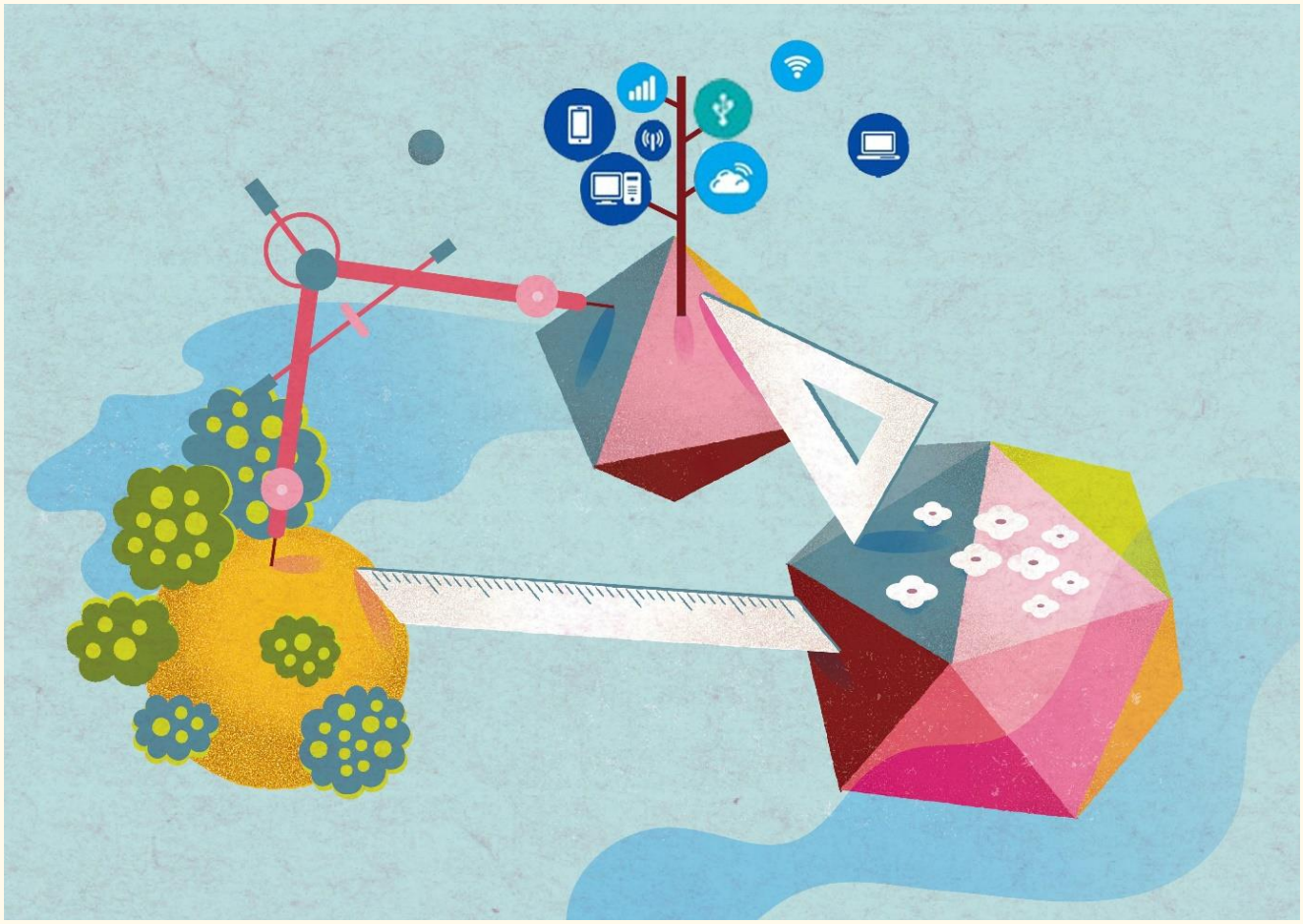
2017 資訊與數學教育研討會

2017 Workshop on Information and Mathematics Education

－ 研討會手冊 －



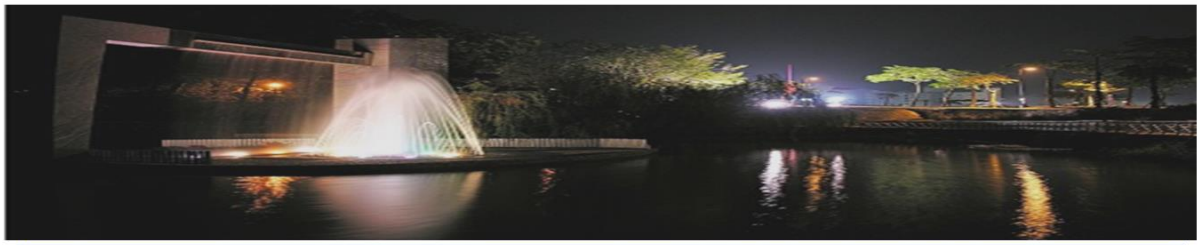
舉辦單位 ： 國立高雄師範大學數學系

舉辦日期 ： 2017 年 3 月 21 日 (星期二)

舉辦地點 ： 高師大燕巢校區致理大樓 MA803 e化教室

主 辦 人 ： 吳明倫 (Ming-Luen Wu)
林英哲 (Ing-Jer Lin)
杜威仕 (Wei-Shih Du)

2017 Workshop on Information and Mathematics Education



Department of Mathematics
National Kaohsiung Normal University
March 21, 2017

Invited Speakers:

林碧珍 教授　　國立清華大學數理教育研究所

左台益 教授　　國立臺灣師範大學數學系

范俊逸 教授　　國立中山大學資訊工程學系

姚如芬 教授　　國立嘉義大學數理教育研究所

呂俊賢 教授　　中央研究院資訊科學研究所

Sponsors: 國立高雄師範大學數學系

Place: 高雄市燕巢區深中路 62 號
高雄師範大學數學系 致理大樓8樓　803 e化階梯教室

Organizers: Ming-Luen Wu (吳明倫)  · Ing-Jer Lin (林英哲)  · Wei-Shih Du (杜威仕) 

E-Mail: mlwu@nknucc.nknu.edu.tw (吳明倫), ijlin@mail.nknu.edu.tw (林英哲), wsdu@mail.nknu.edu.tw (杜威仕)
TEL : (07) 7172930 轉 6800, 6801

高雄師範大學交通資訊

★高市公車直達：搭乘火車者，可於火車站搭 52、248 路公車，於中正文化中心站下車，再步行約 4 分鐘即可到達，72 路公車可於師範大學和平校區門口下車；再轉搭燕巢校區交通車直達。

★公車轉乘:可搭火車站到機場線，於中央公園站下車，轉乘往文化中心之公車，於師範大學和平校區門口下車，再轉搭燕巢校區交通車直達。

或任何可到中央公園站之公車再轉乘，詳細路線圖請參閱高雄市公車處 http://ibus.tbkc.gov.tw/bus/ 。

★高雄捷運：搭高雄捷運至(O7 文化中心站)下車，由第 3 出口出車站，順著和平路走，約 500M 可到達(與高雄大統百貨方向相反) 和平校區；再轉搭燕巢校區交通車直達。

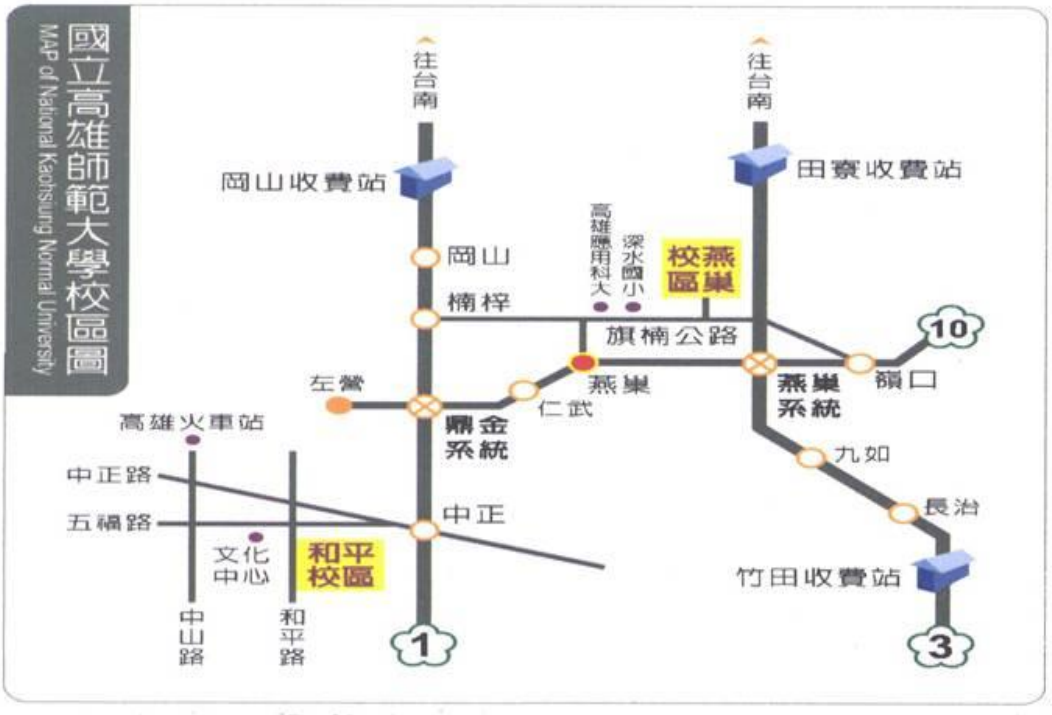
★高鐵：左營車站轉搭高雄捷運至(O7 文化中心站)下車，由第 3 出口出車站，順著和平路走，約 500M 可到達(與高雄大統百貨方向相反)和平校區，再轉搭燕巢校區交通車直達。

★計程車：從火車站到高師大：建國三路-->建國二路-->建國一路-->右轉和平一路-->高雄師大約 2.8KM 和平校區，再轉搭燕巢校區交通車直達。

或從機場到高師大：中山四路-->中山三路(過高架橋第 2 個紅綠燈)-->右轉光華三路-->光華二路-->光華一路-->右轉四維二路(道路縮減)-->(第 3 個紅綠燈左轉)和平一路-->高師大約 7.5KM 和平校區；再轉搭燕巢校區交通車直達。

★開車：二高-->燕巢系統轉(西向)國道 10 號-->仁武交流道-->鼎金系統接中山高(南下)。

交通地圖



Schedule of Programs

Place：高雄師大燕巢校區致理大樓 **MA803 e** 化教室

March 21	Speakers	Titles of Talks
09:10 – 10:00	范俊逸 **(Chun-I Fan)**	**Arbitrary-State Attribute-Based Encryption with Dynamic Membership - An Improved Scheme**
10:00 – 10:10	**Break**	
10:10 – 11:00	左台益 **(Tai-Yih Tso)**	**動態幾何微世界：數學學習伙伴**
11:00 – 11:10	**Break**	
11:10 – 12:00	呂俊賢 **(Chun-Shien Lu)**	**Compressive Sensing and Its Application in Privacy-Preserving Signal Processing**
12:00 – 14:00	**Lunch**	
14:00 – 14:50	林碧珍 **(Pi-Jen Lin)**	**孩子在課堂中的數學論證：以小數乘（除）法的三角關係為例**
14:50 – 15:40	姚如芬 **(Ju-Fen Yao)**	**數學素養與多元評量**

Arbitrary-State Attribute-Based Encryption with Dynamic Membership - An Improved Scheme

范俊逸 (Chun-I Fan)

國立中山大學資訊工程學系

E-mail: cifan@cse.nsysu.edu.tw

摘　要

Attribute-based encryption (ABE) is an advanced encryption technology where the privacy of receivers is protected by a set of attributes. An encryptor can ensure that only the receivers who match the restrictions on predefined attribute values associated with the ciphertext can decrypt the ciphertext. However, maintaining the correctness of all users' attributes will take huge cost because it is necessary to renew the users' private keys whenever a user joins, leaves the group, or updates the value of any of her/his attributes. Since user joining, leaving, and attribute updating may occur frequently in real situations, membership management will become a quite important issue in an ABE system. In this work, we design an ABE scheme which is the first ABE scheme that aims at dynamic membership management with arbitrary states, not binary states only, for every attribute. Our work also keeps high flexibility of the constraints on attributes and makes users be able to dynamically join, leave, and update their attributes. It is unnecessary for those users who do not change their attribute statuses to renew their private keys when some user updates the values of her/his attributes. Finally, we also formally prove the security of the proposed scheme based on random oracles.

動態幾何微世界：數學學習伙伴

左台益 (Tai-Yih Tso)

國立臺灣師範大學數學學系

E-mail: tsoty@ntnu.edu.tw

摘　要

自資訊科技引進數學教室以來，數學發展與資訊技術即交互激盪開展。資訊軟體的發展與設計，促進新的教育理念與教學進路；另一方面認知科學與教學方法的演進與開展，也激發相關數學軟體的開發。如何有效地整合資訊科技於數學學習，尚需了解資訊工具在教學中可能的腳色與功能。本報告嘗試以微世界為理論架構分析動態幾何數學軟體的內涵結構及其做為數學學習探索工具之功能與特色。

Compressive Sensing and Its Application in Privacy-Preserving Signal Processing

呂俊賢 (Chun-Shien Lu)

中央研究院資訊科學研究所

E-mail: lcs@iis.sinica.edu.tw

摘　要

Compressive/Compressed Sensing/Sampling (abbreviated as CS), a kind of new paradigm for simultaneous sampling and compression, has attracted considerable attention recently in diverse fields, including signal processing and information theory. Without being restricted to the constraint of Nyquist rate, compressive sensing can, in theory, perfectly reconstruct the original signal under the constraints that if only a few samples or measurements extracted from an original signal are available and the signal is sparse in the time/space or transform (such as DCT, wavelet, and so on) domain.

In this talk, I will first briefly introduce CS, including its basic properties and sparse signal recovery algorithms. Second, since energy-efficient data collection and privacy-preserving data recovery have received much attention recently, we propose the first encryption framework for the computation-intensive basis pursuit problem to be securely solved in the cloud with the data being efficiently collected using compressive sensing. We provide security and efficiency analyses to show the effectiveness of our method.

孩子在課堂中的數學論證：
以小數乘（除）法的三角關係為例

林碧珍 (Pi-Jen Lin)

國立清華大學數理教育研究所

E-mail: linpj@mail.nhcue.edu.tw

摘　要

本演講將分享師培者與一群教師在小學數學課堂中設計數學任務以提升學童的數學論證教學實踐經驗，作為詮釋即將推動的十二年國教的素養導向之一種可能性。本次演講以理論結合實務為主，演講大綱分為四部分：（一）從小學數學教科書常見的現象：經常以一、二個例子為經過一般化或證明的過程，就要求學童接受一個數學性質或數學定理。（二）您相信小學生可以進行證明嗎？證明通常在國中階段才教。（三）以臆測融入課堂引發學生數學論證的課堂分析：以被乘（除）數、乘（除）數、和積（商）的關係為例。歐美許多國家的數學課程改革均強調數學論證要從小學階段開始，六年前，在台灣的新竹地區小學數學課堂，已開始關注如何引動國小學童的論證發生，我們已發展了將近一百個臆測與論證教學模組了，今藉由此次的演講與大家一起分享，最後，（四）提出臆測與論證的課堂的特色。

數學素養與多元評量

姚如芬 (Ju-Fen Yao)

國立嘉義大學數理教育研究所

E-mail: rfyau@mail.ncyu.edu.tw

摘　要

依據十二年國民基本教育課程綱要數學領域所揭示：數學學習不應只是關注在數、量、形的理解與聯繫，亦應體驗生活情境與數學的連結，培養以數學觀點考察周遭事物的習慣，並觀察問題中的數學意涵、特性與關係，養成以數學的方式，將問題表徵為數學問題再加以解決的習慣，以提高應用數學知識的能力。因此，數學學習的評量，若僅只限於紙筆測驗，恐難窺見學生學習表現的全貌。而多元評量的重點不應只是著重在評量方法的多樣性，更要關照評量目標與評量方式的適配性。透過多元多樣的數學評量方式，包括：紙筆測驗、實作、討論、口頭問答、專題研究或分組報告等，才能理解學生各個面向的數學學習表現。

Department of Mathematics
National Kaohsiung Normal University

地址：82444 高雄市燕巢區深中路 62 號
No.62, Shenjhong Rd., Yanchao District,
Kaohsiung City 82446, Taiwan
電話：(07)7172930 轉 6800,6801
傳真：(07)6051061
網址：http://www.nknu.edu.tw/~math/