ENGG 5383 Applied Cryptography

Sherman Chow
Chinese University of Hong Kong

Spring 2025

Lecture 0: Logistics and Motivation

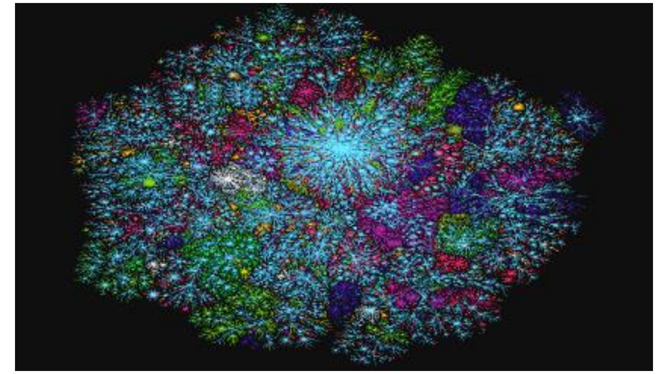
My Contact

- Email: smchow@ie
  - Prepend subject of the email with [ENGG5383]
  - Use your institutional email for correspondences
  - I will not check my junk mail box
- Course website: staff.ie.cuhk.edu.hk/~smchow/5383
- Office hours: Upon request
- Teaching assistant: Ying-yu Pan (py022@ie)

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

- ~3 billion Facebook users
  - was 500 million when I draft this slide
- 5 billion Internet users
  - was 2 billion a decade ago
- 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
  - **S**arbanes–**Ox**ley Act: Financial records
  - **H**ealth **I**nsurance **P**ortability & **A**ccountability **A**ct: Medical data
  - **C**alifornia **C**onsumer **P**rivacy **A**ct: Consumer records
  - **G**eneral **D**ata **P**rotection **R**egulation

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?)

Why still study cryptography?

- The 1st public-key cryptosystem (RSA) was proposed in '78 (multiplicative homomorphism, $E(a) * E(b) = E(a * b)$)
- The 1st practical Identity-based encryption in '01
- The 1st fully homomorphic encryption in '09
- Factoring -> Elliptic curve -> Lattice->Isogeny

- The rise of cryptocurrency / blockchain
- Cloud computing -> Edge computing -> Metaverse
- Increasing popularity of processing encrypted data, zero-knowledge proof (zkSNARK), *etc*.

Security is not the only requirement

- Confidentiality vs. Functionality
  - Searching over encrypted data
  - Processing encrypted data
    - *e.g.*, privacy-preserving machine learning
- Authenticity vs. Privacy
  - Privacy-preserving contact tracing
  - Anonymous credentials
- Even availability and sustainability!
  - Stay tuned

What is Applied Cryptography?

- Foundation in Theory:
  - grounded in theoretical cryptography (*cf*., applied math grounded in math)
  - understanding proofs, algorithms, and mathematical structures is essential
- Application-Oriented Mindset:
  - focuses on solving real-world problems (vs. purely theoretical exploration)
- Interdisciplinary Knowledge:
  - mathematics (*e.g.*, number theory, algebra),
  - computer science (*e.g.*, complexity theory, data structure, algorithm), and
  - engineering for practical implementation, *etc*.
- Proofs with Purpose:
  - formal security guarantees (vs. handwavy, error-prone arguments)

What is Applied Cryptography? (cont.)

- Balancing Security, Efficiency, and Functional Requirements
- Adaptability:
  - understand evolving threats and technologies
  - to design robust solutions in practice
- Practical Constraints:
  - *e.g.*, processing power, memory, and network latency
- Hands-On Implementation:
  - *e.g.*, coding with special libraries, deployment, *etc*.
- Real-World Impact:
  - directly influences critical fields like finance, healthcare, government, democracy, social good, *etc*., making it a high-stakes discipline.

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

- Self-motivation to learn is important in a graduate class!
- Mathematically inclined
  - No advanced math. background is assumed
  - However, "mathematical maturity" is expected
    - familiarity with logics and comfortable with mathematical proof
    - *e.g.*, logic operators (AND, OR, XOR), proof technique: *e.g.*, contrapositivity
  - Knowledge of Basic (Discrete) Probability
    - perhaps some simple combinatorics
  - You should recall/revisit your middle-school (?) math
    - *e.g.*, power arithmetic
  - A quick review of Number Theory will be given
    - revisit your primary-school (?) math, *e.g.*, simple modular arithmetic
- Covered as many tools as possible for your own problem

Introduction to Cryptography

- Security against *computationally-bounded* adversary
  - also known as (a.k.a.) *probabilistic polynomial-time* adversary
- "Symmetric-Key Primitives"
  - Pseudorandom Generator (PRG)
  - Pseudorandom Function (PRF)
  - Pseudorandom Permutation (PRP)
- Hash Functions
- "Public-Key Primitives"
  - One-way Function/Permutation (OWF/OWP)
  - Trapdoor Permutation (TDP)
  - Modeling security of Public-Key Encryption
- Oblivious Transfer, Garbled Circuit

Applied Cryptography

- We construct systems that are practical and efficient with applications in various domains:
  - Cloud computing
  - Database
    - Searchable encryption
  - Distributed system
    - Bitcoin/Blockchain
  - Electronic Healthcare
    - Access Control of Patient Record
    - Outsourcing / Privacy-Preserving Machine Learning
  - Cyber physical systems
    - Selling or buying power in power grid
  - Vehicular Ad-Hoc Network (VANET)
    - Anonymous Communication of traffic conditions
  - *etc*.

What this course can possibly cover?

- online identity and authentication management
- e-cash (not just cryptocurrency)
- cloud computing security and privacy
- secure outsourcing of data and computation
- data provenance
- e-voting systems
- digital rights management
- secure and anonymous routing systems
- geolocation privacy

Interdisciplinary

- Anonymous Reputation System
  - Internet forum, decentralized autonomous organization
- Collaborative Filtering
- Queries over (Distributed) Databases
- Machine learning
  - Decision tree, neural network, transformer
- Data aggregation
  - Federated learning, smart grid
- Online Games Hacking Prevention

How to study so many in one course?

- Learn how to learn
- But what exactly you are going to learn?

- My jobs:
- Introduce the problem scenarios
- Abstract the requirement
  - under the "same" framework
  - distill some "essential" elements
  - with the "same methodology"
- Equip you with the necessary background

What this course is *not* about

- How to make your computer "secure"
- How to securely implement crypto lib. / deploy a secure system
- How to hack, *e.g.*, crack a password-protected account

- We do not discuss specific crypto software or Internet protocols
  - *e.g.*, HTTPS, SSH, SSL/TLS, IPsec, PGP, Tor, Signal, Bitcoin, BitLocker, ...
- What caused the vulnerabilities in TEE (*e.g.*, 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.*, https://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, Privacy
  - ACM Conf. on Computer and Communications Security (CCS)
  - IEEE Security & Privacy (S&P/"Oakland")
  - Usenix Security
  - ISOC Network and Distributed System Security (NDSS)
  - ACSAC, CODASPY, CSF, ESORICS, EuroS&P, PETS, RAID, SACMAT, WiSec, …
- Network/Distributed Computing/WWW
  - IEEE Infocom
  - IEEE Intl. Conf. on Distributed Computing Systems (ICDCS)
  - ACM Principles of Distributed Computing (PODC)
  - ACM 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)
  - IEEE International Symposium on Information Theory (ISIT)

5 Key Expectations

- Class/Online Participation: 5%
  - Do your background reading! (Very important)
  - You need to think, instead of being spoon-fed.
  - Simple questions on http://ureply.mobi
- 2 written assignment: 20%
- (Open-everything) Mid-term exam: 25%
  - Make sure your progress / understanding is good

"Regular" Course-Work (50%)

You need to pass both!

- After you've identified what interests you (& your friends) the most…
- A project proposal: 10%
- An in-class/online 15-20 min presentation: 20%
- Final report: 20%

"Advanced" Research (50%)

Nature of the Project

- Ultimate goal: applying what you have learned,
  - possibly with my help
  - or your groupmates not taking this class (w/ proper declaration)

Publish in the venues you care!

- Implementation / Survey
- Cryptanalysis
- Proposing new cryptosystem!
  - combining features from different works
  - hopefully a somewhat non-trivial combinations

Nature of the Project (cont.)

- Research, or Implementation, or Both

- Through understanding -> Survey -> Original result (Bonus)
- Through understanding -> Learn the Library -> Prototype

- Can be group project (Depending on the final class size)

Paper Reading / Presentation

- The papers are presenting the latest advances
- not meant to be served as a textbook to teach you
- *i.e.*, you need to have multiple passes of the same paper
  - Overall picture -> Components of the work -> Technical Details

- Consultation hour to help you go through it
- You may need to read more to understand it
  - I will give you the hints / pointers

- Understanding and presenting are different things…
  - (or actually you don't really understand)
- Pre-presentation (or rehearsal, with me) to make it perfect

Sample Topics (of IERG5130 in 2019)

- 2. Cryptographic Primitives
- 3. Hardware-assisted Approach
- 4. Access-Control & Functional Encryption
- 5. Privacy-Enhancing Technologies
- 6. Democracy-Enhancing Technologies
- 7. Privacy-Preserving Machine Learning
- 8. Electronic Payment
- 9. Password-Hardening
- 10. Cloud Cryptography

Tentative Schedule

- Weeks 2-3: Foundation of Cryptography
- 1 Week holiday: Assignment 1
- Week 5: Assignment 2
- Week 7: Mid-term
- Week 8: Proposal due
- Week 10: Pre-presentation due
  - problem introduction, survey
- Mid/Late April: Final presentation and Final report

Textbooks

- The Joy of Cryptography // *the following 2 weeks will mostly follow this textbook*
  - https://joyofcryptography.com
- Another suggested textbook: Introduction to Modern Cryptography
  - http://www.cs.umd.edu/~jkatz/imc.html
- A Graduate Course in Applied Cryptography
  - http://toc.cryptobook.us
- Handbook of Applied Cryptography
  - http://cacr.uwaterloo.ca/hac
- A Computational Intro. to Number Theory and Algebra
  - http://shoup.net/ntb
- "Lecture Notes on Introduction to Cryptography" (CMU)
  - https://cs.cmu.edu/~goyal/15356/lecture_notes.pdf
- "Lecture Notes on Cryptography" (UCSD)
  - https://cseweb.ucsd.edu/~mihir/papers/gb.pdf

Class Policy

- Do your reading
- No plagiarism
  - at the very least, you need *paraphrasing*
- Work independently
  - discussion is allowed, but write your own solution
- Acknowledgments of existing ideas, material, *etc*.
- Declaration of usage of any helping tools, to what extent
  - *e.g.*, generative AI
- Any questions?

Paper list in IERG5310 '19 (most covered)

Processing Encrypted Data

Jiafan Wang, *Sherman S. M. Chow*: Secure Strategyproof Ascending-Price Spectrum Auction. PAC 2017: 96-106.

Peizhao Hu, *Sherman S. M. Chow*, Asma Aloufi: Geosocial query with user-controlled privacy. WISEC 2017: 163-172.

Hardware-/Servers-assisted Approach

Minxin Du, *Sherman S. M. Chow*, Qian Wang, Xiang Yue: [Still under submission and hence redacted]. 2019.

Boyang Wang, Ming Li, *Sherman S. M. Chow*, Hui Li: A Tale of Two Clouds: Computing on Data Encrypted under Multiple Keys. IEEE CNS 2014: 337-345.

S. S. M. Chow, Jie-Han Lee, Lakshminarayanan Subramanian: Two-Party Computation Model for Privacy-Preserving Queries over Distributed Databases. NDSS 2009

Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, Sergey Gorbunov: IRON: Functional Encryption using Intel SGX. ACM CCS 2017: 765-781.

Access Control Encryption and Functional Encryption

Xiuhua Wang, *Sherman S. M. Chow*: Cross-Domain Access Control Encryption: Arbitrary-policy, Constant-size, Efficient. S&P 2021:748-761Michel Abdalla, Florian Bourse, Angelo De Caro, David Pointcheval: Simple Functional Encryption Schemes for Inner Products. Public Key Cryptography 2015: 733-751.

Dan Boneh, Amit Sahai, Brent Waters: Functional encryption: a new vision for public-key cryptography. Commun. ACM 55(11): 56-64 (2012).

Georg Fuchsbauer, Romain Gay, Lucas Kowalczyk, Claudio Orlandi: Access Control Encryption for Equality, Comparison, and More. Public Key Crypto.(2) 2017: 88-118.

Ivan Damgård, Helene Haagh, Claudio Orlandi: Access Control Encryption: Enforcing Information Flow with Cryptography. TCC (B2) 2016: 547-576.

Privacy-Enhancing Technologies

Yongjun Zhao, *Sherman S. M. Chow*: Can You Find The One for Me? WPES@CCS 2018: 54-65.

Yongjun Zhao, *Sherman S. M. Chow*: Are you The One to Share? Secret Transfer with Access Structure. PoPETs 2017(1): 149-169 (2017).

Yongjun Zhao, *Sherman S. M. Chow*: Privacy Preserving Collaborative Filtering from Asymmetric Randomized Encoding. Financial Cryptography 2015: 459-477.

Amit Datta, Marc Joye, Nadia Fawaz: Private Data Aggregation Over Selected Subsets of Users. CANS 2019: 375-391.

Elie Bursztein, Mike Hamburg, Jocelyn Lagarenne, Dan Boneh: OpenConflict: Preventing Real Time Map Hacks in Online Games. IEEE Security & Privacy 2011: 506-520.

Democracy-Enhancing Technologies

S. Chow, A. Russell, Q. Tang, M. Yung, Y. Zhao, H.S. Zhou: Let a Non-barking Watchdog Bite: Cliptographic Signatures with an Offline Watchdog. PKC (1) 2019: 221-251.

Tao Zhang, Huangting Wu, *Sherman S. M. Chow*: Structure-Preserving Certificateless Encryption and Its Application. CT-RSA 2019: 1-22.

Russell W. F. Lai, Raymond K. H. Tai, Harry W. H. Wong, *S. Chow*: Multi-key Homomorphic Signatures Unforgeable Under Insider Corruption. AsiaCrypt (2) 2018: 465-492.

Jeremy Clark. Democracy Enhancing Technologies: Toward deployable and incoercible E2E elections. PhD Thesis. University of Waterloo, 2011. 247 pages.

Sherman S. M. Chow, Joseph K. Liu, Duncan S. Wong: Robust Receipt-Free Election System with Ballot Secrecy and Verifiability. NDSS 2008.

Electronic Cash

Sherman S. M. Chow, Ming Li, Yongjun Zhao, Wenqian Jin: Sipster: Settling IOU Privately and Quickly with Smart Meters. ACSAC 2021: 219-234.

E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza: Zerocash: Decentralized Anonymous Payments from Bitcoin. IEEE S&P 2014: 459-474.

Jan Camenisch, Susan Hohenberger, Anna Lysyanskaya: Compact E-Cash. EUROCRYPT 2005: 302-321.

Privacy-Preserving Machine Learning

Lucien K. L. Ng, *S. S. M. Chow*, Donald P. H. Wong, Anna P. Y. Woo, Yongjun Zhao: Goten: GPU-Outsourcing Trusted Execution of Neural Network Training. AAAI 2021.

Florian Tramèr, Dan Boneh: Slalom: Fast, Verifiable and Private Execution of Neural Networks in Trusted Hardware. ICLR 2019.

Raymond K. H. Tai, Jack P. K. Ma, Yongjun Zhao, *Sherman S. M. Chow*: Privacy-Preserving Decision Trees Evaluation via Linear Functions. ESORICS (2) 2017: 494-512.

Password-Hardening

R.W.F. Lai, C. Egger, M. Reinert, *S.S.M. Chow*, M. Maffei, D. Schröder: Simple Password-Hardened Encryption Services. USENIX Security Symposium 2018: 1405-1421.

Russell W. F. Lai, Christoph Egger, Dominique Schröder, *Sherman S. M. Chow*: Phoenix: Rebirth of a Cryptographic Password-Hardening Service. USENIX Sec. 2017: 899-916.

Cloud Storage

Matteo Maffei, Giulio Malavolta, Manuel Reinert, Dominique Schröder: Maliciously Secure Multi-Client ORAM. ACNS 2017: 645-664.