Forensic categories: a framework for SQIsign-like primitives

Ilinca Radulescu*[1]

[1]ENS de Lyon and CNRS – École Normale Supérieure - Lyon, CNRS – France

Résumé

Using the language of categories, we introduce a novel framework abstracting the key features of the isogeny-based post-quantum signature scheme SQIsign. We then show how to construct a digital signature within this framework that, once instantiated with isogenies, recovers (classical) SQIsign. We also illustrate how the framework leads to more advanced primitives, such as a chameleon hash function. We present an instantiation of the framework based on isogenies of supersingular elliptic curves. *Collaboration with Andrea Basso, Luca De Feo, Sikhar Patranabis and Benjamin Wesolowski.*

*Intervenant