Supersingular Isogeny Key Encapsulation

Jessica Bennett

Abstract

Elliptic curve cryptography and post-quantum cryptography are both very exciting developing topics within mathematics. The recently created Supersingular Isogeny Key Encapsulation (SIKE) cryptosystem uses properties of elliptic curves and functions between them in order to generate a secret key shared by two parties in a way that is resistant to quantum attack. However, discoveries in algebraic geometry have lead to an innovative attack on SIKE that allows a third party to retrieve the secret key using modern computational techniques. This paper provides exposition regarding elliptic curves, SIKE, and the attack on SIKE in a way that is accessible to mathematics undergraduates who may be interested in learning more about these topics.