

Grafos de isogenias de curvas elípticas: entrelazando caminos de grados distintos

JOSEP M. MIRET, JORDI PUJOLÀS, JUAN TENA, JAVIER VALERA

Departament de Matemàtica, Universitat de Lleida

josepmaria.miret@udl.cat

Resumen. Recientemente, Luca de Feo et al. [2, 3] han presentado a la convocatoria del NIST una propuesta de firma digital llamada SQISign, basada en isogenias de curvas elípticas supersingulares. Su seguridad se basa en la dificultad computacional de encontrar un camino entre dos curvas del grafo supersingular [6].

En esta charla, damos un algoritmo para obtener los j -invariantes de las curvas del grafo cuyo anillo de endomorfismos tiene un endomorfismo *twisting* [4]. Como consecuencia, mostramos algunas propiedades de la estructura de estos grafos de curvas supersingulares [1] al considerar los entrelazamientos que se obtienen con isogenias de grados coprimos, comparándolos con el caso ordinario [5].

Palabras clave: Cuerpos finitos; Curvas elípticas supersingulares; Grafos de isogenias; Criptografía post-cuántica.

References

- [1] S. Arpin, C. Camacho-Navarro, K. Lauter, J. Lim, K. Nelson, T. Scholl, J. Sotáková (2023). Adventures in supersingularland. *Experimental Mathematics*, 32(2), 241–268.
- [2] L. De Feo, D. Kohel, A. Leroux, C. Petit, B. Wesolowski (2020). SQISign: compact post-quantum signatures from quaternions and isogenies. ASIACRYPT 2020, Lect. Notes Comput. Sci., vol. 12491, 64–93.
- [3] L. De Feo, A. Leroux, P. Longa, B. Wesolowski (2022). New algorithms for the Deuring correspondence: Towards practical and secure SQISign signatures. Cryptology ePrint Archive, Paper 2022/234.
- [4] W. Castryck, L. Panny, F. Vercauteren (2020). Rational isogenies from irrational endomorphisms. EUROCRYPT 2020, Lect. Notes Comput. Sci., vol. 12106, Springer-Verlag, 523–548.
- [5] M. Fouquet, J. Miret, J. Valera (2018). Distorting the volcano. *Finite Fields Appl.*, 49, 108–125.
- [6] S. Galbraith, C. Petit, J. Silva (2017). Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems. ASIACRYPT 2017, Part I, Lect. Notes Comput. Sci., vol. 10624, Springer-Verlag, 3–33.

Agradecimientos. Trabajo financiado parcialmente por el Ministerio de Ciencia e Innovación mediante el proyecto PID2021-124613OB-I00, por la Generalitat de Catalunya mediante el grupo 2021SGR 00434 y por la red Iberoamerica 522RT0131 de CyTeD.

Indicar la preferencia: charla.

Indicar la preferencia: Jueves/Viernes.