Qatar Math Day – 2nd December 2018

Dr. Abdullatif Shikfa

Qatar University

Title	Introduction to Elliptic Curve Cryptography
Abstract	Elliptic curves have unique properties that make them suitable to asymmetric cryptography. In this talk we will start by briefly introducing asymmetric key cryptography based on the hardness of the discrete logarithm problem. We then move to elliptic curves and explain the group operations that they support. Finally, we focus on their applications in cryptography. We will show an example of elliptic curve key agreement protocol as an alternative to the classical Diffie Hellman key agreement protocol and explain the advantage of such approach.