

## Isogeny graphs, modular forms and signatures

Guido Maria Lido

*Università di Roma Tor Vergata, Via della Ricerca Scientifica 1, Roma*  
*e-mail: lido@mat.uniroma2.it*

Giulio Codogni

*Università di Roma Tor Vergata, Via della Ricerca Scientifica 1, Roma*  
*e-mail: codogni@mat.uniroma2.it*

**Abstract.** Given  $p, \ell$  different primes, the *isogeny graphs*  $G(p, \ell)$  is defined as follows: the vertices are supersingular elliptic curves  $E/\mathbb{F}_{p^2}$ , the edges are  $\ell$ -isogenies. Such graphs give an easy visualization of many protocols in isogeny-based cryptography, e.g. the hash function [1] and the signature scheme [4].

It is immediate to see that from each vertex there are exactly  $\ell+1$  outgoing edges (the graph is regular). It is less obvious that, as proven by Eichler in [5], isogeny graphs are *connected* and have the *Ramanujan property*: the non-trivial eigenvalues fall in the Hasse interval.

We look at a generalization of these graphs, adding level structure to the elliptic curves: new interesting phenomena arise, since the graph can be  $k$ -multipartite, but up to this, we prove the Ramanujan property using modular curves.

The initial motivation for these generalizations was to prove security of a zero knowledge proof of knowledge in [2]: the Ramanujan property implies that random walks mix fastly, i.e. that even for not-too-long walks, the last visited vertex is close to uniformly distributed. In [3] we explored the problem in vast generality.

**Keywords:** Isogeny; Cryptography; Modular curves.

### References

- [1] **D. X. Charles, K. E. Lauter, E. Z. Goren**, Cryptographic hash functions from expander graphs. *Journal of Cryptology* 22(1), 93–113 (Jan 2009).
- [2] **A. Basso, G. Codogni, D. Connolly, L. De Feo, D. B. Fouotsa, G. M. Lido, T. Morrison, L. Panny, S. Patranabis and B. Wesolowski**, Supersingular curves you can trust, In: *Hazay, C., Stam, M. (eds) Advances in Cryptology – EUROCRYPT 2023*. EUROCRYPT 2023. Lecture Notes in Computer Science, vol 14005. Springer
- [3] **G. Codogni, G. Lido**. Spectral theory of isogeny graphs. *arXiv preprint* arXiv:2308.13913 (2023).
- [4] **L. De Feo, D. Kohel, A. Leroux, C. Petit, B. Wesolowski**, SQISign: compact post-quantum signatures from quaternions and isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 64-93). Springer, Cham. (Dec 2020).
- [5] **M. Eichler**, The basis problem for modular forms and the traces of the Hecke operators. In *W. Kuyk editor, Modular functions of one variables I*, LNM volume 320, 1973, pages 75-152, Springer-Verlag