ADVANCED CRYPTOGRAPHY ZERO-KNOWLEDGE PROOFS (AND APPLICATIONS

CS499/CS695: Advanced Cryptography

George Mason University, Computer Science, Spring 2022

Instructor: Prof. Foteini Baldimtsi (foteini@gmu.edu)

Office Hours: Thursdays 1:30PM-3:30PM, Engineering 5333

Lectures: Tuesdays 4:30PM-7:10PM, Location: Music/Theater Building 1006

FoteiniBaldimtsi

The course will provide an introduction to zero-knowledge (ZK) proofs - a fundamental tool of cryptography with many applications in both theory and practice. The main idea of a ZK proof is to allow a party (usually called ``the prover''), to prove an assertion without revealing anything but the fact that it is indeed true. In this class we will investigate the foundations of ZK proofs: we will start by discussing proofs-of-knowledge and move into adding the zero-knowledge property. We will cover security definitions and their variations (completeness, soundness and ZK, witness-indistinguishability etc) and we will study and prove clasic types of protocols and transformations such as Sigma-protocols, the Fiat-Shamir paradigm and succinct ZK proofs (SNARKs). Finally we will look into how ZK is being used in practice by looking into applications such as efficient secure computation, anonymous credentials, and privacy-preserving blockchains.

Objectives

The main objective of the class is to teach students an advanced cryptographic primitive and allow them to explore different classes of definitions and cryptographic assumptions and proof techniques. Additionally, students will learn how ZK proofs are used in practice in real-world employed systems.

Course Outcomes: Students taking this class will be able to: (a) understand the security properties achieved by ZK proofs, (b) be familiar with a number of concrete protocols (toolbox) and, (c) gain some experience on how cryptographic tools are used to secure modern systems such as cryptocurrencies.

Prerequisites: There is not hard prerequisite for this course but being familiar with material taught on CS 330, CS487 or CS600 and CS587 . Students will need some level of mathematical maturity, i.e. being familiar with concepts in probability theory (computation of expectation, conditional probability etc) and complexity theory (Turing machines, NP-completeness etc) would be helpful for an easier understanding of formal security definitions and proofs.

Relevant Materials

There is not textbook for the class but below are some useful tutorials, papers that we will go through:

- Zero-Knowledge: a tutorial by Oded Goldreich (2010 version)
- A study of statistical ZK proofs by Salil Vadhan
- The BIU winter school on Zero-Knowledge
- Proofs Algorithms and Zero-knowledge (Justin Thaler)

This class will run on a seminar format. The first 4-5 weeks will be focused on covering the fundamentals of the ZK by going through the classic definitions and constructions.

Assignments: 10% (2 assignments in the first 4 weeks)

Paper Presentation: 40% (after the 5th week, every student will select a paper to present in class, the presentation can happen by slides and/or whiteboard).

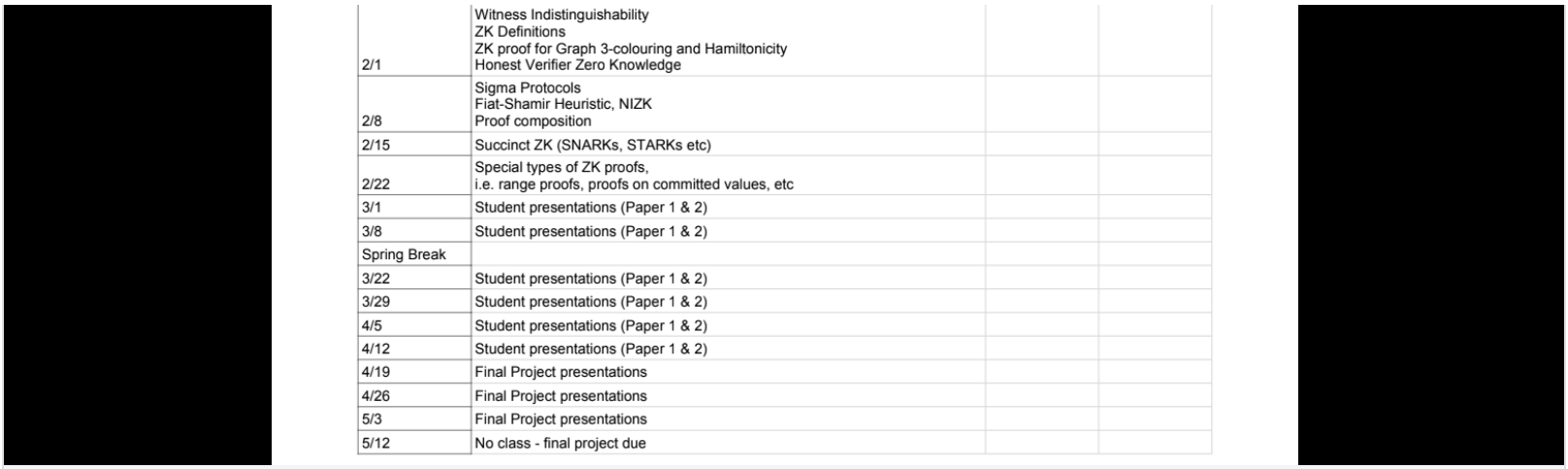
Class/Forum Participation: 10% (during student run presentations, every student needs to read through the assigned paper for the week and send to the presenter (CCing professor) 2 questions on the paper. This needs to happen by noon on Mondays.

Final Project: 40% Final projects will be selected by the end of February. Students can work alone or in groups. A final project can either be research oriented, systemizing knowledge on a specific type of proofs or implementation based.

Graduate Students (CS 695): Graduate students are expected to work on a research oriented project. Students at 499 level can work on a final project that focuses on better exposition/presentation of known results.

Communications: We will use Piazza to communicate with you. If you have a question about the course you should: (a) Come to office hours, OR (b) Post on Piazza. We have already set up different tags for HW problems and lectures. Please don't use private posts/emails to ask technical questions. The rest of the class is probably also interested in your question, so make it public!

Class Schedule (TBA):



2/1	Witness Indistinguishability ZK Definitions ZK proof for Graph 3-colouring and Hamiltonicity Honest Verifier Zero Knowledge		
2/8	Sigma Protocols Fiat-Shamir Heuristic, NIZK Proof composition		
2/15	Succinct ZK (SNARKs, STARKs etc)		
2/22	Special types of ZK proofs, i.e. range proofs, proofs on committed values, etc		
3/1	Student presentations (Paper 1 & 2)		
3/8	Student presentations (Paper 1 & 2)		
Spring Break			
3/22	Student presentations (Paper 1 & 2)		
3/29	Student presentations (Paper 1 & 2)		
4/5	Student presentations (Paper 1 & 2)		
4/12	Student presentations (Paper 1 & 2)		
4/19	Final Project presentations		
4/26	Final Project presentations		
5/3	Final Project presentations		
5/12	No class - final project due		

Class Schedule

Honor code: All students must adhere to the GMU Honor Code. You can discuss lecture material with other students in class but you have to work on the assignments alone. More specifically for this class: (1) I encourage discussions between students on the homework problems but you have to write your solutions completely on your own, without looking at other people's write-ups. (2) You are welcome to use any textbooks, online sources, blogs, research papers, Wikipedia, etc to better understand a notion covered in class or in a homework question. If you do so you have to properly cited it in any submitted work. Failure to do this is plagiarism and is serious violation of the GMU Honor Code and basic scientific ethics, and will not be tolerated. Note that it is not OK to search for solutions to HW problems online.