

摘要:

## 講者:莊治耘博士(AMIS)

## 諸題: Introduce to homomorphic encryption.

Homomorphic encryption is a form of encryption that allows specific types of computations to be carried out on ciphertext and generate an encrypted result that, when decrypted, matches the result of operations performed on the plaintext.

This is a desirable feature in modern communication system. Therefore, homomorphic encryption has been studied extensively in recent years.

In this talk, we will introduce linear homomorphic encryption studied by Guilhem Castagnos and Fabien Laguillaumie and some possible applications.

> 日期:2019年10月23日 時間:PM 14:10~ 地點:R0701

報名方式:請掃描 QR Code 或上電子化核國系统報名報名期間:即日起~108.10.22