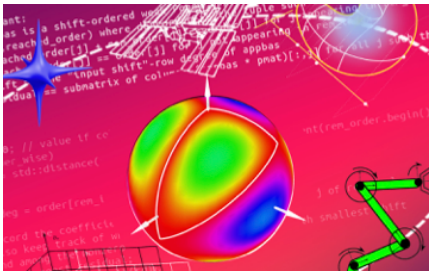

ID de Contribution: **33** Type: **Non spécifié**

Interpolating isogenies by Benjamin Wesolowski

jeudi 28 septembre 2023 11:00 (1 heure)

Abstract. In 2011, Jao and De Feo proposed a key exchange based on the presumed hardness of the following problem: given two elliptic curves, and the images of a few points through a secret isogeny, compute this isogeny.
In 2022, a polynomial-time algorithm was discovered. This powerful new tool has broken many cryptosystems, but has also lead to new constructions, and other applications in algorithmic number theory. We will present this algorithm and some of its applications.