동형암호 기반 연합학습에서 희소화 기법의 효율성 평가

국지형, 이은상
세종대학교

jkook30@gatech.edu, eslee3209@sejong.ac.kr

Efficiency Evaluation of Sparsified Homomorpic Encryption in Federated Learning

Kook Jihyung, Lee Eunsang
Sejong Univ.

요 약

연합학습(Federated Learning)은 각 클라이언트가 자체 데이터를 로컬에서 학습하고, 중앙 서버가 모델 가중치(weight)를 수집·통합하여 글로벌 모델을 갱신함으로써 원시 데이터 공유 없이 학습을 가능하게 한다. 동형암호(Homomorphic Encryption)는 암호문 상태에서의 연산·집계를 지원하여 학습 과정의 추가적 노출을 방지한다. 그러나 연합학습과 동형암호는 각각 통신량과 계산량 증가라는 한계를 가진다. 본 논문에서는 이러한 효율 저하를 완화하기 위해 동형암호 기반 연합학습에 희소화(Sparsification)를 결합하고, MNIST 데이터셋을 기반으로 그 성능을 정량적으로 평가하는 것을 목적으로 한다. 우리는 (i) 평문 기반 연합학습, (ii) 동형암호 기반 연합학습, (iii) 동형암호에 희소화 기법을 적용한 연합학습의 세 조건을 비교하였다. 실험 결과, 평문 대비 동형암호 기반 연합학습은 수행 시간이 2.8 배 증가(75.7s → 214.1s) 하고, 통신량이 약 13.2 배 증가 (166MB → 2,198MB) 하였다. 그러나 동형암호 대비 동형암호에 희소화 기법을 적용한 연합학습은 수행 시간이 약 1.6 배 감소 (214.1s → 133s) 하고, 통신량이 약 4.3 배 감소 (2,198MB → 512MB) 하였다. 정확도 측면에서는 평문 대비 동형암호 기반 연합학습은 약 3.8%p 감소 (98.9% → 95.1%) 했으나, 희소화를 적용했을 때는 동형암호 대비 정확도가 소폭 감소 (95.1 → 93.9%)하는 수준으로 유지되었다.

Ⅰ. 서 론

연합학습 (Federated Learning, FL)은 원시 데이터 공유 없이 각 클라이언트의 로컬 학습 결과를 중앙 서버에서 집계해 글로벌 모델을 갱신함으로써 프라이버시 위험을 줄인다. 그러나 모델 업데이트 자체도 민감 정보를 노출할 수 있어, 이를 보호하기 위해 동형암호 (Homomorphic Encryption, HE)를 활용한 다양한 연구가 제안되고 있다.

동형암호는 암호문 상태에서의 연산과 집계를 가능하게 하여 추가적인 정보 노출을 차단하지만, 연산량과 통신량이 크게 증가한다는 한계를 가진다. 반면, 연합학습 자체도 클라이언트 수와 모델 크기에 따라 통신 부담이 크다는 점에서 효율성 문제가 중첩된다. 따라서 동형암호 기반 연합학습 구조는 프라이버시 강화라는 장점을 제공하는 동시에, 실용성을 제한할 수 있는 병목을 초래할 수 있다.

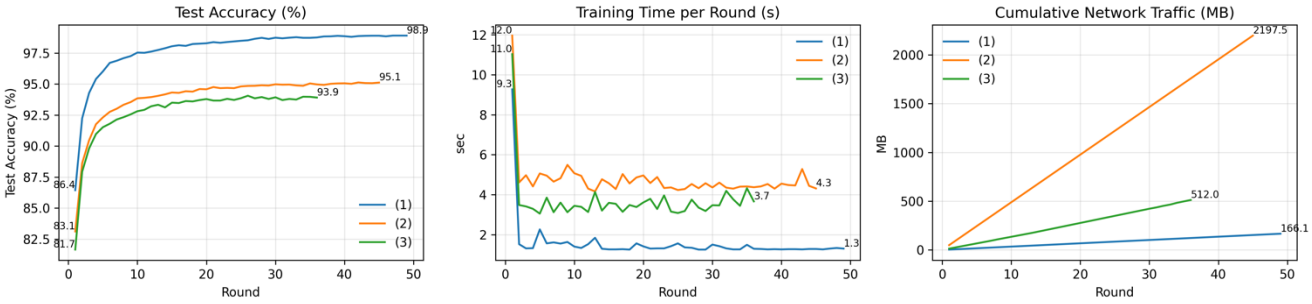
이를 해결하기 위한 대표적인 접근이 희소화(Sparsification, Spars) 기법이다. 희소화는 모델 업데이트 중 중요한 파라미터만을 선택적으로 전송하여 통신량을 줄이는 방식으로, 연합학습의 통신 부담 완화와 동형암호의 연산 효율 개선 모두에 기여할 수 있다. 대표적인 방법으로는 가중치 변화량이 큰 상위 비율만 전송하는 Top-k 방식이 있으며, 단순 무작위 선택에 비해 정확도를 유지하면서도 통신 절감을 달성할 수 있다. 최근 연구인 FedPHE [1]는 이러한 아이디어를 프레임워크 차원에서 구현하여, 보안성과 효율성의 trade-off 를 실험적으로 보여주었다.

본 논문은 FedPHE 프레임워크를 직접·실험하여, 실제 데이터셋 기반에서 성능을 검증하고자 한다. 구체적으로 (i) 평문 기반 연합학습, (ii) 동형암호 기반 연합학습, (iii) 동형암호에 희소화 기법을 적용한 연합학습의 세 조건을 동일한 환경에서 비교하며, 비교 지표는 정확도, 수행 시간, 통신량으로 측정했다. 이를 통해 연합학습에 동형암호 도입이 성능에 미치는 영향을 정량적으로 파악하고, 희소화 적용 시의 완화 효과를 확인한다.

Ⅱ. 본론

본 실험은 benchmark MNIST 데이터셋을 활용하여 세 가지 학습 방식을 비교하였다. 비교 조건은 (1) 평문 기반 연합학습 (Plain-FL), (2) 동형암호 기반 연합학습 (HE-FL), (3) 동형암호에 희소화 기법을 적용한 연합학습 (HE-Spars-FL)이다.

실험 환경은 다음과 같이 통일하였다. 클라이언트 수는 10 개로 고정하고, 각 클라이언트에는 균등한 크기의 데이터셋을 분배하였다. 최대 epoch 수는 100 으로 설정



[그림 1] MNIST 데이터셋에서의 학습 조건별 성능 비교

하였으며, 정확도가 0.1%p 이상 개선되지 않는 상태가 10 epoch 이상 연속될 경우 조기 종료를 적용하였다. 암호화 방식은 CKKS 스킴을 사용하였다. 이러한 설정을 통해 각 학습 조건의 차이가 성능에 미치는 영향을 명확히 확인하고자 하였다.

성능 평가는 정확도 (Accuracy), 수행 시간 (Training Time), 통신량 (Network Traffic)의 세 지표를 중심으로 진행하였으며, 추가적으로 수렴 라운드 (Rounds to Convergence)를 측정하여 학습 효율성을 분석하였다. 그림 1 과 표 1 은 평문 기반 연합학습, 동형암호 기반 연합학습, 동형암호에 희소화 기법을 적용한 연합학습의 성능을 보여준다.

2.1 평문 기반 연합학습

Baseline 으로서 평문 기반 연합학습을 수행하였다. MNIST 데이터셋을 10 개 클라이언트에 균등 분배한 결과, 안정적으로 수렴하며 최종 정확도는 98.9% 수준을 기록하였다. 네트워크 트래픽은 상대적으로 작아 전체 전송량이 166MB 에 불과하였으며, 훈련 시간 또한 다른 조건에 비해 가장 짧았다. 이는 동형암호가 추가되지 않은 순수한 연합학습 구조의 특성을 반영한다.

2.2 동형암호 기반 연합학습

다음으로 CKKS 스킴을 적용한 동형암호 기반 연합학습을 진행하였다. 정확도는 평문 대비 약간 감소하여 95.1% 수준에 머물렀으며, 통신량은 암호문 크기로 인해 급격히 증가하여 2,198MB 에 달했다. 수행 시간 또한 크게 늘어, 암호 연산 오버헤드가 실제 학습 효율성에 상당한 부담을 주는 것을 확인할 수 있었다. 이 결과는 동형암호가 보안성 향상이라는 이점을 제공하지만, 동시에 연산 및 통신 효율성 측면에서 실용적 제약을 가할 수 있음을 보여준다.

2.3 동형암호에 희소화 기법을 적용한 연합학습

마지막으로 CKKS 스킴에 Top-k 희소화 (비율 20%)를 적용하였다. 정확도는 93.9%로 (ii) 동형암호 기반 연합학습 대비 소폭 감소했으나, 통신량은 512MB 로 줄어들며 약 4.3 배 절감했다. 수행 시간 역시 감소하여, 희소화가 통신 및 연산 비용을 동시에 완화하는 효과를 확인할 수 있었다. 이는 희소화가 모델 정확도를 크게 저해하지 않으면서도 동형암호 기반 연합학습의 효율성을 개선할 수 있는 가능성을 시사한다.

Ⅲ. 결론

본 논문에서는 연합학습 환경에서 동형암호를 적용했을 때 발생하는 성능 저하를 정량적으로 평가하고, 희소화 기법을 결합하여 효율성 문제를 완화할 수 있는 가능성을 실험적으로 확인하였다.

Dataset	*Metric*	*(i)*	*(ii)*	*(iii)*
MNIST	수렴 Round	39	35	26
	정확도 (%)	98.9	95.1	93.9
	수행 시간 (s)	75.7	214.1	133.0
	통신량 (MB)	166	2,198	512

[표 1] MNIST 데이터셋에서 학습 조건별 성능 비교

MNIST 데이터셋을 대상으로 한 실험 결과, (i) 평문 기반 연합학습은 가장 높은 정확도와 낮은 수행 시간·통신량을 기록하여 baseline 으로서의 성능을 보였다. 반면 (ii) 동형암호 기반 연합학습은 보안성을 제공하지만 통신량과 연산 오버헤드가 크게 증가하여 실용적 제약이 발생하였다. 이에 반해 (iii) 동형암호에 희소화를 결합한 방식은 정확도의 소폭 감소에도 불구하고 통신량을 대폭 줄이고 수행 시간을 단축시켜, 보안성과 효율성 간의 균형점을 마련할 수 있음을 보여주었다.

따라서 희소화는 동형암호 기반 연합학습의 주요 한계를 완화하는 효과적인 보조 기법으로 활용될 수 있으며, 이는 보안성과 효율성을 동시에 고려해야 하는 실제 연합학습 응용에서 중요한 시사점을 제공한다. 향후 연구에서는 다양한 데이터셋과 모델, 그리고 추가적인 최적화 기법을 탐구하여 보다 실용적인 프라이버시 보존형 연합학습 프레임워크를 구축하는 것이 필요하다.

참 고 문 헌

[1] Li, Y., et al. “FedPHE: A Secure and Efficient Federated Learning via Packed Homomorphic Encryption.” IEEE Transactions on Dependable and Secure Computing 22 (2025): 5448-5463. doi: 10.1109/TDSC.2025.3567301.