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

- 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 *(* indicates graduate-level)*

Cryptography*, **Socioeconomic Aspects of Security***, Information Security*, Computation & Complexity Theory*, **Formal Methods***, **Abstract Algebra***, **Network Security***, Human Factors*, Compilers, Operating Systems

Research Experience

Graduate Research Assistant — May 2023 — Present

Los Alamos National Laboratory — *Los Alamos, NM*

- Primary Advisor: Michael Dixon

Graduate Research Assistant — May 2021 — Present

Purdue University — *West Lafayette, IN*

- Primary Advisor: Christina L. Garman
- **Designing and implementing efficient cryptography** which simultaneously preserves **user privacy and accountability**, with a focus on identity-based schemes such as anonymous credentials.
- **Contributing to open-source projects** 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

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

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

University Service and Activities

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

- **Representing** computer science graduate students by listening to concerns and enacting legislation on their behalf
- **Advocating** for graduate students by discussing quality of life with Purdue and the Greater Lafayette community
- **Lead community outreach** efforts, **advocating** for the safety and belonging of LGBTQ+ students and faculty

`b01lers` Officer — Aug 2022 — Present

- **Teaching computer security and cryptography** skills by creating engaging challenges and presentations
- **Organizing competitions and workshops** for 100+ Capture The Flag (CTF) participants each year
- **Designed and documented cryptographic protocols** to secure an embedded system and **audited** its implementation in a semester-long CTF competition hosted by MITRE, placing 6th out of 60

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 zero-knowledge proof** techniques using matrices, **bilinear pairings and elliptic curves**

zk-creds June 2021 — Jan 2023

- Designed an API and evaluated approaches for a cryptographic library allowing users to efficiently construct **anonymous credential systems** using **zkSNARKs**. Corresponding paper was accepted to IEEE S&P 2023

Publications

Conferences

[1] Michael Rosenberg, Jacob White, Christina Garman, and Ian Miers. "`zk-creds`: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure". In: *2023 IEEE Symposium on Security and Privacy (SP)*. May 2023, pp. 790–808. DOI: 10.1109/SP46215.2023.00108. [17% Accepted].

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**.

Awards and Honors

Best Poster, *MITRE Engenuity* Apr 26, 2023

- Awarded best poster in the 2023 MITRE Embedded Systems Security CTF 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

Membership

ACM Student Member, *SIGSAC* Apr 2021 — Present

Technical Skills

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