Research Statement

Annamira O'Toole **Ph.D. Applicant**

Cryptography is a crucial tool for protecting an individual's right to think and speak independently. My research focuses on authenticated private information retrieval schemes, a core tool for building private web browsing and communications when applied to problems like key transparency, key retrieval, and contact discovery. In the past, I have also worked in zero-knowledge theory and implementation.

Educational Background

I am currently concluding my MSc in computer science jointly between ETH Zürich and EPFL in Switzerland, thanks to funding from the **Master Excellence Fellowship program**.[1] In Zürich, I am working under Professor Kenneth Paterson as a **research assistant the Applied Cryptography Group**. In early 2025, I will complete my **MSc research thesis on anonymous credentials at IBM Research**[2] in Zürich where I will be collaborating with Dr. Kaoutar El Khiyaoui and Dr. Elli Androulaki. In 2023, I graduated from UC Berkeley with degrees in mathematics and computer science, where I also gained a broad exposure to policy through economics and law. My industry experience spans investment-focused engineering at a hedge fund,[3] analyzing interest rates on decentralized token exchanges,[4] and building randomized PCA for genomics datasets.[5] I have previously **contributed to the cryptography package** arkworks.rs,[6] while exploring polynomial commitment schemes for space-efficient SNARKs, essential for modern anonymous credential verification systems and verifiable distributed computation.

Personal Motivation

I view my research as inseparable from the world it is deployed in. I realized the impact of cryptography while learning about how the NSA hid a backdoor in NIST's standardization of the Dual_EC_DRBG elliptic curve pseudorandom number generator, leaked during the 2013 Snowden revelations. Curious, I watched the documentary *Citizenfour*, which shows Snowden's reliance on privacy tools like Tails OS[7] to safely inform the public. The need for privacy-preserving systems grows as data and digital assets increase in value. However, if deploying security features comes at too high a cost, they will not be implemented in the real world. Unfortunately, the resource-efficiency of cryptography comes with a direct trade-off against the privacy it provides. Furthermore, as most of today's communications systems are controlled and standardized by governments, writing effective and enforceable privacy regulation is critical.

Current Research

My current work on private information retrieval (PIR) approaches an almost-ideal research question: it solves useful problems, has a beautiful theory, and yet suffers from shortcomings in implementation, which my work aims to solve. In Zürich, I experienced the **full research life cycle** from ideation, to protocol design trial-and-error, to writing security proofs, and implementation. My work involved surveying PIR literature and identifying the shortcomings of existing schemes, while closely collaborating with post-doc Dr. Francesca Falzon and PhD candidate Laura Hetz. Our project's scheme builds the first **two-server authenticated PIR scheme** that will offer sublinear communication and computation, with a tradeoff on client storage. We plan to submit to a conference in early 2025. I now understand that applied cryptography systems often face drawbacks often cleverly-hidden by publications. For example, certain schemes only work efficiently for limited data formats, or require unusually large parameters to achieve the desired privacy guarantee—drawbacks only ascertainable by digging into the weeds of highly technical privacy proofs. However, it is exactly this investigative process that I learned to love, and that gives rise to open research questions with novel solutions.

PhD Vision

At the start of my PhD, I plan to focus on building applied systems for well-defined use-cases, leaning on my algorithm design and engineering skills while building maturity within cryptography. I dream of collaborating directly with privacy-preserving projects such as Signal (end-to-end encrypted messaging), Brave (private browsing), or Tor network (anonymous communications) to build protocols that are provably secure and well-designed for their immediate use-cases. Specifically, Professor Emma Dauterman's work on scaling oblivious object stores for large use-cases interests me as her techniques were deployed by Signal with ORAM for private contact discovery.[8] As I build maturity during my PhD while working on applied systems, I hope to shift my work towards pure cryptographic contributions, such as signature schemes and authentication primitives. These are also active research areas of Professor Dan Boneh, such as his recent work on efficiently updatable vector commitment opening proofs, which I was studying for potential use in

my authenticated PIR work.[9] Finally, I want to understand on a deep level how cryptographers capture the notion of privacy mathematically. I am interested in reconciling inconsistencies between different notions of privacy that must be combined to prove the security of highly complex systems.

I intend the arc of my PhD to take me through several subfields of cryptography from (1) building end-to-end applied systems for specific privacy use-cases (which I am already working on), to (2) improving upon widely-applicable cryptographic primitives, to (3) a theoretical contribution to cryptography.

Interest in Data Privacy Regulation

My interest in security research goes beyond answering technical questions. I am interested in exploring cases of government-compelled decryption, Section 230 corporate immunity, censorship of ill-defined disinformation, government immunity during classified surveillance operations, and the regulation of digital currencies as securities. These are also active areas of research the Center for Internet and Society at Stanford Law School, where Professor Barbara van Schewick's work has influenced net neutrality debates across the U.S.[10] Alongside my technical research, I hope to learn from and contribute to the center's work during my PhD.

Teaching & Values

In Zürich, I am a member of a vibrant international lab community—from climbing mountains together to leading an internal study group for learning Rust programming. I have had moments of intense intellectual joy while working on my current research, and have formed close working relationships and friendships with my research mentors. I enjoy the process of struggling to keep up with another smart person, only to later slow down and understand their thinking step-by-step, and then offer my thoughts and ideas in return. Cultivating an ethical research environment and healthy learning environment for junior students is extremely important to me. To do so, I have enthusiastically been involved in teaching during my bachelors for UC Berkeley's **undergraduate algorithms course CS 170**,[11] as well as with high school students in Jamaica by **teaching and organizing JamCoders**,[12] and its sister program AddisCoders.[13] My teaching at UC Berkeley awarded me an **outstanding undergraduate instructor award**,[14] and I am excited to continue teaching as a PhD student.

I believe in a future where large corporations as well as governments cannot easily use an individual's data to manipulate their behaviors. This future requires advancements in anti-censorship systems, encrypted and anonymous communication, post-quantum cryptography, updated privacy-preserving internet protocols, and a legal framework for protecting an individual's privacy that is built in collaboration with computer security experts. I hope to help build such a future during and after my PhD. Thank you for your consideration.

Footnotes & References

[1] Merit-based scholarship awarded by EPFL (L'École Polytechnique Fédérale de Lausanne) covering tutition and living expenses.

[2] Project will be a part of IBM's decentralized trust research, with the goal of designing an anonymous credential revocation system. An anonymous credential is a signature or a MAC over some credential data. Instead of just revealing the credential, the user proves (in zero-knowledge) that the credential satisfies certain properties.

[3] Investment Logic Engineering internship at Bridgewater Associates.

[4] Semester-long engineering internship at Gauntlet Network, an R&D firm in the blockchain space.

[5] A contribution to the Python library called Hail, maintained by a team at the Broad Institute of MIT and Harvard

[6] A contribution to a system for elastic proofs within the Rust arkworks.rs package.

[7] A privacy-preserving operating system that is a part of the global non-profit Tor Project.

[8] Emma Dauterman, Vivian Fang, Ioannis Demertzis, Natacha Crooks, and Raluca Ada Popa. Snoopy: Surpassing the scalability bottleneck of oblivious storage. In *SOSP*, pages 655–671, 2021.

[9] Ertem Nusret Tas and Dan Boneh. Vector Commitments with Efficient Updates. In *5th Conference on Advances in Financial Technologies*, 2023

[10] The Center for Internet and Society, directed by Stanford Professor Barbara van Schewick.

[11] CS 170 Efficient Algorithms and Intractable Problems

[12] JamCoders is a summer program in Kingston, Jamaica that teaches intro computer science to 50 high school students each summer.

[13] JamCoders' sister program in Addis Ababa, Ethiopia.

[14] Annual awards to graduate and undergraduate teaching assistants nominated by UC Berkeley faculty and students.