Advanced Topics in Applied Cryptography

Instructor:	Yupeng Zhang
Time:	TuTh 5:00-6:20 pm
Location:	2015 ECEB
Website:	https://starzyp.github.io/ECE598_Fall2023/

Course Description

This course covers techniques in applied cryptography and their applications in machine learning and blockchain to enhance privacy, integrity and scalability. In this course, we will explore the cutting-edge cryptographic techniques such as zero-knowledge proofs and secure multiparty computations. We will discuss the basic concepts and state-of-the-art constructions of these cryptographic schemes. Additionally, we will talk about how to use these techniques to construct privacy-preserving blockchain and crypto-currencies, zkRollups and zkEVM, privacy preserving machine learning and zero-knowledge proofs for machine learning. We will focus on efficiency and scalability constraints in practice, and discuss challenges and solutions to efficiently realize these cryptographic protocols.

The course has no specific prerequisites. Basic knowledge of algorithms and complexities, data structures and programming is recommended.

Course Learning Outcomes

- Students will be able to formally define desired security properties of the cryptographic primitives.
- Students will be able to describe basic mechanisms of blockchain, cryptocurrencies and smart contracts.
- Students will be able to identify security problems in existing techniques and apply cryptographic tools to solve these problems.
- Students will be able to develop and implement efficient cryptographic protocols tailored for real-world applications.

Textbook and/or Resource Materials

No textbook is required for the course. Reading materials will be posted online during the semester.

Grading Policy

- A: >= 90%, B: < 90% and >=80%, C: < 80% and >=70%, D: <70% and >=60%, F: <60%
- Class Participation (10%)
- Reading assignment (30%): Students will submit reviews for one of the reading materials every 1-2 weeks. The reviews should include a brief summary of the paper, the contributions and potential improvements.
- Project (60%): Students will form groups and complete research projects related to the topics of the course. The grading consists of a project proposal, a mid-term progress report, a final presentation and a final project report. Students may propose their own topics or choose from a

list of suggested topics on secure multiparty computations, verifiable computations and zero knowledge proof, privacy-preserving machine learning and blockchain.

- Proposal (10%)
- Mid-term report and presentation (10%)
- Final presentation (20%)
- Final report (20%)

Late Work Policy

Late homeworks are not accepted and are worth 0 points. If you have an extended excused absence (per rule 7) that prevents you from completing a homework, please coordinate with the professor as soon as possible for a make-up.

Course Schedule

Week	Topic	Required Reading	Assignments
1	Introduction to basic cryptography. Discrete math, symmetric-key encryptions, public key encryptions, hash functions		
2	Verifiable Computations and zero-knowledge proofs	Merkle 79	
3	Overview of blockchain and cryptocurrencies	Nakamoto white paper	Project proposal due
4	Interactive proofs	Goldwasser et al. 15, Cormode et al. 12, Zhang et al. 17	
5	Privacy-preserving crypto-currencies and smart contracts	Ben-Sasson et al. 14 Kosba et al. 16	
6	Generic verifiable computations and zero knowledge proofs	Parno et al. 13, Groth16	
7	Zero knowledge proofs for machine learning		
8	Mid-term project presentation		
9	Secure Multiparty Computations, Oblivious transfer and Garbled circuits	Yao 86,	
10	GMW protocols	Goldreich et al. 87	
11	Privacy-preserving Machine Learning	Mohassel et al. 17	
12	Advanced topics such as malicious security, fairness and delivery of output		
13-14	Final project presentation		
			Final report due