一、教學目標: 講授近代密碼學及安全協定中可証明安全性之理論基礎

Objective: The theoretical foundations of provable security for modern cryptography and secure protocols.

二、先修科目: 無 (計算理論、資訊安全、網路安全、或密碼學)

Pre-requisite Courses: Computation theory, information security, network security, or cryptography recommended

三、課程大綱

1. 密碼學的基礎數學工具
2. 單向函式
3. 虛擬亂數產生器與虛擬亂數函式
4. 零知識證明
5. 可証明安全的加密系統與簽章系統

1. Fundamental mathematical tools in provable security
2. One way function
3. Pseudorandom generator and pseudorandom function
4. Zero-knowledge proof
5. Provable Secure Encryption and Signature Systems

四、教學方式: 課堂授課與論文報告討論

Teaching Method: Lectures and paper presentation / discussions

五、參考書目及參考資料:

Textbook: Foundation of Cryptography, Vol. I, O. Goldreich

1. Crypto, Eurocrypt, Asiacrypt conference papers
2. Cryptography: Theory and Practice, Stinson
3. Lecture Notes on Cryptography, S. Goldwasser
4. Lecture Notes on Cryptography, M. Bellare and Rogway
5. Berkeley CS276 class notes, Cryptography, Trevisan and Wagner
6. U. Maryland class notes, Cryptography, J. Katz
7. U. Technion class notes, Cryptography, M. Naor

六、教學進度

1. 密碼學的基礎數學工具 2 weeks
2. 單向函式 4 weeks
3. 應用層面的亂數產生器 1 weeks
4. 虛擬亂數產生器與虛擬亂數函式 5 weeks
5. 零知識證明 3 weeks
6. 可証明的加密系統與簽章系統應用 2 weeks

Schedule:

1. Fundamental mathematical tools, 2 weeks

2. One way function, 4 weeks
3. Practical aspects of pseudorandom number generator, 1 week
4. Pseudorandom generator and pseudorandom function, 5 weeks
5. Zero-knowledge proofs, 3 weeks
6. Provable secure encryption system and signature systems, 2 weeks

七、評量方式: 作業, 論文報告, 及課堂參與

Evaluation: Homeworks, paper presentation, class participation