Math 480A2: Mathematics of Blockchain Protocols

PRELIMINARY DRAFT, SUBJECT TO CHANGE

Course Details

Instructor: Bryan Gillespie, Bryan.Gillespie@colostate.edu

Class time and location: TR 8:00–9:15 am, C364 Clark Building

Course web page: `http://bgillespie.com/courses/m480a2-f22/index.html`

Office hours: T 9:30–10:30 am, R 10:30–11:30 am, or by appointment, 119 Weber Building

Textbook: *Proofs, Arguments, and Zero-Knowledge* by Justin Thaler.

`https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.html`

Grades and Policies

Course grades will be calculated based on the following proportions:

- Homework (60%)
- Midterm Exam (20%)
- Final Presentation (20%)

Homework: Assignments will be posted each Thursday and will be due on the following Thursday in class. Please either (a) write your homework on paper to hand it in, (b) type it in LaTeX and print it, or (c) type it in LaTeX and email me a PDF. Assignments submitted by email should have a timestamp of no later than 8:09 am.

Late homework submissions will be accepted, but the following penalties will apply.

- 8:10 am Thursday until 8:09 am Monday: 80% credit
- 8:10 am Monday until 8:09 am Thursday: 60% credit
- More than one week late: 40% credit

The lowest homework score will be dropped from your overall homework average at the end of the semester.

Collaboration is permitted, but you must list all coauthors on a problem's solution at the top of the page. In addition, your writing must be your own; copying is not permitted and clearly-copied solutions (either from a fellow student or from an online resource) will result in an automatic zero on the assignment.

Exams: The course will include one midterm exam covering around the first half of the course material, and no final exam. In lieu of a final exam, students will give presentations during finals week on a supplementary topic related to the course material.

Presentation: Students will work individually or with a partner to prepare a presentation and a short write-up on a topic related to the course material. Topics will be selected

later in the semester, and presentations will take place during the course's scheduled final examination block.

Covid policies: As per university policies, masks are not required during lectures, but are recommended. If testing positive for Covid, students should refrain from attending class or office hours in person until symptoms have resolved and they have received a negative test result. Rapid antigen tests are available for free on campus:

`https://covid.colostate.edu/register-schedule-screening/`

If dealing with a Covid infection, please get in contact by email to make alternative arrangements for keeping up with lecture materials. Course deadlines may be extended by up to 14 days without late penalties in this case.

Attendance: Attendance in class is important. The class will not follow the textbook closely, but rather, the textbook will be used as a guide and as a reference for important definitions and concepts.

Overview and Topics

The goal of this class is to introduce the theory of succinct non-interactive arguments of knowledge (SNARKs), including necessary background in abstract algebra, cryptography, and verifiable computation. A tentative schedule of topics is listed below.

Week	Dates	Topic
1	Aug 23, 25	Blockchains and verifiable computation
2	Aug 30, Sep 1	Polynomial rings and finite fields
3	Sep 6, 8	Elliptic curves, group law, basic properties
4	Sep 13, 15	Discrete log cryptography
5	Sep 20, 22	Elliptic curve pairings
6	Sep 27, 29	Interactive proof protocols
7	Oct 4, 6	Sum check protocol, GKR protocol
8	Oct 11, 13	Vector and polynomial commitment schemes
9	Oct 18, 20	Arithmetic circuits, R1CS, encoding schemes
10	Oct 25, 27	Fiat-Shamir transformation
11	Nov 1, 3	Knowledge-soundness, zero-knowledge
12	Nov 8, 10	Sigma-protocols
13	Nov 15, 17	Inner product arguments, argument composition
14	Nov 29, Dec 1	Reed-Solomon proximity arguments, FRI
15	Dec 6, 8	Marlin proof system