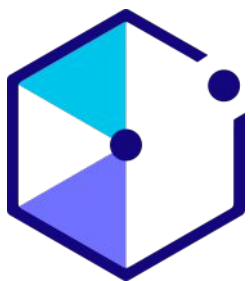


창의적 통합설계 과제 소개

# Multi-layer Perceptron (MLP) with Homomorphic Encryption

김정우 (jungwoo.kim@cryptolab.co.kr)

2023. 09. 01



## TABLE OF CONTENTS

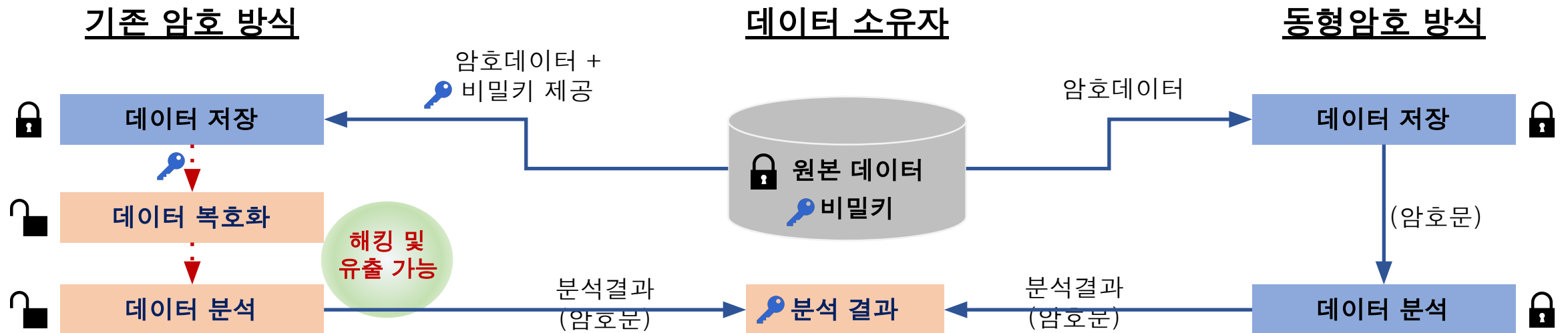
- Chapter 1 동형암호 및 크립토랩
- Chapter 2 MLP with Homomorphic Encryption



# 동형암호

동형암호는 안전한 분석 기술

- 데이터를 암호화한 상태에서 연산하여 데이터 유출 위험 없이 데이터를 분석할 수 있는 최신 암호화 기술





# 크립토랩

원천특허를 보유한 동형암호 Global 1위 기업

- 2009년 등장한 동형암호는 연산의 속도·범위·정확도를 높이는 방향으로 발전
- 크립토랩은 실수 연산이 가능한 CKKS 알고리즘을 개발
- Privacy-preserving Machine Learning 분야에 적용 및 연구

[4세대 동형암호 기술- CKKS]

|       | 1세대 ('09~'11)  | 2세대 ('11~'13)<br>CKKS<br>(BGV, BFV)   | 3세대 ('13~'16)<br>(CGGI)   | 4세대 ('16~)<br>(CKKS)  |
|-------|--|---|---|---|
|       | <ul style="list-style-type: none"> <li>최초의 완전동형암호</li> <li>연산 종류·횟수 제한이 없는 완전동형암호</li> </ul> | <ul style="list-style-type: none"> <li>최초의 사용 가능한 동형암호</li> <li>정수 연산 가능</li> </ul> | <ul style="list-style-type: none"> <li>소용량 데이터 처리에 효과적인 동형암호</li> <li>평문을 1bit로 제한하는 대신 빠른 재부팅</li> </ul> | <ul style="list-style-type: none"> <li>최초의 실수 연산을 지원하는 동형암호</li> <li>암호화 상태에서 반올림 연산이 가능</li> </ul> |
| 연산 속도 | 동형암호 핵심 연산* 속도 (상용화의 핵심)<br>- 최근 연간 8배씩 개선 추세  | 1-bit 처리<br>1,800 초   | 1-bit 처리<br>0.3초  | 1-bit 처리<br>19 $\mu$ s ('19)<br>0.28 $\mu$ s ('21)  |
| 연산 범위 | 동형암호 기반 연산 가능한 데이터 형태<br>- 실수 연산 가능여부가 상용화의 핵심   | 정수 연산만 가능<br>(실수 연산이 불가능하여, 상용화 범위 매우 제한적)  |   |   |
|       |  | 실수 포함 모든 연산이 가능   |   |   |

[글로벌 동형암호 라이브러리의 CKKS 활용]

| Library  | Org.      | 지원 Scheme |     |      |      |
|----------|-----------|-----------|-----|------|------|
| Helib    | IBM       | BGV       | BFV | CGGI | CKKS |
| SEAL     | Microsoft | BGV       | BFV | CGGI | CKKS |
| Palisade | Duality   | BGV       | BFV | CGGI | CKKS |
| Lattigo  | EPFL      | BGV       | BFV | CGGI | CKKS |

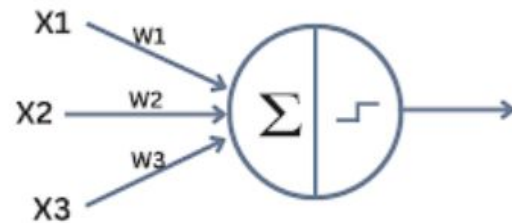
홈페이지 : <https://www.cryptolab.co.kr/>



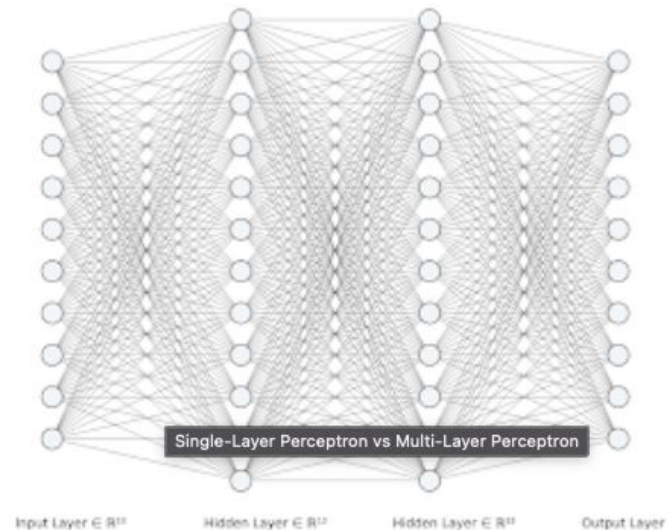
# MLP with Homomorphic Encryption

## 배경

- MLP
  - MLP 구현에 필요한 연산
    - Matrix multiplication + Activation
  - 동형암호가 지원하는 연산
    - Element-wise addition & multiplication



Single-layer perceptron



Multi-layer perceptron



## MLP with Homomorphic Encryption

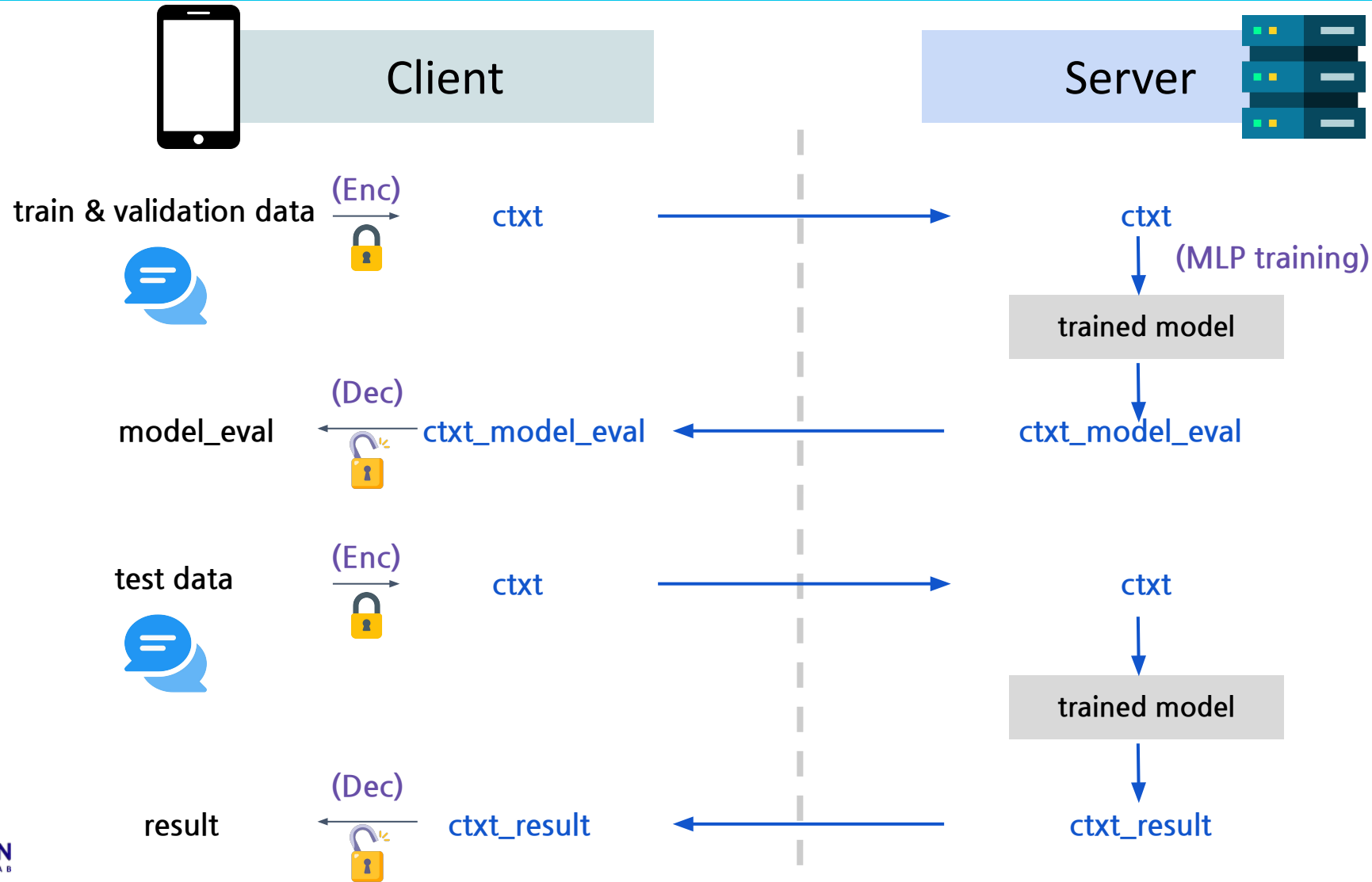
### 개발 및 연구

- 동형암호 적용한 MLP
  - **Matrix multiplication + Activation**
    - HETAL: Efficient Privacy-preserving Transfer Learning with Homomorphic Encryption, ICML '23
      - 효율적인 Matrix multiplication & Softmax 알고리즘 제안 (1-layer)
  - **Multi-layer로 확장**
    - # layers  $\geq 2$
    - 비선형함수의 근사함수 검증
    - Training & Inference 구현 확장



# MLP with Homomorphic Encryption

개발 및 연구 (optional)





## MLP with Homomorphic Encryption

### 개발내용 및 필요지식

- 개발내용
  - HETAL 논문의 행렬곱, softmax 구현 학습
  - 이를 이용한 MLP 구현 - 괜찮은 결과가 나올 경우, 추후 논문 출판 목표
  - (Optional) MLP를 이용한 간단한 AI 서비스 구현
- 필요지식
  - Python 언어
  - 동형암호 (기업에서 교육) & HETAL, ICML '23 논문 이해
  - MLP training & inference





# QnA

- 크립토랩 : [www.cryptolab.co.kr](http://www.cryptolab.co.kr)
- 신준범 CTO/ [junbum.shin@cryptolab.co.kr](mailto:junbum.shin@cryptolab.co.kr)
- 김정우 팀장/ [jungwoo.kim@cryptolab.co.kr](mailto:jungwoo.kim@cryptolab.co.kr)