Computational Algebra in Rust

Crypto Internship Proposal

Snips UVSQ

Spring 2017

Motivation

Experimenting with modern cryptographic primitives (such as supersingular isogenies or lattices) involves assessing their efficiency, both in lab experiments but at some point also in real-world applications. But while it is common for academic experimental libraries to be written in e.g. C/C++, Sage (Python), or Julia, this is not always ideal for experimenting with real-world applications, either because of the language itself or because it implies large software dependencies. Hence these experimental primitives are often somewhat inaccessible for testing in real-world applications as they first need to be re-implemented, potentially by people with less expertise in algebraic optimisations.

The Rust language is an interesting alternative to C/C++ that could potentially help bridge the gap between lab and real-world experimentation. It has efficiency comparable to other systems languages, yet also offers conveniences such as zero-cost abstraction, type safety, functional constructs, and a modern build system. However, current cryptographic libraries in Rust often start from scratch and re-implement common algorithms for computational number theory and algebra, making the landscape quite ad-hoc

Objectives

- Test suitability of Rust as an language for experimental implementations of cryptographic primitives, with a goal of making it easier to not only test these in real-world settings, but also potentially help close the gap to production-ready implementations
- Provide optimised algorithms for operations commonly used in cryptography (rings, finite fields, polynomials, sampling)
- Expected outcome is Rust library with optimised algorithms (potentially open source)

Skills

- Suitable for Math/CS student with good mathematical maturity (algebra and algorithms)
- Some prior programming experience needed (not necessarily in Rust)

Format

- 4-6 month full-time internship position at Snips
- collaboration with the CRYPTO research team at Université de Versailles – Saint-Quentin
- Suitable for those interested in pursuing research in computational algebra or cryptography

Company

Snips is young start-up located in the centre of Paris. Our primary focus is on data science and machine learning, but since we encourage the principle of *Privacy by Design*, we also have a growing team working on privacy enhancing technologies, such as secure computation, homomorphic encryption, and differential privacy. We are currently around 40 employees, including data scientists, software engineers, designers, and cryptographers.