Subject Introduction
CSCI471/CSCI971 Advanced Computer Security

Associate Professor Jiageng Chen

School of Computer Science

Central China Normal University

Contact Details and Lecture Time

- Associate Professor Jiageng Chen (陈嘉耕)
  - jiageng.chen@mail.ccnu.edu.cn
- Consultation Time:
  - Wednesday: 16:00 – 18:00
- Lecture time:
  - Tuesday: 13:40 – 15:40, 8216

Subject Organization

- This subject is worth 6 credit points

- According to University policy, 1 credit point is equivalent to 2 hours of work including class attendance, per week. That is, for this subject, 12 hours per week.

Lecture Material

- Moodle
- Check the web site regularly. Any change to the subject will be announced on the eLearning site. Any information posted to the eLearning site is deemed to have been notified to all students.
- Urgent communications will be sent be email, check that every day if possible.

What is this subject about?

- Cryptographic foundations for computer security.
  - Cryptographic primitives.
  - Cryptanalysis.
  - Mathematics for public key cryptography.
  - Security proofs and modeling.

The objectives of this subject

- Describe the fundamental requirements of cryptographic systems.
- Analyze and understand formal presentations of security systems.
- Apply some cryptanalytic techniques.
- Appreciate the difference between symmetric key and public key systems, at the application level and the underlying mathematical level.
- Interpret and possibly develop security proofs.

Required Background

- Some familiarity with number theory
- Some familiarity with algebra
- Having studied some cryptography will help a lot

Approximate Contents

- Introduction, cryptology.
- Encryption, block ciphers: AES
- Linear cryptanalysis, differential cryptanalysis
- Number theory for cryptography
- Hashing
- Integrity
- Security notions
- Public Key cryptography
- ElGamal, Cramer-Shoup. Signature schemes
- Elliptic curve cryptography
- Bilinear pairing
- Identity based cryptography

References

- **A Graduate Course in Applied Cryptography by D. Boneh and V. Shoup**
- **Introduction to Modern Cryptography, Jonathan Katz, Yehuda Lindell, 2014**
- **Understanding Cryptography, Christof Paar and Jan Pelzl, 2010.**
- **Block Cipher Companion, Lars R. Knudsen, Matthew J.B.Robshaw**
- William Stallings. Cryptography and Network Security: Principles and Practices. Prentice Hall.

Assignments and Assessment

- Assignments will cover the following topics, which are worth 35% in total.
  - Block ciphers and cryptanalysis,
  - Mathematics of cryptography,
  - Security proofs,
  - Implementations,
  - Miscellaneous topics.
- The Final assignment is a group project consisting of presentation and report, and is worth 10%.
- The exam is worth 55%. You must get at least 40% for the exam to get a P (pass). There is no minimum requirement for the assignments.

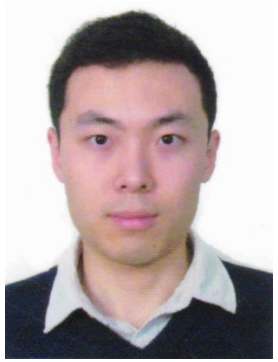
Assignments and Assessment

- If you require additional time to complete an assignment you must submit claims for extensions electronically via SOLS, before the DUE date.
- You may be granted an extension if your circumstances warrant it.
- If you are in hospital for the last week or similar, and cannot get in contact I will understand.

华中师范大学信息安全实验室招生

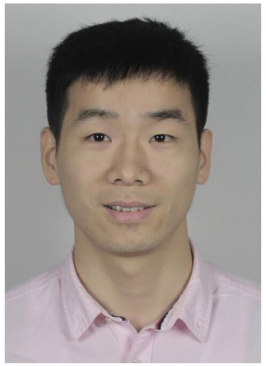
合作单位：

- 导师成员：



陈嘉耕 副教授
JAIST博士学位

李沛 讲师
波尔多大学博士学位



姚世雄 讲师
武汉大学博士学位

- 研究方向：
  1. 密码协议 （5人）
  2. 密码分析，GPU快速实现（3人）

  特点：理论研究，追踪世界前沿科研成果；
  与武汉其他高校和海外研究机构保持长期合作关系
  适合：对数学不反感，喜欢逻辑思考并勇于创新探索的学生
  目标：发表高水平国际期刊会议论文，撰写专利

  3. 区块链 （3人）
  4. 手机移动应用研发
  （Android，IOS） （3人）

  特点：有工业级项目支撑
  适合：较强的动手能力，特别是编程能力较好的学生
  目标：习得前沿的工业项目开发技能，撰写专利，发表论文