1147-11-241 **Steven D Galbraith*** (s.galbraith@auckland.ac.nz), Mathematics Department, University of Auckland, Auckland, New Zealand. *Isogeny cryptography: strengths, weaknesses and challenges.*

Isogeny-based cryptography is a candidate for post-quantum cryptography. It was first suggested by Couveignes, Charles-Goren-Lauter and Rostovtsev-Stolbunov, and received a major boost with the work of Jao and de Feo. Currently it is a very active area of research. This talk will give a brief overview of post-quantum cryptography and isogeny-based cryptography. I will discuss some of the strengths and weaknesses of isogeny-based crypto, and mention a number of open problems. (Received January 14, 2019)