Elliptic Curves in Cryptography

Diana Mocanu

Abstract

Cryptography is the study of secure communication techniques used in increasingly many everyday tasks such as instant messaging and online transactions. Modern cryptography is heavily based on number theory, with the latest research using elliptic curves to construct quantum-resistant cryptosystems. In this talk, we will review basic theory of elliptic curves and then we will see how to construct two public key cryptosystems using it, discussing their security at the same time.

Time: 12 p.m, 26th January 2022 **Location:** B3.02

Organisers: Lucas Lavoyer de Miranda (lucas.lavoyer-de-miranda@warwick.ac.uk), Sunny Sood (s.sood.1@warwick.ac.uk)

Website: https://warwick.ac.uk/fac/sci/maths/research/events/seminars/areas/postgraduate/21-22