Bachelor-Thesis

A Multi-precision Implementation of the Supersingular Isogeny Key Encapsulation (SIKE) Scheme

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Institute for Scientific Computing

SCIENTIFIC COMPUTING

Giang Nam Nguyen, M.Sc.
Contact person

Hochschulstr. 1
S1|03, Room 8
64289 Darmstadt

giang_nam.nguyen@tu-darmstadt.de

Date
July 25, 2022

Supersingular Isogeny Key Encapsulation (SIKE) is one of the remaining candidates in the current 4th round of the NIST post-quantum cryptography standardization process.[1] In fact, this scheme originates from a paper of De Feo, Jao and Plut [1] which proposes a key exchange scheme based on the hardness of the Computational Supersingular Isogeny (CSSI) problem.

Creating a reliable runtime model for solving CSSI relies on the runtime of solving many CSSI instances, which are defined in different finite fields. On the other hand, SIKE's software implementation uses fixed memory layouts tailored for a set of finite fields. While the fixed precision arithmetic allows many optimizations specialized for the fixed fields, it is hard to adapt the codebase for a different finite field.

Currently, we have a multiprecision implementation of one CSSI-attacking algorithm which operates on affine coordinate points. However, a known disadvantage of the affine coordinate is that the arithmetic requires many expensive inverse computations. Therefore, our goal is to adapt the projective representation to the codebase. This projective representation offers the more efficient x-only arithmetic without the expensive inverse.

To address the aforementioned issues, this thesis focuses on a new multiprecision implementation of the x-only arithmetic. An approach could be to implement the operations in extension fields using the multiprecision library GMP.[2]

A performance comparison between the new implementation and the fixed-precision implementation can be conducted on the same set of parameters used in the NIST competition. The applicability of the new implementation for attacking CSSI can be assessed by evaluating its performance for solving the CSSI instances published in a state-of-the-art cryptanalysis [2]. To that end, this thesis will clarify the trade-off of scarifying performance for the ease of using a multiprecision library.

Recommendations

- Knowledge about post-quantum cryptography, in particular elliptic curve cryptography, is nice to have.
- Good programming skills in C/C++.
- The student is encouraged to write this thesis in English.

Literature

[1] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 19–34, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[2] Craig Costello, Patrick Longa, Michael Naehrig, Joost Renes, and Fernando Virdia. Improved classical cryptanalysis of sike in practice. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *Public-Key Cryptography – PKC 2020*, pages 505–534, Cham, 2020. Springer International Publishing.

[1] https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions
[2] https://gmplib.org/