Teaching Statement

Yibin Yang

One of my primary reasons for seeking a career in academia is my passion for teaching. This passion and appreciation have been cultivated through my experiences and opportunities: learning from teachers and colleagues who shaped my mind and outlook, as well as TAing courses and mentoring more junior PhD students. It truly gives a sense of joy and accomplishment to see a student develop their understanding and own research in part due to my contribution as a teacher and mentor.

Teaching Experience. In addition to delivering research talks to various audiences, at Georgia Tech, I TA'd *Intro to Graduate Algorithms* once and *Blockchain & Cryptocurrencies* three times.

The online *Graduate Algorithms course* with 450 students provided a unique large-course experience. Among many things, I learned how to manage logistics and design course materials tailored to a large and diverse group of students at significantly varying levels of expertise.

The *Blockchain course*, offered by my advisor, was a newly designed and relatively smaller (80-100 students) course. I had the opportunity to significantly contribute to course development, particularly by designing class materials, homework assignments, exams, and coding projects. Among these, I am especially proud of the success of the *Buzzcoin* project I co-invented.

We operated an Ethereum-based class cryptocurrency called Buzzcoin; students were to earn Buzzcoin by interacting with smart contracts. Our innovation was to foster student social interactions, mimicking the real-life blockchain ecosystems. Many of our contracts required collaboration among multiple students to achieve payouts, with various incentives to encourage participation. In-person and online, students formed alliances, built trust, and engaged in — permitted and encouraged by us — misrepresentation, social engineering, and technical attacks.

One such attack is quite memorable: a student sold (of course only Buzz could be used for payments!) problem solutions with an embedded Trojan that stole victims' secret keys and, hence, coins. The student was a skillful social engineer. He[1] first offered to submit solutions on others' behalf and asked for their secret keys. As expected, victims did not trust strangers with their keys, but they did fall for the subsequent offer where the student sold the Python code to be run by the victims themselves. The student's code simply posted the victims' keys on the Buzzcoin blockchain so that he could read them.

The Buzzcoin project consistently received very positive feedback, such as:

> *"This was one of the most fun assignments I've ever had, in this gamified process I learnt a lot more than I had expected. ... Tldr; Buzzcoin Carnival was a complete success!"*

TAing for the Blockchain course also allowed me to engage extensively with students from diverse backgrounds through weekly office hours and online interactions. The course, open to undergraduate and graduate students, attracts a wide range of participants, including many non-CS majors, drawn by the popularity of cryptocurrency. However, the rigorous cryptographic definitions presented in the course pose challenges for many students. To accommodate their varied backgrounds, I tailored my explanations to enhance each student's understanding. For example, when explaining the concept of IND-CPA security, I used intuitive probabilistic arguments for students with mathematical backgrounds, concrete examples of attacks for those with security/engineering backgrounds, and real-world examples of (in)correct application usage for students with financial backgrounds. Additionally, I offered personalized appointment-based one-on-one sessions to help students see the broader picture and history of each primitive. I received highly positive student feedback in the course survey. Students described me as

> *"effective, considerate, open-minded, accessible, helpful, knowledgeable, ..."*

I am looking forward to bringing similar innovation and passion to the courses I teach as a Professor.

[1] He revealed his identity in a post-mortem.

Mentoring Experience and Outreach. Beyond the classroom, I have been actively involved in mentoring junior students on research projects, including one undergraduate, one Master's student, and three junior PhD students. Currently, I am collaborating with one of the PhD students on utilizing Fully Homomorphic Encryption to optimize arithmetic garbling, another on creating more efficient ZKP toolchains based on my recent work, and a third on investigating undefined behavior in ZKP implementations. I expect publications in each of these thrusts.

As a mentor and collaborator, I helped shape the research agenda, delivered lectures on related work, led meetings, and, most importantly, provided both research-oriented and logistical advice. My goal is to assist students in discovering their research interests and to help them embark on their research journeys smoothly, effectively, and with confidence.

I take advantage of outreach opportunities. For example, I serve as the Manager of the Georgia Tech Center for Math Kangaroo, an international math competition for K-12 students. It is extremely rewarding to have an opportunity to guide bright young minds and foster their interests in STEM.

Teaching Interests. As a cryptographer focusing on *Zero-Knowledge Proofs* (ZKP) and *Secure Multi-Party Computation* (MPC), I am enthusiastic about teaching any crypto-related course, particularly advanced ZKP and MPC, at both undergraduate and graduate levels. As an applied cryptographer, I would like to offer a mix of theory and practice in the following courses, making it more appealing to broader audiences, especially undergraduates:

- **Implementable Cryptography:** Motivated by my internship experiences and cryptography's increasing adoption in industry — and the growing demand for crypto-competent engineers, I would like to offer a course covering both theoretical foundations and implementations of cryptographic schemes, focusing on those used in the real world.
- **Blockchain:** I plan to bring the Blockchain course from Georgia Tech. In this course, I will cover both fundamental and advanced cryptographic tools used in cryptocurrency. Crucially, I am excited to initiate and further develop the "Mascotcoin" project.

More broadly, as a researcher at the intersection of theory and systems, I can teach a range of courses, from theoretical, such as *Algorithms* and *Complexity*, to systems, such as *Network Security*, *Systems Security*, and *Computer Organization and Programming*, especially at the undergraduate level.

Teaching and Mentoring Philosophy. My teaching and mentoring philosophy follows Einstein's approach of "attempt[ing] to provide conditions in which [students] can learn." To me, this means fostering learners' interest in the topic and encouraging self-directed exploration. As a PhD student, I benefited from this philosophy myself — it led to my deeper understanding and greater satisfaction in my work. I strive to create an environment where students engage meaningfully with the material and develop their own understanding. I would like to highlight three important aspects of my vision:

- **Personalization:** Each student enters a course with unique objectives, and every junior researcher begins their journey with different research interests and career goals. It is crucial for me to understand the needs of each student, whether in the classroom or research lab, and provide them with personalized learning as much as possible. I plan to achieve this by conducting frequent office hours, small-group and one-on-one meetings, and adjusting instruction and materials.
- **Autonomy:** Letting students (at least partially) lead their studies and research exploration is a broad direction. I would like to highlight one particular scenario — "learning by typing." Implementing cryptography offered me numerous benefits, such as better understanding of the problem at hand, including its importance and relevance, and discovering unexpected bottlenecks, which often motivate new research problems and others. Recognizing that implementation is often missing in cryptography courses, I would like to include it in my teaching and mentoring.
- **Encouragement:** Studying cryptography involves a long and steep learning curve. As a lecturer and mentor, I will identify and celebrate the successes of my students, even seemingly small or incremental. In my experience, even small recognition can go a long way in maintaining determination and have an outsize effect on students' progress.

Of course, applying this (or any) teaching and mentoring philosophy should adjust depending on the context. For example, for undergraduates, I aim to develop objective yet engaging and intuitive courses and research contents, such as using short stories to illustrate cryptographic definitions. For graduate students, I intend to provide greater flexibility in exploring potential topics, such as research course projects focusing on a broad direction without rigid constraints.