Carnegie Mellon

Elaine Runting Shi
Professor
Carnegie Mellon University

March 19, 2025

Dear Colleagues,

I would like to enthusiastically nominate the paper "zkPi: Proving Lean Theorems in Zero-Knowledge" by Evan Laufer, Alex Ozdemir, and Dan Boneh (published in ACM CCS'24) for the prestigious NSA Best Scientific Security Paper award.

zkPi is a system that converts proofs in Lean, an interactive theorem prover, to succinct zero-knowledge proofs (also called SNARKs). This is an amazing paper that makes an important connection between formal methods and cryptography. In order to convert Lean proofs to ZKP, the core contribution the paper makes is building an efficient zkSNARK for dependent typing. zkPi successfuly proves 57.9% of the theorems in stdlib, and 14.1% of the theorems in mathlib, within 4.5 minutes per theorem

I believe that zkPi will lead to numerous applications and make impact. For example, this semester, I am visiting a blockchain non-profit company called 0xPARC. We are building a new programming abstraction (called Pods) for writing a class of applications using ZKP and proof-carrying data (PCD). The high-level concept is that each pod can carry 1) data which can be signed by the owner of the pod; and 2) lemmas or theorems about its own data or data from some underlying pods that it depends on. We can then construct derived pods, which may prove derived theorems relying on lemmas and theorems proven in previous pods. Currently, we envision building Pods using zkPi as an important building block.

To enable the theory-to-practice transition of modern cryptography, an important barrier is how to develop elegant programming abstractions for cryptography. This requires research at the intersection of formal methods and crytography. Today, this is still an underrepresented area partly due to the need to overcome the steep learning curves in both fields to make contributions. However, I believe that this cross-disciplinary area will rapidly

increase in importance in the near future, especially as decentralized computing platforms such as blockchains and cloud providers roll out more cryptographic applications in the real world. Both 0xPARC and I myself have been promoting this "programmable cryptography" vision, and encouraging more funding and interest in this space.

Since zkPi is an exemplifying and innovative work that builds a new connection between PL and cryptography, I strongly believe that it is a perfect fit for the NSA Best Scientific Security Paper award.

Please do not hestiate to reach out to me if you have further questions.

Sincerely,

Elaine Shi