國立台灣科技大學 114學年 第2學期　課程大綱

Spring 2026 NTUST Course Outline

授課教師：蔡明憲

Instructor:Ming-Hsien Tsai

課程名稱：決策程序與密碼驗證應用

Course Title：Decision Procedures with Applications to Cryptographic Verification

2026/11/3

課程代號： MI5316701 Course Code 學分數： 3 Credits	必選修：選修/半學年 Required/Electve:Elective/Half Yr. 先修課程： Prerequisites
節次教室： T6(TR-611) T7(TR-611) T8(TR-611) Time/Location	
專業核心能力： Core Professional Competencies	解決問題之能力(Problem Solving)
課程網址： Course Website	
課程宗旨： Course Objectives	關鍵系統（例如核電廠、密碼實作）中的軟體錯誤可能導致嚴重的損害或是安全弱點，因此確保軟體實作的正確性是相當重要的。尤其在AI時代，許多程式皆為AI所撰寫，不熟悉程式語言與軟體安全的使用者經常會產生錯誤且危險的程式碼。一般程式設計師確保軟體安全與正確性的方法多半依賴測試，然而測試往往僅能確認極少部分的輸入，並無法提供完全的保證。除了測試以外，正規驗證是一項提供軟體正確性高度保證的技術，在本課程中，我們將介紹一個自動化的驗證方法。在此驗證方法中，軟體實作的正確性會被轉換為決策問題，而這些決策問題會再被自動決策程序所解答。我們也會展示如何應用這項驗證方法來驗證產業函式庫（例如Bitcoin、OpenSSL）中的密碼實作。 Software bugs in critical systems such as nuclear power plants and cryptographic implementations may induce severe damage or security vulnerabilities. It is thus important to ensure the correctness of software implementations. Particularly in the AI era, where much code is written by AI, users unfamiliar with programming languages and software security often generate erroneous and hazardous code. While most programmers rely on testing to ensure software security and correctness, testing typically only verifies a small fraction of inputs and cannot provide complete guarantees. Formal verification is a technique that provides high assurance of software correctness. In this course, we will introduce an automatic verification approach, where the correctness of a software implementation is transformed to decision problems. Those decision problems are then solved by automatic decision procedures. We will also show how this approach is applied to the verification of cryptographic implementations in industrial libraries such as Bitcoin and OpenSSL.
課程大綱： Outline of Lectures	1. 前言 (Introduction) 2. 命題邏輯 (Propositional Logic) 3. 無量詞理論 (Quantifier-free Theories) 4. 滿足性模數理論 (Satisfiability Modulo Theories, SMT) 5. Z3Py 教學指南 (Z3Py Tutorial) 6. 軟體驗證 (Software Verification) 7. 密碼軟體驗證 (Cryptographic Software Verification) 8. 命題邏輯的決策程序 (Decision Procedures for Propositional Logic) 9. 無量詞理論的決策程序 (Decision Procedures for Quantifier-free Theories)
	講授 Lecture：0%

授課方式： Method of Instruction	分組討論 Group discussion：0% 案例研討 Case study：0% 操做練習 Practical exercises：0% 講授 Lecture：%
教科書： Textbooks	
參考書目： References	
修課須知： Notice	
評量方式： Grading	
備註說明： Notes	