# Orienting supersingular isogeny graphs

Leonardo Colò David Kohel

Supersingular isogeny graphs have been used in the Charles–Goren–Lauter cryptographic hash function [1] and the supersingular isogeny Diffie–Hellman (SIDH) protocole of De Feo and Jao [2]. A recently proposed alternative to SIDH is the commutative supersingular isogeny Diffie–Hellman (CSIDH) protocole, which in which the isogeny graph is first restricted to $\mathbb{F}_p$-rational curves $E$ and $\mathbb{F}_p$-rational isogenies then oriented by the quadratic subring $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$ generated by the Frobenius endomorphism $\pi : E \to E$. We introduce a general notion of orienting supersingular elliptic curves and their isogenies, and use this as the basis to construct a general oriented supersingular isogeny Diffie-Hellman (OSIDH) protocole.

## Références

[1] D. Charles, E. Goren, and C. Lauter. Cryptographic hash functions from expander graphs. *J. Cryptography* bf 22 (1), 93–113, 2009.

[2] D. Jao and L. De Feo. Towards quantum-resistant cryptosystems from supersingular curve isogenies. In *Post-Quantum Cryptography*, LNCS **7071**, 19–34, Springer, 2011. `https://eprint.iacr.org/2011/506`.

[3] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. CSIDH : an efficient post-quantum commutative group action. Cryptology ePrint Archive, 2018/383, `https://eprint.iacr.org/2018/383`