Re: Award Nomination for "Accelerating Zero-Knowledge Proofs Through Hardware-Algorithm Co-Design," Nikola Samardzic, Simon Hogan Langowski, Srinivas Devadas, Daniel Sanchez (Massachusetts Institute of Technology). *Published in the 57th International Symposium on Microarchitecture (MICRO), November 2024*

April 5, 2025

Dear NSA Cybersecurity paper competition committee:

We are pleased to enthusiastically nominate the above paper to the NSA Cybersecurity Best Paper Competition.

The paper is a unique blend of applied cryptography, computer architecture, and hardware design. It details the design of a hardware accelerator, NoCap, that achieves transformative speedups of Zero-Knowledge Proofs (ZKPs). ZKPs provide publicly verifiable integrity of computation run on an *untrusted* computer (also called the prover), and are already deployed in decentralized finance and blockchain applications, and in cryptocurrencies such as Ethereum. Verifiable integrity of computation is essential in the AI and machine-learning space; however, inference and training are significantly more complex computations than financial transactions, and prior to this work, were out of reach for ZKPs. This is because proof generation time is 4-5 orders of magnitude larger than the corresponding native computation due to the heavy cryptographic machinery involved.

NoCap generates publicly verifiable proofs of computations *three orders of magnitude faster than a 32-core CPU*, while requiring an order of magnitude less silicon chip area. NoCap therefore enables new use cases for ZKPs that are critically necessary for trustworthy AI.

There is a tremendous variety in ZKP schemes–elliptic-curve-based, lattice-based, and hash-based. Elliptic-curve schemes are the most popular in blockchains, due to their short proofs and fast verification times. While hash-based schemes have significantly longer proofs, with clever design of parallel and pipelined functional units and intelligent data movement, proof generation in these schemes can be dramatically accelerated unlike in the curve-based schemes. Importantly, the paper contributes a ZKP scheme that is a novel combination of ZKP primitives for Interactive Oracle Proof (IOP) and Polynomial Commitment Scheme (PCS), namely, the Spartan IOP and the Orion PCS. Amdahl's Law states that to get a 1000x speedup, you cannot ignore even 0.1% of the computation, and the choice and parameterization of primitives is critical, as is every aspect of hardware design!

NoCap has very high potential for long-term impact for three key reasons. First, NoCap's large speedups unlock new, transformative use cases for ZKPs as described above. Second, NoCap introduces a new approach to design cryptographic primitives that are amenable to acceleration, enabling cryptographers to build even better protocols. As an immediate consequence of this publication, cryptographers now realize that ZKPs based on elliptic curves (due to requiring large prime moduli) are very difficult to accelerate even with custom hardware, and, more importantly, that there are dramatic differences in performance of ZKP schemes if custom hardware such as NoCap can be built. NoCap is already having an impact, as it has sparked cryptographers to design ZKPs that improve on Spartan+Orion. Third, NoCap's design shares key characteristics with accelerators for other emerging cryptographic primitives like Fully Homomorphic Encryption (FHE) and Private Information Retrieval (PIR), paving the way for a post-quantum-secure, universal cryptographic accelerator that efficiently supports all these emerging primitives.

In summary, the nominated paper showcases with great clarity the potential in codesign of hardware and cryptography, and strongly motivates collaboration between the hardware and cryptography communities.

Nomination submitted by the 57th International Symposium on Microarchitecture Program Co-Chairs.

Alaa R. Alameldeen
Associate Professor
School of Computing Science
Simon Fraser University
8888 University Drive, Burnaby BC V5A 1S6, Canada
Email: alaa@cs.sfu.ca
Web: http://www.cs.sfu.ca/~alaa/

Daniel A. Jiménez
Professor
Department of Computer Science and Engineering
Texas A&M University
TAMU 3112, College Station, TX 77843-3112
Email: djimenez@cse.tamu.edu
Web: https://people.engr.tamu.edu/djimenez/index.html