# Cryptography Final Project

## Presentation Schedule

The presentations will be done over the regular zoom link for the lectures. You can prepare slides or use a shared whiteboard. Please try to attend all the presentations and participate in the discussion.

**Tuesday December 8, 9.30-10.30**

| | |
|---|---|
| 9.30 - 9.42 | Shiyuang Deng: Oblivious RAM |
| 9.42 - 9.54 | Yinxi Liu: The Cans and Cannots: Why Cryptographic Obfuscation is not yet Optional? |
| 9.54 - 10.06 | Qinghua Devon Ding: On the share size of monotone access structures A and it dual A* |
| 10.06 - 10.18 | Ruiyuan Gao, Yijun Yang: How cryptography can help AI & ML and the challenge of them |

**Tuesday December 8, 10.30-11.30**

| | |
|---|---|
| 10.30 - 10.42 | Shengju Qian, Liying Lu: Learning Based Communications Protection with Neural Cryptography |
| 10.42 - 10.54 | Fung Chung Kit: Code-Based Public-Key Cryptography |
| 10.54 - 11.06 | Cheung Tsun Ming, Tang King Hei: Lattice-based cryptography |
| 11.06 - 11.18 | Tsun-Yu Yang: The impact of quantum computing and how we should deal with it |

**Wednesday December 9, 9.30-10.30**

| | |
|---|---|
| 9.30 - 9.42 | Zhao Jia: Hash-based signatures |
| 9.42 - 9.54 | Xin Deng: Introduction to ECDSA |
| 9.54 - 10.06 | Yicheng Xie, Runyue Huang: Introduction to Stream Ciphers Attacks |
| 10.06 - 10.18 | Mui Hong Yin: A survey of cryptographic accumulator schemes and applications |

**Wednesday December 9, 10.30-11.30**

| | |
|---|---|
| 10.30 - 10.42 | Yu Zheng: What cryptography can do in private prediction? |
| 10.42 - 10.54 | Zhuolun He: Logic obfuscation |
| 10.54 - 11.06 | Jinming Wu: Implementation & Experimentation of Yao's Garbled Circuit Protocol for Two-Party Computation |
| 11.06 - 11.18 | Tao Hu, Zetong Yang: An implementation of the RSA encryption scheme |

## Project type

Here are some types of projects you can do. If none of these fit your needs you can propose your own. You can do the project individually or with a partner. You will need to submit a report and present your findings in class.

**Survey project.** The purpose of this type of project is to survey a small slice of cryptography and present your findings to the class. Example topics might be a survey of proposed two-party computation schemes, the NIST post-quantum crypto competition https://csrc.nist.gov/Projects/Post-Quantum-Cryptography, proofs of work or any topic of your choice.

**Teaching project.** You can pick a "textbook" crypto topic that we didn't cover in class and present it, for example: practical constructions of pseudorandom functions or hash functions, composition of cryptographic protocols, private information retrieval, oblivious RAM, pseudorandom generators from one-way functions, or indistinguishability obfuscation. A starting point could be the textbooks and lecture notes listed on the web page but you may need to go beyond that and dig a bit deeper on the internet.

**Experimental or implementation project.** Try out implementing some one or several cryptographic protocols and discuss your findings about their efficiency, implementation challenges, and so on. One example is a secure two-party computation of a function of your choice. You can use existing packages you find online, write your own code, or do both and compare performance.

**Research project.** There are lots of open problems in crypto from the super-theoretical (is secure encryption possible at all) to the very applied (how to speed up bitcoin transactions or make mining less wasteful). If you don't know where to start but want to try, start by checking out the humongous Cryptology e-print archive https://eprint.iacr.org/ (but be selective because some of these papers haven't been reviewed). This is a good source for the other types of projects too.  You are not expected to produce a new research result by the end of the semester, but you should understand the problem deeply enough so you get a good sense of which strategies might work and which definitely won't.

## Timeline

**Friday November 6.** Find your partner, identify your project, and add the title and short description to this document. Please avoid duplicating projects. If you are looking for a partner you can advertise below or use the "find a project partner" function on piazza.

**Monday December 7.** ~~Friday December 4.~~ Please turn in a draft of your report here.

**Tuesday December 8 and Wednesday December 9.** Class presentations. I expect that each group should have about 10-15 minutes to present followed by a 5-minute discussion. It is important that you have a clear point in mind and deliver it well. You may use slides, the board, or nothing at all. If there is no interest in discussion I may ask a member of the audience to summarize what they learned from your talk.

**Friday December 11.** Turn in a final copy of your report. There is no length requirement. Focus on the quality of the writing. The report should be at a level accessible to a student who has attended CSCI 5440 but does not have any knowledge beyond that.

## Partner search

If you are looking for a project partner, you can write a bit about your interests here.

## Projects

Please write down your name(s), the title of your project, and a short description by **Friday November 6**.

Name: Jinming Wu (SID: 1155150570)
Title: Implementation & Experimentation of Yao's Garbled Circuit Protocol for Two-Party Computation
Type: Implementation
Description: This is an implementation of Yao's garbled circuit protocol for Two-Party Computation using Python and the evaluation of its efficiency with comparison of the existing libraries (for example, `jigg`).

Name: Qinghua Devon Ding
Title: On the share size of monotone access structures A and it dual A*
Description: Given a linear sharing scheme for monotone access structure A, we can always construct another linear sharing scheme for A* with the same share size. Such construction can be derived via the equivalence between linear secret sharing and monotone span programs. Now consider a more general setting. We define s(A) as the minimum share size for 1-bit secret over all secret sharing schemes. If we limit our attention to linear sharing schemes, then previous results imply s(A)=s(A*). However, does s(A)=s(A*) in general? We'll look into this problem and try to find the correct tools to study it.

Name: Yu Zheng (SID: 1155113945)

Topic: What cryptography can do in private prediction?
Type: Survey
Description: Private prediction using neural networks is a branch of privacy-preserving deep/machine learning. For example, a patient (client) expects to know whether he is sick by asking a hospital (server). The server already has a model for prediction (e.g., disease diagnosing), while a client inputs a query to a model and then gets the output. The security refers to the client keeps the input/output private and the server protects the model privacy (This is very general). A kind reminder is that this topic does not consider the training phase, where a model is generated from scratch over some specific data distributions.
In this course, we have learned homomorphic encryption, secret sharing, garbled circuits, and etc. Different cryptographic tools play different roles for various functions in private prediction, e.g., homomorphic encryption efficient for linear operations. Our goal is to outline the main works in this topic and make a classification. And then, we will point out some potential research ideas/directions.

Name: Yinxi Liu (SID: 1155149728)
Title: The Cans and Cannots: Why Cryptographic Obfuscation is not yet Optional?
Description: Program obfuscation has long been an appealing subject for software developers and cryptographers. Intuitively, we should send user programs they can execute, without letting them know how the programs work. This leads to the definition of "virtual black box (VBB) obfuscation". However, Barak et al. have shown that this definition does not work in practice. Specifically, they prove that there is a deterministic private-key encryption scheme that is unobfuscatable in the sense that, given any encryption program with a private key embedded, one can efficiently compute the private key. Later, researchers tried to find certain functions for which we can build black-box obfuscation, or lose the definition so that we can produce a general obfuscation construction algorithm. Two loosed definition: indistinguishability obfuscation (IO) and extractability obfuscation (EO) show the potential of a wide application.

Name: Xin Deng (student ID:1155150821)
Project Type: Survey
Topic: Introduction to ECDSA
Description: In this project, I am going to introduce ECDSA briefly, which is a cryptographic algorithm to generate digital signature of data in order to allow users to verify its authenticity without compromising its security. It has been used by Bitcoin to ensure that funds can only be spent by their rightful users.

Name: Ruiyuan GAO (SID: 1155157018), Yijun YANG (SID: 1155140307)
Title: How cryptographic can help AI & ML and the challenge of them
Type: Survey

Description: The development of the Artificial Intelligence (AI) and Machine Learning (ML) method largely increases what we can do in regard to massive data. However, in the deployment stage of the AI system, there are potential risks for involved parties. For example, system user's privacy, system designer's intellectual property, and computation parties all need secure environments to operate and communicate. This is how cryptographic comes into the stage. On the other side, some researchers are trying to use the great power of the AI system to design cryptanalysis. However, in theoretical cryptographic, there are several proved to be secure under learning strategies. That's the limitation of AI and ML methods.
In this project, we want to conduct a survey from both sides. First, we investigate where cryptographic strategy (e.g., secure Multi-Party Computation and Homomorphic Encryption) can be used in recent AI systems. Second, we want to know how secure the cryptographic method (e.g., LPN, LWE) is against the attack of the AI system. And what an AI system can help to construct cryptanalysis.

Name: Fung Chung Kit (SID: 1155129885)

Title: Code-Based Public-Key Cryptography

Type: Teaching project / Survey

Description: The first Code-Based Cryptography was introduced in 1978 by McEliece. Its security level has remained stable over 40 years. It can against quantum computers by scaling up its parameters against advances in computer technology. A lot of work in Post-Quantum Cryptography is based on the code-based method. I would want to first revisit McEliece work. Then using a nowadays code-based quantum resistant Public-Key cryptography (from Post-Quantum Cryptography) as example, to show how code-based public key cryptography evolved to against the advances in computer technology.

Name: Tsun-Yu Yang (SID:1155131469)
Title: The impact of quantum computing and how we should deal with it
Type: Survey
Description: Quantum computing is the use of quantum phenomena such as superposition and entanglement to perform computation. Some believe that quantum computers are able to solve certain hard problems, such as integer factorization in RSA encryption, in a much faster way

than the classical computers. That is to say, if large-scale quantum computers are built, they could break many of the public-key encryption schemes that are currently used, which could compromise the integrity of Internet communication. Therefore, in this survey, I would like to know what quantum computing is, how it can break some hard problems fast, when a large-scale quantum computer will be eventually built, and how we should re-design our cryptography system from being hacked by the quantum computer.

Name: ZHAO Jia (SID:1155145513)
Title: Hash-based signatures
Type: Survey/Teaching
Description: Hash-based signatures recently gained a lot of attention as a potential replacement for today's signature schemes when large-scale quantum computers are built. The main reason probably consists in the reliable security estimates — also for security against attacks aided by quantum computers. This distinguishes hash based signatures from other post-quantum signature schemes.  What's more, hash-based signatures need no computationally expensive mathematical operations like big integer arithmetic. The only requirement is a secure cryptographic hash function. In this project, we will look into hash-based signature schemes, like the Lamport's OTS, WOTS, WOTS+, XMSS.

Name: Shiyuan DENG (SID:1155092079)
Title: Oblivious RAM
Type: Survey/Teaching
Description:
Will survey the oblivious RAM literature. Will present the oblivious RAM in both hase based protocol and probability based protocol.

Name: Yicheng Xie (SID:1155145498) /Runyue Huang (SID:1155149033)
Topic: Introduction to Stream Ciphers Attacks
Type: teaching
Description: This project aims to bring an elementary introduction to the cryptanalysis of stream ciphers, which is a popular encryption algorithm in daily life. First, we will introduce some information about Stream Cipher. Stream cipher is achieved by applying XOR operation, with excellent performance. Therefore, it is quite favoured by many developers. Next, we will introduce two specific attacks against this type of encryption, named "Reused Key Attack" and "Bit-flipping Attack".

At last, we will demonstrate an attack on WEP protocol, which used to be a popular wireless LAN encryption protocol. The nature of WEP attack is exactly based on the weakness of stream ciphers.

Name: Mui Hong Yin (SID: 1155154518)
Project type: Survey/Teaching project
Title: A survey of cryptographic accumulator schemes and applications
Description:
Cryptographic accumulator is a one way membership function. It composes a set of values into a short binding commitment and allows to generate a membership/non-membership proof based on the short binding commitment. In this project, we will revisit the proposed schemes of accumulator and the application of the accumulator.

Name: Shengju Qian (SID: 1155136875), Liying Lu (SID: 1155136878)
Title: Learning Based Communications Protection with Neural Cryptography
Type: Survey
Description:
We survey whether neural networks can learn to use secret keys to protect information from other neural networks, which has been discussed in recent literature. In this setting, specific cryptographic algorithms to these neural networks are not prescribed ; instead, three neural networks, representing Alice, Bob and Eve, will be trained end-to-end. Alice and Bob will communicate with each other by encrypting and decrypting the messages and try to protect the confidentiality of their data from Eve. While Eve will try to reconstruct the plaintext as accurately as possible. The networks are trained in an adversarial way to learn the correct data distributions. In this project, we demonstrate that neural networks can learn to protect communications.

Name: Tao Hu (SID: 1155136880), Zetong Yang (SID: 1155137928)
Title: An implementation of RSA encryption scheme.
Type: Implementation project
Description: In this project, we will try to implement the RSA encryption scheme in python. RSA is a public-key cryptosystem that is widely used for secure data transmission. In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers. The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are

no published methods to defeat the system if a large enough key is used. We are going to implement the RSA encryption scheme in python language and explore the challenges and time efficiency and security. Also, we will compare it with the standard RSA library and report the differences.

Name: Cheung Tsun Ming (SID:1155062384), Tang King Hei (SID: 1155093581)
Title: Lattice-based cryptography
Type: Survey/Teaching
Description: Lattice-based cryptographic schemes involve lattices in constructions or security proofs. Different lattice-based cryptographic schemes have been devised based on the hardness of well-studied lattice problems. Several classical cryptographic schemes like RSA, Diffie-Hellman cryptosystems are thought to be insecure against quantum computers, while lattice-based cryptosystems remain to be candidates for post-quantum cryptography. In this project, we will go through the basics and mathematical foundation of lattice-based cryptography, and the possible implication of development in quantum cryptography.

Name: Zhuolun He (SID:1155136879)
Title: Gate-level Netlist Reverse Engineering
Type: Research
Description: We aim to extract word-level information from gate-level netlists. To simplify our discussions, we reduce the problem to identifying target structures (e.g., adders) in the netlist. Previous works proposed to use structural/functional information for extraction, mainly targeting simple adder structures (e.g., ripple carry adders). We want to extend the idea for more structures, and with new techniques.