Jacob D. White

Email: white570@purdue.edu
Website: cs.purdue.edu/homes/white570
GitHub || LinkedIn: jdwhite48
ORCID: 0000-0002-6850-2133

Education

Ph.D., Computer Science, *Purdue University* Apr 2022 — (Exp.) May 2026
- GPA: 3.77 / 4.00

M.S., Computer Science, *Purdue University* Aug 2021 — May 2022

B.S., Computer Science, Mathematics, *Purdue University* Aug 2017 — May 2021
- Minor in Psychology with Concentrations in Security, Systems Engineering

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

Research and Development Experience

Graduate Research Assistant, *Purdue University* May 2021 — Present
- Primary Advisor: Dr. Christina Garman
- **Designing and implementing efficient cryptography** which simultaneously **preserves user privacy and attribution** for distributed, identity-based **Internet infrastructure and applications**.
- **Contributing to open-source cryptographic libraries** to improve usability, especially for zero-knowledge (zkSNARK) circuits, gadgets, and constraints.
- **Writing and publishing** academic papers to top cybersecurity and cryptography conferences (e.g., IEEE S&P).

Graduate Research Intern, *Los Alamos National Laboratory* May 2023 — Aug 2023
- Primary Mentor: Michael Dixon
- **Implemented a library for securing and validating network routing**, leveraging secure multi-party setup for zero-knowledge proof systems to eliminate the need for centralized management of and trust in pre-shared secrets.
- **Improved state-of-the-art in Internet routing security** with novel privacy guarantees which protect sensitive network and business relationships. Crucially, compared to other public key-based approaches, our implementation offers better authentication while remaining competitive in terms of bandwidth.
- **Presented research results** to scientists and non-technical audiences alike, conveying the key technical and strategic insights to dozens of other students, researchers, and group leaders within the division.

Software Development Intern, *LifeOmic* May 2019 — Aug 2019
- **Updated and deployed** an auxiliary web service used by 100+ medical professionals to access DICOM medical imaging data, modernizing the UI/UX design and deployment processes and ensuring secure authenticated access.

Leadership and Service

Purdue University Indianapolis Transition Coordinator, *Purdue University* Sep 2023 — Present
- **Facilitating** the needs of the Purdue Computer Science (CS) department to extend **quality instruction** to Purdue University Indianapolis (PUI) campus for Fall 2024 and beyond.
- **Leading regular meetings** with CS department heads and Purdue administration to communicate the needs of graduate teaching assistants and other student instructors as IUPUI transitions into PUI campus.

Cryptography Reading Group Organizer, *Purdue University* Sep 2023 — Present

Graduate Teaching Assistant, *Purdue University* Aug 2023 — Present
- **Guiding and assisting** students by holding weekly office hours, grading projects and exams, and asynchronously answering dozens of technical questions for **over 90 students**.
- **Courses**: CS 526 **Information Security** (Fall 2023)

Purdue Graduate Student Government (PGSG) Senator, *Purdue University* Aug 2022 — Present
- **Representing** computer science graduate students by listening to concerns and enacting legislation on their behalf.

- **Advocating for students** by discussing quality of life with Purdue leaders and the Greater Lafayette community.
- **Leading community outreach** efforts, advocating for the safety and belonging of underrepresented minorities.

`b01lers` Officer Aug 2022 — Present

- **Teaching computer security and cryptography** skills to new and returning members alike **by presenting on introductory workshops** and write-ups, and by creating engaging hands-on challenges for others to compete in.
- **Organizing competitions** for 100+ Capture The Flag (CTF) participants globally each year.
- **Led the design team** to secure an embedded system in a semester-long CTF competition, placing 6^{th} out of 60.

Student Supervisor, *Earhart Dining Court* Oct 2019 — May 2020

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

Selected Projects

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 for cryptographic signature and proof verification, while keeping details about user variables secret.
- Implementing a witness-indistinguishable and zero-knowledge proof systems **using linear algebra techniques over 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 applications using anonymous credentials and zkSNARKs. Corresponding paper was accepted to IEEE S&P 2023.

IoT Network Isolation May 2020 — Aug 2020

- Configured an Internet of Things (IoT) network and used network tools to monitor, analyze, and isolate IoT devices.

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 (S&P)*. May 2023, pp. 790–808. DOI: 10.1109/SP46215.2023.10179430. Preprint: https://eprint.iacr.org/2022/878. [17% Accepted].

Presentations

[1] Jacob White and Michael Rosenberg. `zk-creds`: *Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure*. Urbana, IL, USA, Sept. 2023. Invited talk for security seminar at UIUC.

[2] Jacob White and Michael Dixon. *Authenticating Internet Routing Using Zero-Knowledge Proofs*. Los Alamos National Laboratory. Aug. 2023. Approved for unlimited public release under LA-UR-23-29806.

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*. MITRE, Apr. 2023. **BEST POSTER AWARD**.

Certificates

Intercultural Diversity and Inclusion, *Purdue CILMAR* Oct 2023

Responsible Conduct of Research (RCR) – Graduate Students, *CITI Program* Jul 2021

Awards and Honors

Best Poster Award, *MITRE Engenuity* Apr 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, Java, JavaScript
Tools and Frameworks: Git, LaTeX, Arkworks, Wireshark, Scapy, NumPy, Pandas, Qt, Z3, EasyCrypt