Joclean: The Joy of Cryptography in Lean

Pawel Wozniak

April 5, 2026

Overview

The goal of this project is to provide formalization in Lean4 for the Library-based proofs introduced in *The Joy of Cryptography* (`https://joyofcryptography.com`) book by Mike Rosulek. Given such implementation, the generated proofs of cryptographic primitives would be (a) formaly verified, (b) easily exportable to the LaTeX typesetting (`https://github.com/rosulek/joc/tree/main/tex`) prepared by the author. Because implementing the entire book is definitely not possible within the project timeframe, here is what a possible MVP could contain:

1. **Structures**. Find a right way to encode the `Interface` that represent the public set of functions of the library, the `Library` which models the cryptographic primitive as a set of procedures and global/private state and the `Adversary`, which can be linked against libraries and call their code.
2. **Proofs and Tactics**. Implement the notion of "interchangeability" for libraries with equal interface, the ability to "chain" libraries together. Think about a tactic that would allow to perform the *hybrid proof technique* (2.4) or *the three-hop maneuver* (2.4.1).
3. **Exporting (*)**. Find a way that would allow to export the library proofs with minimal overhead, using metapgramming (or other approaches).

Core Property

I would like to have a fully working proof of Claim 2.4.2 and possibly one of the Exercises implemented using the architecture described in the Overview.

Challenges

The hardest part will be to find a right design of `Interface`, `Library` and `Adversary`, that will allow to perform the proofs on implemented enitites with minimal overhead (eg. re-using the `Lean4` or `Mathlib` constructions). Then, the proving a Claim 2.4.2 should be rather doable.