Caleb Geren

c.geren@utah.edu • 480-289-1661

Research interests

Zero-knowledge proof systems, cryptography

Education

2025 – Present **University of Utah** – Salt lake City, UT
Ph.D. in Computer Science

Member of the Security & Privacy research cluster researching privacy preserving proof systems such as zero knowledge proofs and SNARKs. Currently, I am exploring how to make these systems both more time and space efficient, especially where they are plausibly post-quantum.

2021 – 2025 **Lehigh University** – Bethlehem, PA
B.S. in Computer Science
B.A. in Mathematics

Publications

2024 **Blockchain for Large Language Model Security and Safety: A Holistic Survey**
Caleb Geren, Amanda Board, Gaby G. Dagher, Tim Andersen, Jun Zhuang
ACM SIGKDD Explorations Newsletter, Volume 26, Issue 2

2023 **Scaling Zero-knowledge to Verifiable Databases**
Tal Derei, Benjamin Aulenbach, Victor Carolino, **Caleb Geren**, Michael Kaufman, Jonathan Klein, Rishad Islam Shanto, Henry F. Korth.
Proceedings of the 1st Workshop on Verifiable Database Systems

Honors and scholarships

2025 Honorable Mention - Graduate Research Fellowship Program (GRFP; GRFP site)
Honorable mention in the extremely competitive 2024-2025 GRFP cycle where my project proposol focused on novel approaches to accelerating zk-SNARKs on modern architectures.

2024 Boise State University Blockchain REU (BREU; BREU site)
REU fellowship which provided me with the opportunity to develop blockchain research concerning large language model applications.

2023 DAAD Rise Scholarship Recipient (DAAD; RISE site)
International scholarship which pairs undergraduate students from North America, Great Britain, and Ireland with faculty at German universities for summer research.

Research experience

Aug 2025 – Present
Kahlert School of Computing *Building Time and Space Efficient zk-SNARKs*
Advisor: Pratik Soni

- zk-SNARKs are typically inefficient in either the Prover's space complexity, time complexity, or in the Verifier's communication complexity.
- Developing time and space efficient arguments in zero-knowledge which minimize expensive operations and allow for efficient verification.

Dec 2022 – May 2025
Lehigh University Blockchain Lab *Accelerating zk-SNARKs on GPUs*
Mentor: Henry F. Korth

- An attempt to parallelize the zk-SNARK proving system Plonk in order to scale zero-knowledge systems generally.
- Preliminary results from existing Plonk implementations gave way to promising avenues towards an implementation of the Plonk prover which exploits a multi-streaming technique on GPUs. After exploration, the multi-streaming technique proved infeasible in light of certain computational bottlenecks in the underlying Plonk computation.

May 2024 - July 2024
Boise State University Blockchain REU *Blockchain for LLMs: A Survey*
Mentor: Gaby Dagher

- A thorough exploration into the complementary nature of blockchain in the realm of large language model safety and security was conducted.
- Resulted in a first author KDD '24 publication, with much of the drafting, outline, and research questions developed independently.

Teaching experience

Fall 2023
Fall 2024
Teaching assistant, CSE 242: Blockchain Systems (Lehigh University)
Delivered a lecture on the details of the Plonk proving system (see Talks and Posters), as well as held office hours and graded assignments on a weekly basis.

Spring 2024
Teaching assistant, CSE 340: Algorithms (Lehigh University)
Held twice weekly office hours reviewing homework assignments, course content, and grading assignments.

Talks and Posters

August 2024
Poster: Integrating Blockchain with LLMs: Towards a Secure and Safe Technology
Poster given at the Idaho Conference for Undergraduate Research (ICUR).

November 2023 **Lecture: An In-Depth Look at the Plonk Zero-knowledge Proving System: Plonk By Hand**
Lecture delivered in the Blockchain Systems course CSE 242 covering the details of the zk-SNARK construction Plonk.

August 2023 **Poster: Blockchain Systems and Applications Research**
Presentation given at Lehigh Summer Research Internship.

April 2023 **Poster: Scaling Zero-Knowledge Proof Generation for Large Blockchain Applications**
Presented to Lehigh University's internal I-DISC conference.

Other interests

Besides my passion for cryptography, I also love to rock climb, snowboard, canyoneer, and ice climb!