Jinhyun So

jinhyuns@usc.edu 323-459-7903
https://jinhyun-so.github.io/ https://github.com/jinhyun-so

Research Interests

Key problem that I want to solve: How can multiple data-owners (e.g., hospitals, financial institute, mobile users) jointly train a machine learning model while

- (1) enabling efficient and scalable training,
- (2) keeping their individual datasets private from the other parties,
- (3) providing robustness against malicious behavior of adversarial users.

Key words: federated learning, privacy-preserving machine learning, large-scale distributed computing, byzantine-resilience, coding/information theory, optimization

Education

Ph.D. in Electrical and Computer Engineering, University of Southern California (expected) Aug 2022
Advisor: Prof. Salman Avestimehr

M.S. in Electrical Engineering, KAIST, South Korea 2012
Advisor: Prof. Yong H. Lee
Thesis: Digital Predistortion Techniques Based on Envelope Feedback
GPA: $4.12/4.30$

B.S. in Electrical Engineering, KAIST, South Korea 2010
Major GPA: $4.05/4.30$

Experience

Research Assistant (PhD), University of Southern California, USA 2017–Present
Supervised by Prof. Salman Avestimehr

- Proposed coding centric approaches for a fully-decentralized machine learning framework that achieves scalability and privacy protection (**NeurIPS** 2020, **IEEE JSAIT** 2021).
- Proposed a scalable, efficient and secure aggregation protocol for federated learning (**ICML** Workshop 2020, **IEEE JSAIT** 2021)
- Proposed the first single-server Byzantine-resilient and privacy-preserving aggregation framework for federated learning (**IEEE JSAC** 2020).
- Proposed a lightweight and versatile design for secure aggregation for both synchronous and asynchronous federated learning (**MLSys** 2022, ITW 2021, **NeurIPS** 2021 Workshop).
- Implemented an open research library and benchmark that facilitates the development of new federated learning algorithms and fair performance comparisons (**Best Paper**, **NeurIPS** 2020 Workshop).

Research Intern, Microsoft Research, Redmond, USA Jun–Aug 2021
Mentored by Kevin Hsieh

- Develop an asynchronous federated learning framework for satellite networks with time-varying and deterministic topology (submitted to ICML 2022).

Research Engineer, Samsung Electronics, South Korea Jan 2013–Jun 2017
Systems Development Team, System LSI

- Developed and implemented algorithms for cellular modem chips (3G HSDPA, LTE-A).
- Researched algorithms for 5G cellular system and IoT chips.

Research Assistant (M.S.), KAIST, South Korea Jan 2011–Dec 2012
Supervised by Prof. Yong H. Lee

- Developed a digital predistortion algorithm for wireless communication (ICASSP 2012).

Awards

Best Paper Award, NeurIPS SpicyFL Workshop 2020 2020
Annenberg Fellowship, University of Southern California 2017–2022
Graduate Student Fellowship, KAIST, South Korea 2011–2012
Army Commendation Medal, US Army 2010

KOSAF Fellowship, Korea Student Aid Foundation (KOSAF) 2004–2008
Samsung SDI Fellowship, Samsung SDI 2003–2008

PUBLICATIONS

Google Scholar: https://scholar.google.com/citations?user=taFevmQAAAAJ&hl=en&authuser=4
Citations: 400+
Journal papers: 3 | Conference papers: 11 | Pre-prints: 1 | Patents (granted): 4

Pre-print Papers

[1] **J. So**, K. Hsieh, B. Arzani, S. Noghabi, A.S. Avestimehr, R. Chandra "FedSpace: An Efficient Federated Learning Framework at Satellites and Ground Stations," *preprint arXiv:2202.01267*.

Journal Papers

[J1] **J. So**, B. Güler, and A. S. Avestimehr. "Byzantine-resilient secure federated learning," in *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 7, pp. 2168-2181, Jul. 2021. doi: 10.1109/JSAC.2020.3041404

[J2] **J. So***, B. Güler*, and A. S. Avestimehr. "CodedPrivateML: A fast and privacy-preserving framework for distributed machine learning," in *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 441-451, Mar. 2021. doi: 10.1109/JSAIT.2021.3053220

[J3] **J. So**, B. Güler, and A. S. Avestimehr. "Turbo-aggregate: Breaking the quadratic aggregation barrier in secure federated learning," in *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 2641-8770, Mar. 2021. doi: 10.1109/JSAIT.2021.3054610

Conference Papers (peer-reviewed, including workshops)

[C1] **J. So***, C. He*, C Yang*, S. Li, R.E. Ali, B Guler, Q. Yu, and S. Avestimehr. "LightSecAgg: a Lightweight and Versatile Design for Secure Aggregation in Federated Learning," in *the 5th Conference on Machine Learning and Systems (MLSys)*, Aug. 2022.

[C2] **J. So***, R.E. Ali*, B Guler, J. Jiao, A.S. Avestimehr, "Securing Secure Aggregation: Mitigating Multi-Round Privacy Leakage in Federated Learning," in *International Workshop on Trustable, Verifiable and Auditable Federated Learning in Conjunction with AAAI (FL-AAAI-22)*, Mar. 2022.

[C3] **J. So**, R.E. Ali, B. Guler, A.S. Avestimehr. "Secure Aggregation for Buffered Asynchronous Federated Learning," in *Workshop on New Frontiers in Federated Learning in Conjunction with NeurIPS* Dec. 2021.

[C4] C Yang, **J. So**, C. He, S. Li, Q. Yu, and S. Avestimehr. "LightSecAgg: Rethinking Secure Aggregation in Federated Learning," in *IEEE Information Theory Workshop (ITW)*, Dec. 2021.

[C5] **J. So***, R.E. Ali*, A.S. Avestimehr. "On Polynomial Approximations for Privacy-Preserving and Verifiable ReLU Networks," in *Workshop on Privacy-preserving Machine Learning in Conjunction with NeurIPS*, Dec. 2020.

[C6] C. He, S. Li, **J. So**, M. Zhang, H. Wang, X. Wang, P. Vepakomma et al. "Fedml: A research library and benchmark for federated machine learning," in *Workshop on Scalability, Privacy, and Security in Federated Learning (SpicyFL) in Conjunction with NeurIPS*, Dec. 2020.

[C7] **J. So**, B. Güler, and A. S. Avestimehr. "A Scalable Approach for Privacy-Preserving Collaborative Machine Learning," in *the 34th Conference on Neural Information Processing Systems (NeurIPS)*, Dec. 2020 (acceptance rate: 20.1%).

[C8] **J. So**, B. Güler, and A. S. Avestimehr. "Turbo-Aggregate: Breaking the Quadratic Aggregation Barrier in Secure Federated Learning," in *ICML Workshop on Federated Learning for User Privacy and Data Confidentiality*, Jul. 2020. (Long Presentation).

[C9] **J. So**, B. Güler, P. Mohassel, and A. S. Avestimehr. "CodedPrivateML: A Fast and Privacy-Preserving Framework for Distributed Machine Learning," in *International Workshop on Coding Theory For Large-scale Machine Learning (CodML) in Conjunction with ICML*, Jun. 2019.

[C10] **J. So**, S. Choi, S. H. Ahn, E. Jeong, and Y. H. Lee. "Digital Predistortion Based on Envelope Feedback," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Mar. 2012.

[C11] S. Choi, E. Jeong, B. Lee, **J. So**, and Y. H. Lee. "New Predistortion Technique for Wideband Power Amplifiers of Dual-Band Transmission Systems," in *the 21st Joint Conference on Communications & Information 2011*, May. 2011.

Patents

[P1] **J. So**, S. Heo, S. Yeo, S. Kong, J. Lee, and M. Kim. "Communication device and control method thereof," Grant, U.S. Patent (US9712345), and Korea Patent (No.2015-0151308)

[P2] S. Heo, **J. So**, Soobok Yeo, and Mingu Kim. "Receiver apparatus and reception method in wireless communication system" Grant, U.S. Patent (US9479360), Korea Patent(10-0118975)

[P3] **J. So**, S. Choi, S. H. Ahn, E. Jeong, and Y. H. Lee. "Low-cost digital predistortion apparatus and method using envelope detection feedback" Grant, U.S. Patent (US9148093), Korea Patent (10-1389880)

[P4] S. Choi, S. H. Ahn, E. Jeong, **J. So**, and Y. H. Lee. "Method and Appratus for pre-compensation of self-local oscillator coupling effect in transmitters," Grant, Korea Patent (10-1265241)

*: equal contribution.

SERVICES

Technical Program Committee

- ICML 2021 Workshop on Federated Learning for User Privacy and Data Confidentiality (FL-ICML'21)
- AAAI 2022 Workshop on Trustable, Verifiable and Auditable Federated Learning (FL-AAAI'22)
- ACL 2022 Workshop on Federated Learning for Natural Language Processing (FL4NLP-ACL'22)
- International Workshop on Trustworthy Federated Learning in Conjunction with IJCAI 2022 (FL-IJCAI'22)

Reviewer

- IEEE Transactions on Neural Networks and Learning Systems (TNNLS), International Conference on Machine Learning (ICML), IEEE Journal of Selected Areas in Communications (JSAC), IEEE International Symposium on Information Theory (ISIT), IEEE Transactions on Information Forensics and Security (TIFS), IEEE Communication Magazine, IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transactions on Neural Networks and Learning Systems (TNNLS), Journal of Machine Learning Research (JMLR)

SKILLS

Python, Matlab, C/C++, git, LaTeX, Inkscape