NUKSNEXT

Research

Colloquium

量子資訊安全入門

主講人：戴濬琮 教授

國立中興大學理學院

時　間：112年12月20日（三）14：30

地　點：應用數學系多媒體教室(理408室)

摘　要：

雖然量子電腦還在如火如荼的研發當中，但已開始影響資訊安全領域的發展。在一方面，如果未來真的研發出了通用型量子電腦，就有機會實現 Shor 演算法破解現今最常用的 Rivest-Shamir-Adleman (RSA)加密演算法。另一方面，我們也可以改由量子技術分發密鑰，以避免密鑰分發時被竊聽者攻擊；或為了避免亂數產生器被破解，改用量子方法生成亂數。在這次演講中，我們會先比較 HTTPS 加密連線和未加密的 HTTP 連線的差異；比較量子通訊和古典通訊的不同；最後再簡介量子密鑰分發和量子亂數產生器。

師生共學社群

活動由「112-116年高等教育深耕計畫」經費補助

國立高雄大學 National University of Kaohsiung