# Abstract

In this work, our focus is improving the computation of $\ell$-degree isogenies between supersingular Montgomery curves over a finite field, with $\ell$ an odd prime. In particular, we obtained parallelized formulas from the square-root Vélu formulas in [BFLS20] and [ACR22].
More precisely, we elaborated new algorithms and, from the sequential version of square-root Vélu presented in [ACR22], we obtained the expected cost function of our parallelized formulas. Subsequently, we implemented the obtained algorithms in C using OpenMP and integrated them into the SQALE'd CSIDH protocol.

To the best of our knowledge, our results are until now the most efficient way to compute $\ell$-isogenies of Montgomery curves, considering 2 or 4 cores available. We expect that it will have a great impact on isogeny-based schemes. Concerning the implementation, we highlight that thread synchronization is our main bottleneck for achieving higher performance. Large parameter sets with at least 2048 bits are of interest for secure CSIDH instantiations [BS20, Pei20, CCJR22], where the synchronization cost becomes easier to manage for those cases. Additionally, we centered on the dummy-free CSIDH variant of [CCC+19]. We focus to implement our formulas on large parameters and thus we limited our experiments to the SQALE'd CSIDH from [CCJR22]. Since our CSIDH software differs with respect to CTIDH, we limited our CTIDH analysis to simulations.