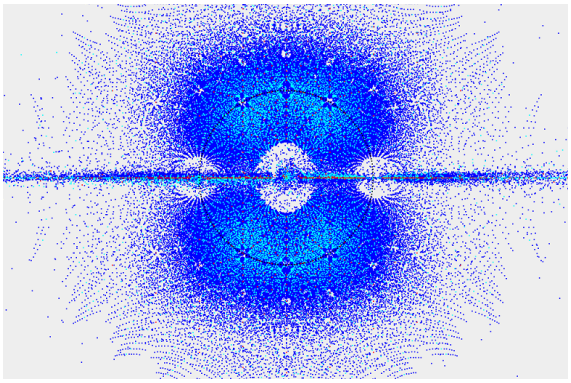
The Principal Ideal Problem for quaternion algebras



Since the development of the Deuring correspondence, quaternion algebras have served as a bridge between number theory and the geometry of supersingular elliptic curves. In recent years, this connection has become a cornerstone of post-quantum cryptography, where the security of protocols like SQIsign relies on the hardness of the Endomorphism Ring Problem. Another natural problem arising in this setting is the Principal Ideal Problem (PIP): given a right ideal in a maximal order, find a generator.

While the PIP in the standard quaternion algebra $B_{p,\infty}$ is well-studied for dimension 1, its extension to higher dimensions and more complex matrix rings is gaining increasing attention. Recent developments have seen a shift toward *higher-dimensional* isogeny-based cryptography, utilizing superspecial abelian varieties. In this setting, it is interesting to study algorithms to solve the PIP in matrix rings $M_g(\mathcal{O})$, for $g \geq 2$. Recent results gave a general polynomial time solution to this problem. However, concrete instantiations of this algorithms in many settings are still lacking.

This project aims to build upon these results by exploring the boundaries of the PIP in broader algebraic settings. One possible direction is to work towards an implementation of the recent PIP algorithms in various new settings, like quaternion algebras $B_{p,\infty}$ where $p \equiv 1 \bmod 4$ or particular families of maximal orders. Another possible direction is is to move to more general definite quaternion algebras over $\mathbb{Q}$, i.e. ramifying at more than one prime p. Finally, the impact of the PIP problem in the cryptanalysis of different schemes can be explored.

The student should preferably have some background in algebraic geometry and number theory.

Practicalities

Promotor:	Frederik Vercauteren		
	Wouter Castryck		
Daily supervisor:	Riccardo Invernizzi	riccardo.invernizzi@esat.kuleuven.be	office B01.15
	Gioella Lorenzon	gioella.lorenzon@esat.kuleuven.be	office B01.15
Nature of the work:	40% literature, 30% theoretical work, 30% implementation		
Number of students:	1		

 © 2025 – 2026 COSIC