Challenge 2nd Place
- 2016: 국가암호공모전 우수상: 이지원, 오현옥, 이승화, 김지혜, Combnatorial Subset Difference Public Key Broadcast Encryption Scheme"
- 2016: 한국을 빛내는 서울공대 박사 70인
- 2016: 한국컴퓨터종합학술대회 우수논문상: 윤정준, 이정혁, 김지혜, 오현옥, "최소 보안 연산을 가지는 전방향 보안 전자서명"

- 2014: Best lecturer (강의 우수 교수) from Hanyang University
- 2003: Best paper from Samsung on SOC (System on Chip) Design Conference 2003
- 1998: A prize at the 8th Korean National Programming Contest
- 1996: Awarded by the head of Alumni Association of Engineering School at Seoul National University for graduation with the highest honor at the department of Computer Engineering
- 1996: Awarded by the president of Seoul National University for graduation with the highest honor at the department of Computer Engineering
- 1989: Silver medal at the 3rd Korean Mathematical Olympiad

교내 매체

- <뉴스H> 2021.10.28 익명·효율·신뢰성 보장, 미래 대변혁 이끌 블록체인 기술

1. ↑ <뉴스H> 2025.08.14 한양대·국민대 연구팀, 검증형 인공지능 기술 'vCNN'로 IEEE TDSC 2024 최우수논문상 단독 수상