AI Top Conference 특별세션

일자_ 2023년 11월 23일(목) 09:00~10:20

장소_ 라한셀렉트 경주 컨벤션C

프로그램

시 간	발표주제	발표자(소속)
09:00~09:20	Deep Convolutional Neural Networks on Fully Homomorphic Encryption (ICML 2022)	이은상 교수(세종대)
09:20~09:40	Election Coding for Distributed Learning: Protecting SignSGD against Byzantine Attacks (NeurIPS 2020)	손지용 교수(연세대)
09:40~10:00	An Information-Theoretic Justification for Model Pruning (AISTATS 2022)	노승문 교수(홍익대)
10:00~10:20	Robust Deep Learning from Crowds with Belief Propagation (AISTATS 2022)	옥정슬 교수(포항공대)

강연 소개

Deep Convolutional Neural Networks on Fully Homomorphic Encryption (ICML 2022)

이은상 교수

세종대학교 소프트웨어학과

- 세종대학교 소프트웨어학과 조교수(2022.09~현재)
- 서울대학교 전기정보공학부 박사후연구원(2020.09~2022.08)
- 서울대학교 전기정보공학부 석박통합과정(2014.09~2020.08)
- 서울대학교 전기정보공학부 학사(2010.03~2014.08)

최근, 완전 동형 암호를 활용한 컨볼루션 신경망의 구현이 큰 관심을 받고 있다. 초기 연구들은 네트워크의 레이어 개수를 줄이거나 ReLU와 같은 비대수적 함수를 저차수 다항식으로 근사하는 방식으로 진행되었다. 이러한 접근법은 실행 시간은 줄일 수 있지만, 네트워크 구조 변경과 추가적인 훈련을 필요로 한다. 본 발표에서는 기존 딥러닝 네트워크와 사전 훈련된 파라미터를 그대로 활용하는 접근법에 중점을 둔다. 또한, 최신 기술인 멀티플렉스 병렬 컨볼루션과 허수부-제거 부트스트래핑 기술을 소개한다. 이 연구를 통해 기존 최첨단 방법에 비해 평균 추론 시간을 134배 개선하였으며, 대표적인 완전 동형 암호 스킴 중 하나인 RNS-CKKS에서 ResNet-110을 높은 정확도로 구현하였다.

Election Coding for Distributed Learning: Protecting SignSGD against Byzantine Attacks (NeurIPS 2020)

손지용 교수

연세대학교 응용통계학과

- Chief Scientist, Wecover Platforms(2023)
- Visiting Researcher, Krafton AI(2023)
- Postdoc, Electrical and Computer Engineering, University of Wisconsin-Madison(2021~2022)
- Ph.D., Electrical Engineering, KAIST
- Best Paper Award, IEEE International Conference on Communications (ICC)(2017)

The paper introduces "Election Coding," a coding framework ensuring Byzantine-robustness in distributed learning with SignSGD, minimizing communication load. It presents two code types (Bernoulli and algebraic) to tolerate attacks and guarantee convergence, offering insights and perfect tolerance. Real dataset experiments validate improved Byzantine resilience in SignSGD-based systems.

An Information-Theoretic Justification for Model Pruning (AISTATS 2022)

노승문 교수

홍익대학교 전자전기공학부

- STANFORD University MS/PhD
- 홍익대학교 부교수

We study the neural network (NN) compression problem, viewing the tension between the compression ratio and NN performance through the lens of rate-distortion theory. We choose a distortion metric that reflects the effect of NN compression on the model output and derive the tradeoff between rate (compression) and distortion. In addition to characterizing theoretical limits of NN compression, this formulation shows that pruning, implicitly or explicitly, must be a part of a good compression algorithm. This observation bridges a gap between parts of the literature pertaining to NN and data compression, respectively, providing insight into the empirical success of model pruning. Finally, we propose a novel pruning strategy derived from our information-theoretic formulation and show that it outperforms the relevant baselines on CIFAR-10 and ImageNet datasets.

Robust Deep Learning from Crowds with Belief Propagation (AISTATS 2022)

옥정슬 교수

포항공과대학교 인공지능대학원

- 포항공과대학교 인공지능대학원/컴퓨터공학과(2019~현재)
- UW/UIUC, Postdoctoral Researcher(2018~2019)
- KTH Royal Institute of Technology, Postdoctoral Researcher(2017~2018)
- 한국과학기술원 박사(2016)
- 한국과학기술원 학사(2011)

Crowdsourcing systems enable us to collect large-scale dataset, but inherently suffer from noisy labels of low-paid workers. We address the inference and learning problems using such a crowdsourced dataset with noise. Due to the nature of sparsity in crowdsourcing, it is critical to exploit both probabilistic model to capture worker prior and neural network to extract task feature despite risks from wrong prior and overfitted feature in practice. We hence establish a neuralpowered Bayesian framework, from which we devise deepMF and deepBP with different choice of variational approximation methods, mean field (MF) and belief propagation (BP), respectively. This provides a unified view of existing methods, which are special cases of deepMF with different priors. In addition, our empirical study suggests that deepBP is a new approach, which is more robust against wrong prior, feature overfitting and extreme workers thanks to the more sophisticated BP than MF.