Best Paper Award



1st ACM Workshop on Large AI Systems and Models with Privacy and Safety Analysis (LAMPS), 14 October 2024

co-located with the 31st ACM Conference on Computer and Communications Security

Presented to

Tianshuo Cong, Delong Ran, Zesen Liu, Xinlei He, Jinyuan Liu, Yichen Gong, Qi Li, Anyu Wang, and Xiaoyun Wang

For

Have You Merged My Model? On The Robustness of Large Language Model IP Protection Methods Against Model Merging

Bo Li, Wenyuan Xu, Jieshan Chen, Yang Zhang, Jason Xue, Shuo Wang, Guangdong Bai, and Xingliang Yuan

LAMPS 2024 Organizing Committee

