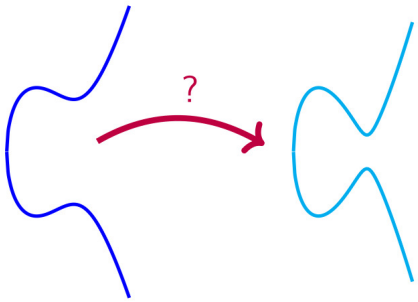
Impact of Wesolowski's attack on isogeny-based cryptography



The security of modern cryptography relies on hardness assumptions that no longer hold once adversaries have access to quantum computers. Cryptographers therefore need to investigate problems that are hard even for quantum computers, and to build cryptographic schemes from them. Among the main candidates is isogeny-based cryptography, whose security relies on the difficulty of computing an isogeny, i.e. a "nice" algebraic map, between supersingular elliptic curves defined over a finite field.

Since the Delfs–Galbraith attack of 2013, the best known algorithms for this problem have all run in classical time $\tilde{O}(p^{1/2})$, where p is the characteristic of the finite field, and admit low-memory variants. In July 2026, however, Wesolowski presented a new heuristic attack that exploits the existence of an isogeny between a curve and its Frobenius conjugate, i.e. its image under the map $(x, y) \mapsto (x^p, y^p)$, of smaller degree than we would expect between two random curves. This attack runs in time and memory $p^{1/3+o(1)}$ and offers continuous time/memory tradeoffs up to the previous state-of-the-art complexity. Nevertheless, its impact is not yet fully understood. For instance, it is unclear whether its low-memory regime yields a concrete speedup over the previous algorithms. Moreover, its effect on the security parameters of many schemes remains to be determined.

The goal of this thesis project is to improve our understanding of the consequences of this attack for isogeny-based cryptography. The project will start with a study of the existing literature, after which different paths can be taken. One possible direction is to compare the low-memory variant of Wesolowski's attack with the previous attacks, which will involve concrete implementations. Another possible direction is to select several isogeny-based schemes and investigate how they are affected by the attack, in order to develop appropriate countermeasures. A third option is to study how this new algorithm affects the concrete complexity of other hard problems in the field, such as computing the endomorphism ring of an elliptic curve.

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

Practicalities

Promotor:	Frederik Vercauteren		
Daily supervisor:	Arthur Herlédan Le Merdy	arthur.herledanlemerdy@esat.kuleuven.be	office B01.22
	Matthias Kerkhofs	matthias.kerkhofs@esat.kuleuven.be	office B01.29
Nature of the work:	40% literature, 30% theoretical work, 30% software		
Number of students:	1		

 © 2026 – 2027 COSIC