

FHE-School 2025

박재현

크립토랩 FHElab

프로그램 개요

동형암호 집중 연구 프로그램

- ① 연구에 필요한 내용만 속성으로 기초 내용 학습
- ② 흥미에 맞추어 연구에 필요한 선행 연구를 공부
- ③ 인턴 진행 및 논문 작성 후 제출

⇒ 단기간에 동형암호 연구자 양성

동형암호 (Homomorphic Encryption)

(완전)동형암호 ((Fully) Homomorphic Encryption)

암호화된 상태에서 연산할 수 있는 암호.

두 개의 암호문 $ct_1 = \text{Enc}(m_1)$, $ct_2 = \text{Enc}(m_2)$ 에 대해

$$\text{Dec}(ct_1 + ct_2) = m_1 + m_2$$

$$\text{Dec}(ct_1 \times ct_2) = m_1 \times m_2$$

를 만족하는 암호.

⇒ (Ring)-Homomorphic Encryption

동형암호 (Homomorphic Encryption)

Why 동형암호?

- 사용자의 정보를 유출하지 않으면서 데이터를 처리할 수 있는 기술
- 우리나라가 기술적으로 경쟁력을 가지고 있는 분야
- 상대적으로 적은 배경지식으로도 연구를 시작할 수 있음
- 연구에 대한 수요보다 공급이 적은 블루오션

서울대학교 10-10 & 크립토랩

동형암호 분야 최고 수준 연구팀

- 2024년: Crypto, Eurocrypt, Asiacrypt (2편), CCS (4편) 등
- 2023년: Crypto, CCS, ICML 등

최고 수준 동형암호 라이브러리 (HEaaN)

- CPU 및 GPU 최적화
- 최신 동형암호 알고리즘 포함

강사 소개

주 강사: 박재현 (크립토랩 FHElab)

크립토랩 FHElab에서 2024년 9월부터 근무 중.

서울대 수리과학부 박사 (전공: 동형암호).

주로 동형암호 가속 관련 연구를 수행.

서울대 조교, ENS Lyon 강사 등 강의 경험 다수.



Phase I (동형암호 기초 이론 교육)

온라인/현장/녹화 방식의 강의로 진행 (2시간씩 주당 3회)

① 동형암호의 기초 및 응용

- 암호학 및 보안 기술
- 동형암호 개념 및 스킴 소개
- 동형연산 및 동형재부팅
- 동형암호 응용

② 동형암호 구현 실습

- 동형암호 라이브러리 사용법 설명
- 동형암호 기초 응용 구현

Phase I → Phase II:

중간평가 (필기시험, 절대평가)

Phase II (동형암호 심화 이론 교육 및 실습)

실제 동형암호 응용 공부 및 구현

① 선행 연구 공부 및 리딩 세미나

- 페이즈 시작 시 연구 주제 선정 (e.g. 가속화/기계학습/보안)
- 비슷한 분야끼리 묶어 소그룹 형성 후 협력하여 학습

② 구현

- HEaaN 라이브러리를 통해 각자 주제 구현
- 대면/비대면으로 멘토와의 질의응답

Phase II → Phase III:

구현 결과 발표

Research Proposal 및 연구 기관 지원

Phase III (파트타임 인턴)

서울대 혹은 크립토랩 중 하나로 배정되어 연구 진행 (급여 지급).

① 서울대학교 수리과학부 암호학 연구실 (천정희 교수님):

- 이론 위주의 연구 진행
- 서울대학교 자연과학대학 27동

② 크립토랩 동형암호팀:

- 응용 및 구현 위주의 연구 진행
- 서울대학교 자연과학대학 501동

Phase III 동안 혹은 그 이후까지 논문 작성 후 국가암호공모전 및 분야의
탑 컨퍼런스/저널에 제출하는 것이 목표.

Phase III (파트타임 인턴)

연구 가능 주제

- ① 동형암호 가속화
 - 알고리즘 가속화, 하드웨어 가속화
- ② 동형암호 응용
 - 동형암호 기반 기계학습, 통계, 데이터베이스, 위치기반서비스 등
- ③ 동형암호와 보안
 - 암호학적 안전성, 보안적 안전성
- ④ 동형암호 시스템
 - 동형암호 컴파일러 등

Phase IV (풀타임 인턴)

- ① 서울대학교 수리과학부 암호학 연구실 (천정희 교수님)
- ② 크립토랩 동형암호팀
- ③ FHElab (크립토랩 프랑스 연구 지사):
 - 위치: 프랑스 리옹 중앙역 부근
 - Damien Stehlé, Guillaume Hanrot, Alain Passelègue, Jai Hyun Park
 - 추천 받은 우수성과자에 한하여 선발

논문 제출 컨퍼런스 예시: Eurocrypt, IEEE S&P, USENIX Security, etc.

마치며



- 동형암호는 수학 및 컴퓨터 과학 전반이랑 맞닿아 있는 매력적인 분야
- 단기간에 이론부터 연구까지 전과정을 경험하는 흔치 않은 기회



감사합니다

fheschool2357@gmail.com