# 國立陽明交通大學應用數學系
# 學術演講公告

主講人：Prof. Sze Yiu Chau (Chinese University of Hong Kong)

講　題：RSA Signature Forgery Attacks Against Weak Implementations

時　間：113 年 10 月 1 日(星期二) 下午 14:00 –15:00

地　點：(光復校區) 科學一館 213 室


Abstract

RSA signature is a cornerstone of network security, widely used by different systems and applications as the means of achieving cryptographic authentication guarantees. In this talk, we will revisit the problem of verifying RSA signatures. Using different techniques, our recent research revealed many instances of unwarranted leniency in implementations of RSA signature verifiers. Critically, our findings suggest that many systems are susceptible to variants of the Bleichenbacher-style RSA signature forgery attack. We will look at how this attack, enabled by weak implementations, can nullify the security guarantees promised by the underlying cryptography, and discuss how this threat can be mitigated in practice.


敬請公告　歡迎參加

*應用數學系　啟*