ESGI 195 Challenge: Formalizing the Mathematics of Cryptography in ACL2

This ESGI195 challenge is sponsored by Kestrel Institute: kestrel.edu

Overview

Kestrel Institute is a non-profit computer science research center with interests in formal methods, program synthesis and refinement, program analysis and verification, theorem proving, and planning. A large part of our activities involves using the ACL2 theorem prover and related tools to verify software. Of particular interest is cybersecurity, which has widespread applications, e.g., in medical devices, digital infrastructure, and even blockchains.

Challenge Focus

Our focus is primarily on elliptic curve cryptography. One of the important challenges in this field is identifying elliptic curves that are practical for cryptographic use. There are two main parameters that govern this applicability, the number of points on the elliptic curve, and the order of the generated subgroup. The number of points on the curve can be computed using Schoof's Algorithm, or the improved Schoof-Elkies-Atkin (SEA) Algorithm. This algorithm can be implemented directly in ACL2 or another high-level language, like C++, but what is really needed is a formal proof of correctness in the ACL2 theorem prover. What assurances do we have that when the algorithm claims there are N points in a given curve, there really are exactly N points in the curve?

The goal is to make significant progress towards a proof of correctness of SEA using ACL2. With roots in Edinburgh, ACL2 is the latest version in the Boyer-Moore family of theorem provers. It has a strong community, and it is used in academia and industry, particularly for hardware verification. It is easy to learn, and anyone with even limited

experience using other theorem provers, e.g., Lean, Isabelle, or Rocq, will be able to make a strong contribution.

The proof itself is interesting, as an artifact demonstrating the capability of ACL2 to formalize important mathematical results. But it is also of practical importance, as it allows ACL2 to reason about the correctness of cryptographic algorithms in large software systems.

There are many other problems related to cryptography that Kestrel Institute is interested in formalizing in ACL2. For instance, there are many interesting problems in post-quantum cryptography, such as Module-Lattice-Based cryptography. We would also be interested in progress on formalizing these in ACL2.

Participants will help to identify key lemmas and proof sketches that can be carried out in ACL2. The goal is to formalize the SEA algorithm, or post-quantum encryption. These sketches will make use of the ACL2 Community Books, which contain many useful and relevant formalizations already. For example, the standard proof of Schoof's algorithm makes use of the Chinese Remainder Theorem, which is already formalized in ACL2. In other cases, the necessary prerequisites may not be formalized already. So it is expected that mathematical creativity will be necessary to either fill in the gaps or discover alternative proofs that avoid them.

Outcome

The expected outcome is a roadmap, including appropriate lemmas, for the formalization of meaningful cryptography algorithms in ACL2, such as Schoof's Algorithm. The roadmap should be sufficient to permit a successful proof effort after ESGI. In particular, we are interested in growing the ACL2 community, so we would welcome continued collaboration with the participants on this and other ACL2 verification projects.