

- ADMM-based distributed learning with differential privacy,” *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1002–1012, 2019.
- [60] D. Alistarh, D. Grubic, J. Li, R. Tomioka, and M. Vojnovic, “QSGD: Communication-efficient SGD via gradient quantization and encoding,” in *Proc. Adv. Neural Inf. Process. Syst.*, 2017, pp. 1709–1720.
- [61] J. Bernstein, Y.-X. Wang, K. Azizzadenesheli, and A. Anandkumar, “signSGD: Compressed optimisation for non-convex problems,” in *Proc. Int. Conf. Mach. Learn.*, 2018, pp. 560–569.
- [62] H. Wang, S. Sievert, S. Liu, Z. Charles, D. Papailiopoulos, and S. Wright, “ATOMO: Communication-efficient learning via atomic sparsification,” in *Proc. Adv. Neural Inf. Process. Syst.*, 2018, pp. 9850–9861.
- [63] C. Beguier, M. Andreux, and E. W. Tramel, “Efficient sparse secure aggregation for federated learning,” 2020, *arXiv: 2007.14861*.
- [64] C.-Y. Chen et al., “ScaleCom: Scalable sparsified gradient compression for communication-efficient distributed training,” in *Proc. Adv. Neural Inf. Process. Syst.*, 2020, pp. 13551–13563.
- [65] M. Danilova et al., “Recent theoretical advances in non-convex optimization,” in *High-Dimensional Optimization and Probability: With a View Towards Data Science*. Berlin, Germany: Springer, 2022, pp. 79–163.
- [66] J. H. Bell, K. A. Bonawitz, A. Gascón, T. Lepoint, and M. Raykova, “Secure single-server aggregation with (poly) logarithmic overhead,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2020, pp. 1253–1269.
- [67] W. Diffie and M. E. Hellman, “New directions in cryptography,” in *Proc. Democratizing Cryptogr.: Work Whitfield Diffie Martin Hellman*, 2022, pp. 365–390.
- [68] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.



**Rui Hu** (Member, IEEE) received the BEng degree in electrical engineering from Jinan University, Guangdong, China, in 2017, and the PhD degree in electrical and computer engineering from the University of Texas at San Antonio, San Antonio, TX, USA, in



**Yanmin Gong** (Senior Member, IEEE) received the BEng degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2009, the MS degree in electrical engineering from Tsinghua University, Beijing, China, in 2012, and the PhD degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2016. She is currently an Associate Professor in the Department of Electrical and Computer Engineering, The University of Texas at San Antonio, San Antonio, TX, USA.

Her research interests include security and privacy, machine learning, wireless networks, and Internet of Things. She is a recipient of the NSF CAREER Award, NSF CISE CRII Award, Cisco Research Award, IEEE Computer Society TCSC Early Career Researchers Award for Excellence in Scalable Computing, and Rising Star in Networking and Communications Award by IEEE ComSoc N2Women. She is currently an associate editor of ACM Computing Surveys and IEEE Wireless Communications.