MPCAR: Scalable and Secure MPC-based AllReduce SC'26

Hao Qi (University of Florida) • Weicong Chen (University of California, Merced) • Chenghong Wang (Indiana University)
Caiwen Ding (University of Minnesota) • Xiaoyi Lu (University of Florida)

1 APPLICATION IMPACT

Distributed AI + scientific computing

AllReduce repeatedly aggregates model gradients and simulation data across hundreds or thousands of ranks.

Privacy • scalability • speed

Cloud | HPC | AI/ML

Sensitive data on shared infrastructure

2 MOST IMPORTANT INNOVATION

Protect each AllReduce phase differently

RANK INPUT

REDUCTION
Secret-share MPC
Masks cancel

DISTRIBUTE
Asymmetric OTP
Lightweight

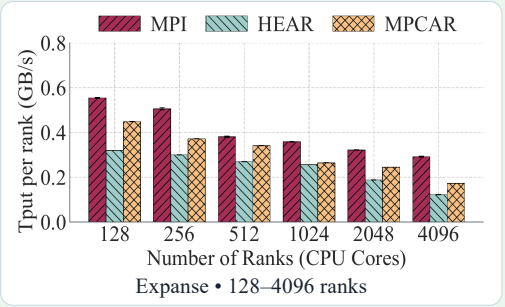
No expensive post-AllReduce decryption

Collective co-design • pipeline • SIMD

3 PERFORMANCE EVIDENCE

41.2% **Higher throughput**

vs. state-of-the-art secure AllReduce



Validated across five platforms

UP TO 8192 RANKS

21.3% APP SPEEDUP