Jacob D. White

white570@purdue.edu || cs.purdue.edu/homes/white570 || jdwhite48 || 0000-0002-6850-2133

Education

Purdue University — *West Lafayette, IN*

Ph.D., Computer Science — May 2022 — (Exp) May 2026

- Advisor: Christina L. Garman
- GPA: 3.77 / 4.00

M.S., Computer Science — Aug 2020 — May 2022

B.S., Computer Science; B.S., Mathematics; Minor, Psychology — Aug 2017 — May 2021

- Concentrations: Security, Systems Engineering

Relevant Coursework

Cryptography, Information Security, Socioeconomic Aspects of Security, Computation & Complexity Theory, Compilers, Formal Reasoning about Programs, Network Security, Operating Systems, Human Factors in Engineering

Research Experience

Graduate Research Assistant — May 2021 — Present

Purdue University — *West Lafayette, IN*

- Primary Advisor: Christina L. Garman
- Designing and implementing efficient cryptographic systems which simultaneously preserve user privacy and accountability, especially using identity-based schemes such as anonymous credentials.
- Contributing to open-source projects in order to improve the usability of various cryptographic tools, especially zero-knowledge proof-based systems such as Groth-Sahai, Arkworks zkSNARKs, and anonymous credentials
- Writing and publishing academic papers to top cybersecurity and cryptography conferences (e.g. IEEE S&P)

Professional Experience

Software Development Intern — Summer 2019

LifeOmic — *Indianapolis, IN*

- Updated an auxiliary web service used by medical professionals to access DICOM medical imaging data, modernizing the UI/UX design and deployment processes and ensuring secure authenticated access

Student Supervisor — Oct 2019 — May 2020

Earhart Dining Court — *West Lafayette, IN*

- Trained and managed employees to perform various tasks, ensuring the satisfaction of 2000+ customers daily

Publications

Technical Reports

[1] Michael Rosenberg, Jacob White, Christina Garman, and Ian Miers. ***zk-creds:*** *Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure*. Cryptology ePrint Archive, Paper 2022/878. July 2022. https://eprint.iacr.org/2022/878. **Accepted to IEEE S&P 2023**.

Posters

[1] Siddharth Muralee, Muhammad Ibrahim, Jacob White, Bo-Shiun Yen, Ashwin Nambiar, and Alan Ma. *Protected Automotive Remote Entry Device (PARED) Protocol*. In: MITRE Embedded Security Capture The Flag Poster Session. Purdue University, Apr. 2023. **BEST POSTER AWARD**.

Software

Groth-Sahai Proof Library June 2021 — Present

- Developing a cryptographic library in Rust which allows users to create efficient proofs about the satisfiability of pairing product equations and other algebraic equations, while keeping details about user variables secret
- Implementing existing zero-knowledge proof techniques which use bilinear pairings, elliptic curves, and matrices

zk-creds June 2021 — Jan 2023

- Designed the high-level API for a cryptographic library allowing users to construct efficient anonymous credential systems using zkSNARKs, and researched various approaches. Corresponding paper was accepted to IEEE S&P.

University Service

Purdue Graduate Student Government (PGSG) Senator Aug 2022 — Present

- Representing computer science graduate students by listening to concerns and enacting legislation on their behalf
- Engaging in discussions with Purdue and the Greater Lafayette community to improve quality of life for students

`b01lers` **Officer** Aug 2022 — Present

- Creating challenges to teach and encourage others to develop valuable skills in computer security and cryptography
- Organizing Capture The Flag (CTF) competitions, presentations, and workshops for 100+ participants each year
- Led the design and documentation of cryptographic protocols to secure an embedded system (and audited its implementation) in a semester-long CTF competition hosted by MITRE

Membership

ACM Student Member, *SIGSAC* Apr 2021 — Present

Awards and Honors

Best Poster, *MITRE Engenuity* Apr 26, 2023

- Awarded to the team with the best poster in the 2023 MITRE Embedded Security Capture The Flag competition

Dean's List, *Purdue University College of Science* 2017 — 2021

- Awarded each semester for attaining at least a 3.5 cumulative GPA and a 3.0 semester GPA

Technical Skills

Programming Languages: Rust, C/C++, Python, Coq, JavaScript, Java
Tools and Frameworks: LaTeX, Git, Wireshark, NumPy, Pandas, Arkworks, Scapy, Qt, React