國立清華大學數學系學術演講
NTHU MATH Colloquium

講題　Introduction to Secret sharing

講者　莊治耘博士
AMIS (帳聯網路科技股份有限公司) 密碼學工程師

時間　2024.01.09 (Tue.) 15:30 – 16:20

地點　第三綜合大樓**2樓 Room 201**

Abstract

Secret sharing is a method that distributes a secret among participants, where each person receives a portion of the secret known as a "share."

Only when the required number of shares meeting specific conditions are collected, the original secret can be reconstructed. Each individual share does not leak any information of the secret. In this presentation, we will introduce cryptographic secret sharing protocols, including Blakley's scheme, Shamir's scheme, and Tassa scheme, within the realm of cryptography. Additionally, we will explore some associated issues and topics.