창의적 통합설계 과제 소개

Multi-layer Perceptron (MLP) with Homomorphic Encryption

김정우 (jungwoo.kim@cryptolab.co.kr)

2023. 09. 01

HEAAN CRYPTO LAB

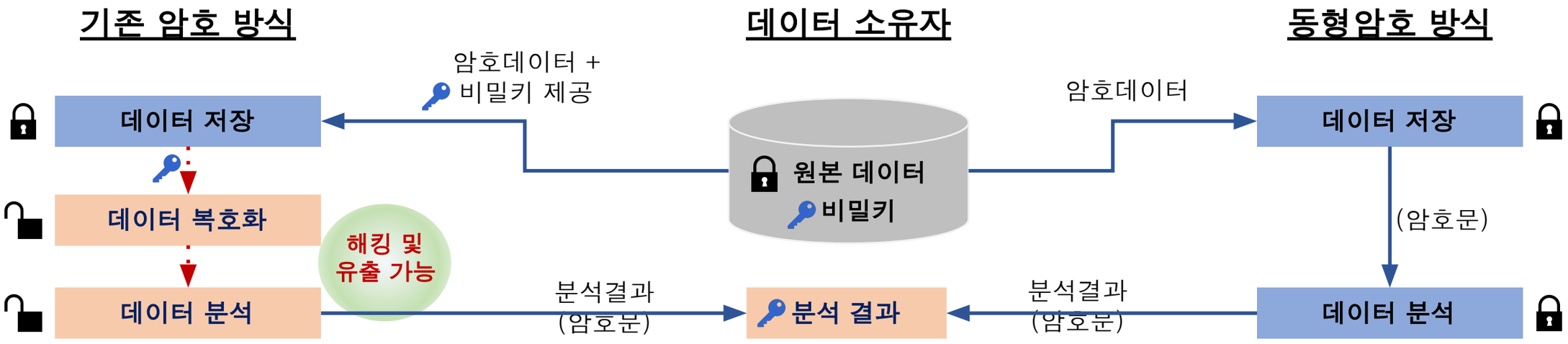
CRYPTO LAB
주식회사 크립토랩

TABLE OF CONTENTS

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]

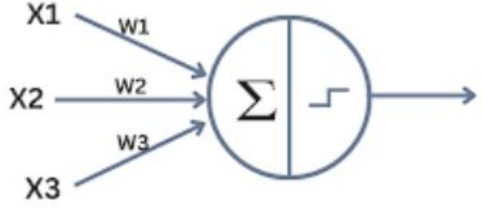
[글로벌 동형암호 라이브러리의 CKKS 활용]

홈페이지 : https://www.cryptolab.co.kr/

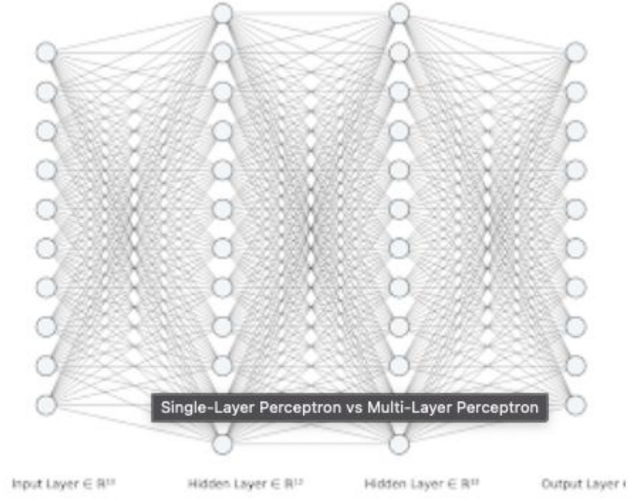
MLP with Homomorphic Encryption

배경

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



Single-layer perceptron



Multi-layer perceptron

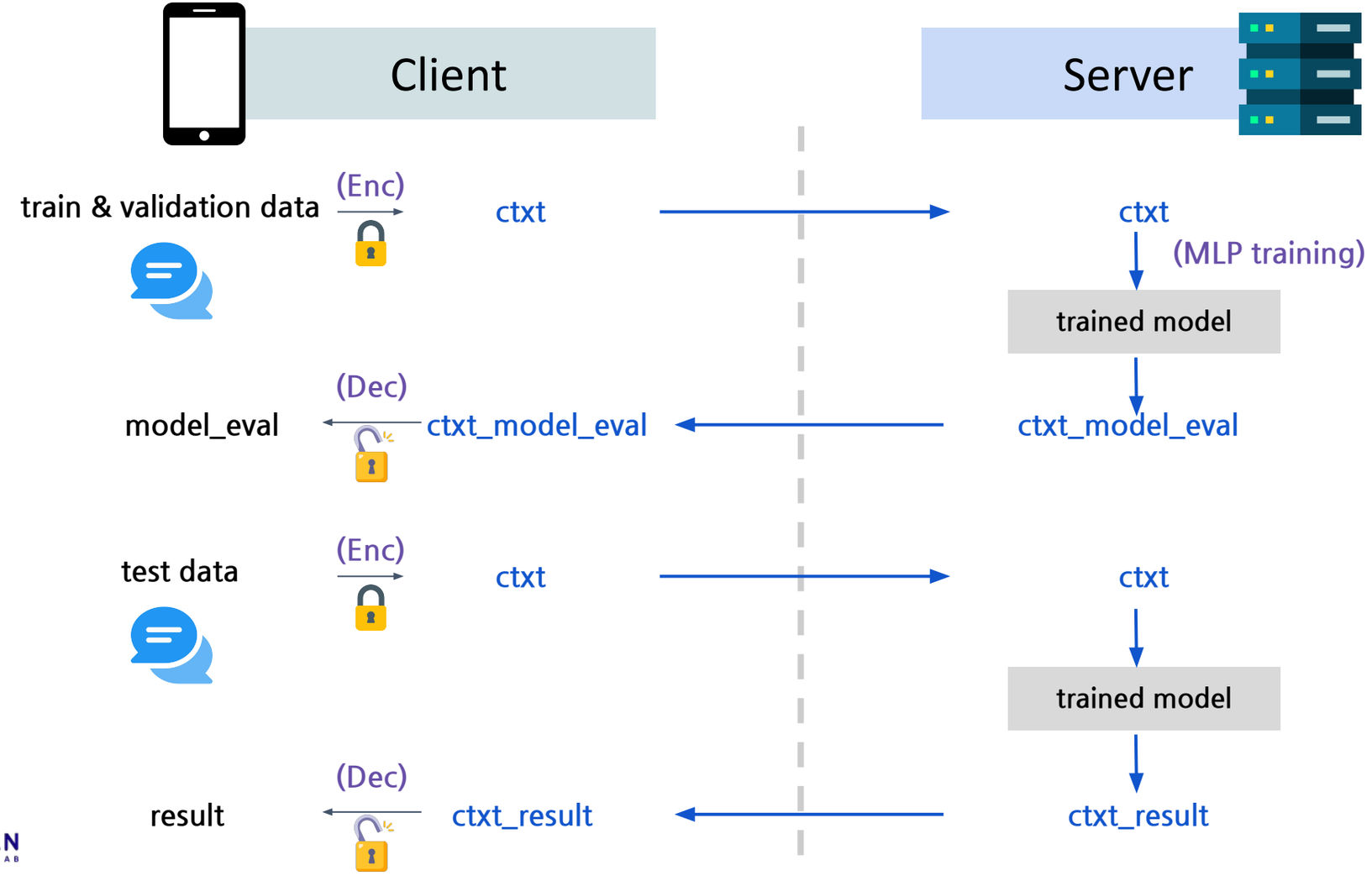
MLP with Homomorphic Encryption

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 ≧ 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
- 신준범 CTO/ junbum.shin@cryptolab.co.kr
- 김정우 팀장/ jungwoo.kim@cryptolab.co.kr