ENGG 5383 Applied Cryptography

Sherman Chow
Chinese University of Hong Kong
Fall 2020
Lecture 0: Logistics and Motivation

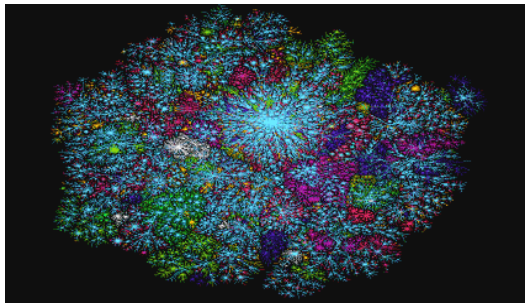
My Contact

- Email: smchow@ie.cuhk.edu.hk
  - Prepend subject of the email with [ENGG5383]
  - Use your institutional email for correspondences
  - I will not check my junk mail box
- Course website:
  - http://staff.ie.cuhk.edu.hk/~smchow/5383
  - redirected from course.ie.cuhk.edu.hk/~engg5383 (IE VPN)
- Teaching assistant: TBA
  - Tutorial session: TBA

What is Cryptography?

- From Greek: “kryptos” (secret) and “grapho” (writing)
- Originally, the “art” of “secret writing”
- You don’t know how to read
- You don’t know how to write
- Control access (learning & influencing) to “information”
- So, only cipher/encryption and (digital) signature?
- Much more!

Why study Cryptography?



- Data is always under transmission
- Internet/cloud storage
- Outsourcing computation/storage
- 500 million Facebook users
- 2 billion Internet users
- Everyone's data is digitalized!
  - personal info., credit card, health record, etc.

Data Confidentiality

- Many massive security breaches
- E.g., PlayStations got hacked (April 2011)
  - Sony said that the credit card numbers were encrypted, but the hackers might have made it into the main database [CNN]
- It is as secure as its **weakest link**.

I have faith. Why can't I trust in them?

- Conflict of interests
  - R&D, insider info, strategic plan
  - Government agencies
- The Law
  - Medical records (HIPAA)
    - Health Insurance Portability & Accountability Act
  - Financial records (SOX)
    - Sarbanes–Oxley Act

What are you trusting?

- Data is stored in more than one server
  - Trusting all servers / insiders / other tenants
- Relying on the server for access control
  - Horizontal or vertical privilege escalation
- A company have many employees
  - Careless/Cheating employees
- Encryption (number-theoretic assumptions?)

What this course is about

- Definitions & Constructions of many "Crypto. Objects"
- What are the algorithms involved?
- How to define the security properties?
- How to design objects that satisfy them?
- How to prove that the definitions are satisfied?

Nature of this course

- Graduate class
  - Self-motivation to learn is important!
- Mathematically inclined
  - No advanced Math. background is assumed
  - However, "mathematical maturity" is expected
    - comfortable with mathematical proof techniques
  - Knowledge of Basic Probability
  - Knowledge of Basic Concepts about Algorithms
  - A quick review of Number Theory will be given
- Covered as many tools as possible for your own problem

Applied Cryptography

- We construct systems that are practical and efficient.
- Found applications in various domains:
  - Cloud computing
  - Database
    - Searchable encryption
  - Distributed system
    - Electronic Cash, Bitcoin
    - Electronic Voting
  - Electronic Healthcare
    - Access Control of Patient Record
    - Outsourcing / Privacy-Preserving Pattern Matching
  - Power grid
  - Vehicular Ad-Hoc Network (VANET)
  - etc.

What this course is *not* about

- How to make your computer "secure"
- How to deploy a secure system
- How to crack a password-protected account

- How to implement HTTPS, SSH, SSL/TLS, IPsec, etc.
- What caused the vulnerabilities in Java, Intel, SGX, etc.

- We do not discuss cryptanalysis of "symmetric-key" primitives
  - E.g., hash function, pseudorandom number generator, AES, etc

Course outcome

- You know a suite of cryptographic tools for your problem.
- You know what you are talking about when you are saying "an (encryption) scheme XXX is secure".
- You can make sense out of a specification of cryptographic scheme and should be able to program it.
- You can "cryptanalyze" a cryptographic scheme.
  - Hopefully, your implementation will be free from any silly mistake.
- Be interested in cryptography!

Crypto. as a scientific discipline [Shamir]

Is thriving as a scientific area of research:

- Taught at most major universities
- Attracts many excellent students
- Discussed at many conferences
- Published in hundreds of papers (e.g., http://eprint.iacr.org)
- Major conferences have >500 attendees
  - (Major trade shows have >10,000 attendees)
- Received the ultimate seal of approval from the CS community
  - Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, 2002
  - Silvio Micali and Shafi Goldwasser, 2012
  - // Lesile Lamport (distributed system, designed Lamport signature), 2013

Cryptographic Conferences

- IACR Flagship Conferences: *Crypto, EuroCrypt, AsiaCrypt*
- IACR Specialist Conferences:
  - *CHES (Cryptographic Hardware and Embedded Systems)*
  - *FSE (Fast Software Encryption)*
  - *PKC (Public Key Cryptography)*
  - *TCC (Theory of Cryptography Conference)*
- Conferences in Cooperation with IACR (e.g.:) *AfricaCrypt, CANS, LatinCrypt, MyCrypt, Selected Areas in Cryptography (SAC), InsCrypt, Financial Crypt., Post Quantum Crypt.*
- Others: *ACISP, ACNS, ACSW-AISC, CT-RSA, ECC, ICICS, ICITS, ICISC, IndoCrypt, ISC, ISPEC, SCN, Pairing, ProvSec, Qcrypt, SCIS, SEC, SEcrypt, WISA, …*

Other Conferences with Crypto. Papers

- Security
  - ACM Conf. on Computer and Communications Security (CCS)
  - IEEE Security & Privacy (S&P/"Oakland")
  - Usenix Security
  - ISOC Network and Distributed System Security (NDSS)
  - ESORICS, EuroS&P, PETS, WiSec, SACMAT, …
- Network/Distributed Computing/WWW
  - IEEE Infocom
  - IEEE Intl. Conf. on Distributed Computing Systems (ICDCS)
  - ACM Principles of Distributed Computing (PODC)
  - The Web Conference
- Theory
  - IEEE Foundations of Computer Science (FOCS)
  - ACM Symposium on Theory of Computing (STOC)
  - ACM Conf. on Innovations in Theoretical Computer Science (ITCS)

Tentative Assessment

- 2 written assignments: 40%
- An (in-class open-note) mid-term exam: 20%
- (Group-)Project with report and presentation: 40%
  - Implementation / Survey
  - Cryptanalysis
  - Proposing new cryptosystem!
  - (2-student Group/Individual: Depending on the final class size)

Tentative Schedule (1)

- 02: Sep 17, Sep 18
  - Foundations, Basic Primitives
- 03: Sep 24, Sep 25
  - Public-Key Encryption (PKE) // then 1-week holiday
  - [Homework 1 assigned]
- 04: Oct 8, Oct 9
  - Hash Function, and Digital Signatures
- 05: Oct 15, Oct 16
  - Security Proof, Random Oracle Model
  - [Homework 2 assigned]
- 06: Oct 22, Oct 23
  - Zero-Knowledge Proof, Privacy-Enhancing Crypto. (Guest Lecture)

Tentative Schedule (2)

- 07: Oct 29, 30 --- Functional Encryption (& Project Intro.)
- 08: Nov 5, 6 --- [Mid-Term]
- 10: Nov 12, 13 --- Pairing, Anonymous Credentials
- 11: Nov 19, 20 --- Searchable Encryption
- 12: Nov 26, 27 --- Some Selected Topics
- 13: Dec 3, 4 --- Some Selected Topics
  - E.g.: proof of storage, computing on encrypted data, etc.
  - Also serve as sample presentation for the project
- Mid/Late-Dec: [Presentations]

Textbooks

- There is no required textbook for the course.
- Recommended textbook
  - Modern Cryptography: Theory and Practice by Wenbo Mao
- Many online resources
- Handbook of Applied Cryptography
  - http://cacr.uwaterloo.ca/hac
- A Computational Intro. to Number Theory and Algebra
  - http://shoup.net/ntb
- "Lecture Notes on Cryptography"
  - http://cseweb.ucsd.edu/users/mihir/papers/gb.html

Similar/ Related Courses Worldwide

- Brown University
- Massachusetts Institute of Technology
- New York University
- Stanford University
- University of California, Berkeley
- University of Maryland
- University of Texas, Austin
- University of Toronto
- University of Waterloo
- etc.

Class Policy

- Do your reading
- No plagiarism
  - at the very least, you need paraphrasing
- Work independently
  - discussion is allowed, but write your own solution
- Any questions?