Teaching Statement

Sarah Scheffler

Throughout my time as a student, I had the pleasure of taking classes that I looked forward to every day, where I truly got to engage with the material in a way that helped me master it and left me with a deep enjoyment of the subject. I also attended classes that were confusing and boring, barely stayed afloat on the fumes of tired graduate students, and left me feeling like I would have been better off reading a free textbook on the subject rather than attending class.

As a teaching assistant and in outreach programs, I had my first tastes of the tremendous amount of high-level planning and low-level building that is required to make a class a truly great and equitable experience for all students. I hope to teach at an institution that values teaching alongside research.

Teaching philosophy

In teaching any course, my goal is to enable an equitable learning experience for students regardless of prior opportunity. My approach to achieving this goal incorporates three practical steps: First, intertwine the teaching of core concepts with examples from a wide variety of domains and applications; many students who struggle to understand a concept in a vacuum will find an easier time understanding it by example. Second, structure the class such that formative assessments can confirm that all students have an understanding of the core concepts, including by calling on all students, quick feedback on assignments, and low-stakes quizzes to measure student progress. Third, offer assignments that allow students to interact with the topic from a wide variety of perspectives, focusing on learning by doing.

These principles hold for teaching a class on any topic, but as an example, in teaching a class on cryptography I would incorporate not only traditional assignments, but also projects incorporating encryption policy challenges on topics like disinformation, labor activism, or free speech.

Teaching and Lecturing Experience

I have designed multiple courses from the ground up for high school outreach programs, from short six-session Introduction to Programming sessions to a much more intensive three week summer "day camp" on Cybersecurity. The key goal of these outreach programs was to foster interest, and I designed activities and interactive lessons with the key goal of engaging all students. I was pleased to see that building interest also resulted in greater learning—the students not only found the activities fun, they also covered more ground than would have been possible for a more "standard" introduction.

During graduate school, I also acted as a Teaching Fellow for two separate offerings of Applied Cryptography, a joint graduate/undergraduate class taught by Prof. Mayank Varia. My responsibilities included grading, running office hours, helping students on Piazza, giving assorted lectures, and behind-the-scenes work to make a smooth homework submission process.

Mentorship

Academic mentorship. Mentoring is what made me realize I wanted to pursue a career as a professor: I genuinely found the experience of working with junior students and helping them achieve their research goals to be one of the most rewarding experiences of my life.

My biggest opportunity for mentorship was for a project at the end of my Ph.D. program. I supervised three Boston University undergraduate students doing research in cryptography for 1.5 years, culminating in a conference publication at Applied Cryptography and Network Security 2021. Two of those students have since entered Ph.D. programs in cryptography; one of them informed me that her interest was a direct result of my mentorship. During this research project, I ensured that my mentees had appropriately scoped main and stretch problems with reasonable deadlines that would build their skills for the next phase of research.

I held weekly meetings with them and also ensured that I was approachable and available for issues that popped up between meetings.

I am also mentoring a current undergraduate student at Princeton who is acting as my research assistant for an ongoing policy-heavy project. At the beginning of the project, we met frequently to develop the formal goals, scope, and methods for our analysis; now that those are set, we conduct periodic check-ins to see how her work is going and make adjustments when needed.

In addition to formal academic mentorship, I also acted as an unofficial academic mentor for at least four junior Ph.D. students in my graduate program. I walked these students through the process of reading cryptography papers, taught them how to review papers, and helped them build their first research plans. I am especially thrilled to have been specifically sought after as a role model for female students in the group.

Personal mentorship. I have found purpose in mentorship ever since my undergraduate experience as an officer in PRISM (People Respecting Individuals' Sexualities at Mudd), where I led a number of small group discussions around LGBTQ+ issues. Around the same time I also participated in a program called Building Bridges, in which I developed my skills for conversing about difficult topics with students of many racial, sexual, and cultural identities. These approaches for leading and participating in constructive dialogue have remained relevant throughout my career. During the pandemic I was contacted by younger students in my graduate program who were struggling to adapt to graduate school life; I listened to each of them and helped them with strategies to address their various problems, from financial to motivational to interpersonal. I am proud of my reputation as someone who is approachable and who can help problem-solve both academic and non-academic challenges.

K12 Outreach for Diversity, Equity, and Inclusion

I have maintained a consistent interest in improving equity and inclusion in computer science and cryptography. With the goal of equity in mind, I helped build and run Code Creative, a computer science course we specifically built for Boston-area high school students who do not have access to a computer science course in their schools. And with the goal of increasing inclusion and diversity, I also built and ran the first iteration of Codebreakers, a three-week cybersecurity class for high school women that has continued with minor variations to this day. I also volunteered as a teaching assistant for RACECAR Crash Course which prepared high school students for the Beaver Works Summer Institute (BWSI) RACECAR course run at MIT. The first offering of the Crash Course was for students primarily of races underrepresented in STEM; the second offering was for Boston-area women.

Event Organization

In my interdisciplinary research area, I have found workshops and similar events to be a useful way to unite people across different research areas, and bring together different perspectives that inform the policy and technical design of cryptographic systems. To contribute to this cause, this year I am co-hosting a three-part event called "Privacy Enhancing Technologies for the Public Interest." The overall workshop series aims to bring together a wide net of stakeholders, researchers, and activists to set a future research agenda on privacy research. The first workshop, set to occur in October 2022, is specifically aimed at junior researchers to share interdisciplinary research methods and foster collaborations.

Teaching at Princeton

I am enthusiastic and qualified to teach Princeton's standard and advanced cryptography courses (COS433 and COS533), as well as information security (COS432), networks (COS461), theory of computation (COS487), computational complexity (COS522), or fairness in machine learning (COS534). The Princeton Computer Science department would also benefit from my introduction of an applied cryptography class that could go deeper than a standard cryptography class into the design of symmetric ciphers and hash functions, discuss attacks and side channels, and teach the implementation of secure cryptography code.

Furthermore, I would enjoy teaching a topics course on privacy-preserving computing. The course would focus on various practical methods for performing private computation, especially multi-party computation, differential privacy, and homomorphic encryption.