Oriented Supersingular Elliptic Curves and Class Group Actions

Leonardo Colò David Kohel

We recently defined an OSIDH protocol [3] — for oriented supersingular isogeny Diffie-Hellman — by imposing the data of an orientation by an imaginary quadratic ring $\mathcal{O}$ on the category of supersingular elliptic curves. Starting with an elliptic curve E_0 oriented by a CM order $\mathcal{O}_K$ of class number one, we push forward the class group action along an ℓ-isogeny chains, on which the class group of an order $\mathcal{O}$ of large index ℓ^n in $\mathcal{O}_K$ acts. The map from ℓ-isogeny chains to its terminus forgets the structure of the orientation, and the original base curve E_0. For a sufficiently long random ℓ-isogeny chain, the terminal curve represents a generic supersingular elliptic curve.

One of the advantages of working in this general framework is that the group action by $\mathcal{Cl}(\mathcal{O})$ can be carried out effectively solely on the sequence of moduli points (such as j-invariants) on a modular curve, thereby avoiding expensive generic isogeny computations or the requirement of rational torsion points.

The proposed attacks of Onuki [6] and Dartois-De Feo [4] and their analyses motivate the idea of enlarging the class group without touching the key space using *clouds*. In this talk we propose two approaches to augments $\mathcal{Cl}(\mathcal{O}_n(M))$ in a way that no effective data is transmitted for a third party to compute cycle relations. In both cases, it comes down to an extension of the initial chain by the two parties separately. In particular, while the original OSIDH protocol made exclusive use of the class group action at split primes in $\mathcal{O}$, we extend the protocol to include descent in the eddies at non-split primes (inert or ramified) or at large primes which are not cost-effective for use for longer isogeny walks.

References

[1] 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`

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

[3] L. Colò and D. Kohel, Orienting supersingular isogeny graphs. In *Journal of Mathematical Cryptology*, vol. **14.1**, Walter de Gruyter, 414–437, 2020. `http://dx.doi.org/10.1515/jmc-2019-0034`.

[4] P. Dartois and L. De Feo. On the security of OSIDH. In *Cryptology ePrint Archive, Paper 2021/1681*, 2021. `https://eprint.iacr.org/2021/1681`

[5] 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`.

[6] H. Onuki. On oriented supersingular elliptic curves. In *Finite Fields and their Applications*, **69**, 2021.