1163-11-1513 **Paul Bottinelli**, **Victoria de Quehen*** (victoria.dequehen@isara.com), **Chris Leonardi**, **Anton Mosunov**, **Filip Pawlega** and **Milap Sheth**. *On the Separation between Isogeny Assumptions.*

Many isogeny-based cryptosystems rely on the hardness of the Supersingular Decision Diffie-Hellman (SSDDH) problem. However, most cryptanalytic efforts have targeted the more generic supersingular ℓ^e-isogeny problem — an established hard problem in number theory. In this work, we question if the two additional pieces of information given in practical SSDDH instances — the action on a torsion subgroup, and the domain elliptic curve's endomorphism ring — can lead to improved attacks on such cryptosystems. We show that SIKE/SIDH are secure against our techniques. However, in certain settings, e.g. multi-party protocols, our results may suggest a larger gap between the security of these cryptosystems and the ℓ^e-isogeny problem. Our analysis relies on the ability to find many endomorphisms on the base curve that have special properties. We give a correspondence between these endomorphisms and solutions to quadratic forms. We informally discuss the parameter sets where these endomorphisms should exist. Finally, we present a minor variation of the SIKE protocol that avoids exposing a known endomorphism ring. (Received September 15, 2020)