LINCOLN LABORATORY SUPERCOMPUTING CENTER

244 WOOD STREET
LEXINGTON, MASSACHUSETTS 02420-9176

Area Code 781
981-LLSC

4 Apr 2025

To: Science of Security Paper Competition

I am pleased to nominate "Accelerating Zero-Knowledge Proofs Through Hardware-Algorithm Co-Design" presented at the 57th IEEE/ACM International Symposium on Microarchitecture (MICRO).

Zero-Knowledge Proofs are a powerful tool for addressing many security challenges in modern distributed computing environments. Performance and energy efficiency are key concerns when using these approaches in practical settings. The integration of security capabilities into hardware has become a common practice for enabling broad adoption of novel security approaches.

The NoCAP accelerator presented in the paper provides significant acceleration for Zero-Knowledge Proofs and are big step forward in making these techniques practical and widely available. The architecture represents an elegant co-design blending algorithm innovation with novel hardware organization to produce a programmable vector processor for accelerating Zero-Knowledge Proofs.

Sincerely,

Jeremy Kepner

Dr. Jeremy Kepner
Lincoln Laboratory Fellow
Society for Industrial and Applied Math (SIAM) Fellow
Lincoln Laboratory Supercomputing Center Head
IEEE High Performance Extreme Computing (HPEC) Co-Chair