國立中興大學
應用數學系 學術演講

主講人：楊策仲 博士

講題：

Elliptic Curves Cryptosystem and Supersingular Isogeny Diffie-Hellman key exchange

摘要：

The Diffie-Hellman key exchange protocol is the foundation in public key cryptosystem. The elliptic curve cryptosystem(ECC) is a standard example and widely used now. The ECC uses the algebraic group structure of an elliptic curve over a finite field. The security of this protocol depends on the hardness of solving discrete logarithm problem(DLP). In 1994, Shor presents a quantum algorithm which solves DLP (breaks ECC) and factorization problem (breaks RSA) in polynomial time using quantum computers. De Feo and Jao, in 2011, proposed supersingular isogeny Diffie-Hellman(SIDH) key exchange protocol which is quantum-resistant. In January 2019, SIKE (supersingular isogeny key encapsulation), which is an incarnation of SIDH, was chosen as one of the seventeen second-round contenders, to become a NIST(National Institute of Standards and Technology) standard for post-quantum key establishment. The secuity of this protocol is based on the hardness of computing isogenies between two supersingular elliptic curves.

In this talk, I will introduce ECC and SIDH key exchange protocol. Then I will talk about an extension of SIDH to genus-2 hyperelliptic curves over finite fields. That is, use the jacobians of superspecial genus-2 hyperelliptic curves and product of two supersingular elliptic curves together with Richelot isogenies to construct a genus-2 isogeny cryptosystem.

時間：109 年 11 月 26 日(四) 上午 11 時

地點：資訊科學大樓 501 室

歡迎本系所師生踴躍參加

國立中興大學應用數學系 敬邀