The ARCS Seminar

The Rise and Fall of Supersingular Isogeny Diffie Hellman

Stefan Erickson
Colorado College

Abstract: The need for secure communications in the computer age has created the need for cryptosystems based on computationally difficult problems. The two most important examples are the factoring problem for RSA and the elliptic curve discrete logarithm problem. While these problems are still considered infeasible on conventional computers, they would be quickly solvable on a sufficiently powerful quantum computer. Thus, researchers have been searching for new cryptosystems which would be resistant to quantum algorithms.

One such cryptosystem based on the isogenies between supersingular elliptic curves was proposed by De Feo, Jao, and Plut in 2011. It was believed that this new system based on maps between elliptic curves would not be vulnerable to the known quantum attacks. It reached the final round of the Post-Quantum Cryptography Standardization competition before a devastating attack was announced by Castryck and Decru in July 2022. Based on genus 2 hyperelliptic curves, it provides the encryption key using a conventional computer in a matter of minutes.

This talk will provide a gentle introduction to both cryptography and elliptic curves. We'll describe the clever construction of an agreed secret key between two parties using supersingular isogenies. We'll then outline the even-more-clever construction of the Castryck-Decru attack. No more than an undergraduate abstract algebra background is assumed.

Time and Place: Wednesday, September 18 from 4:30–5:30PM (Mountain Time Zone) in ENG 239

The Rings and Wings Seminar is an activity of ARCS.
`https://arcs-center.org`