Disorientation faults in CSIDH

Gustavo Banegas[1], Juliane Krämer[2], Tanja Lange[3,4], Michael Meyer[2], Lorenz Panny[4], Krijn Reijnders[5], Jana Sotáková[6], and Monika Trimoska[5]

[1] Inria and Laboratoire d'Informatique de l'Ecole polytechnique, Institut Polytechnique de Paris, Palaiseau, France
gustavo@cryptme.in
[2] University of Regensburg, Germany
juliane.kraemer@ur.de, michael@random-oracles.org
[3] Eindhoven University of Technology, the Netherlands
tanja@hyperelliptic.org
[4] Academia Sinica, Taipei, Taiwan
lorenz@yx7.cc
[5] Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl, monika.trimoska@ru.nl
[6] University of Amsterdam and QuSoft, Amsterdam, The Netherlands
j.s.sotakova@uva.nl

Abstract. The cryptographic community is actively looking for alternatives for protecting our data and communications from adversaries with a large quantum computer. One of the families of post-quantum cryptography is based on the hardness of finding isogenies of elliptic curves. The isogeny-based scheme SIDH and its instantiation SIKE have recently been broken by a surprising polynomial-time attack. However, the CSIDH cryptosystem and protocols based on the CSIDH group action are not affected by the attack and remain a noteworthy target for cryptanalysis.
In this work, we investigate a new class of fault-injection attacks against the CSIDH family of cryptographic group actions. Our disorientation attacks effectively flip the direction of some isogeny steps, resulting in an incorrect output curve. The placement of the disorientation fault during the algorithm influences the distribution of the output curve in a key-dependent manner. We explain how an attacker can post-process a set of faulty outputs to fully recover the private key. We provide full details for attacking the original CSIDH proof-of-concept software as well as the CTIDH constant-time implementation. Finally, we present a set of lightweight countermeasures against the attack and discuss their security. This presentation will focus on analysing the graph of faulty curves formed in the post-processing stage and getting an intuition on how it can be used to infer constraints on the secret key. This is joint work with Gustavo Banegas, Juliane Krämer, Tanja Lange, Michael Meyer, Lorenz Panny, Krijn Reijnders and Jana Sotáková.

Keywords: Fault-injection attack · isogenies of elliptic curves · post-quantum cryptography