Jacob D. White

✉ jdwhite.pub@gmail.com ⌂ cs.purdue.edu/homes/white570
GitHub || LinkedIn: jdwhite48 ORCID: 0000-0002-6850-2133

Education

Purdue University — West Lafayette, IN

Ph.D., Computer Science — Apr 2022 – (Exp.) May 2027

- Advisor: Christina Garman
- GPA: 3.66 / 4.00

M.S., Computer Science — Aug 2021 – May 2022

B.S., Computer Science, Mathematics — Aug 2017 – May 2021

- Minor in Psychology and Concentrations in Security and Systems Engineering

Relevant Coursework

Cryptography, Network Security, Legal & Ethical Aspects of Security, Human Factors, Security Analytics, Formal Reasoning, Abstract Algebra, Computation & Complexity Theory, Networks, Compilers, Operating Systems

Research and Development Experience

Purdue University — West Lafayette, IN

Graduate Research Assistant — May 2021 – Present

- Advisor: Christina Garman
- **Designing and implementing efficient cryptography** which simultaneously **preserves user privacy and attribution for Internet and blockchain-based applications** requiring identity verification.
- **Writing and publishing** academic papers to top security and and privacy conferences (e.g. IEEE S&P).

Los Alamos National Laboratory — Los Alamos, NM

Graduate Research Intern — May 2023 – Aug 2023

- Mentor: Michael Dixon
- **Implemented a library for securing OSPF and BGP network routing**, using zero knowledge proofs to eliminate the need for centralized authentication and to protect the privacy of network and business relationships.
- **Presented preliminary research results** to scientists and non-technical audiences alike, conveying key technical and strategic insights to dozens of students, researchers, and group leaders within the division.

LifeOmic — Indianapolis, IN

Software Development Intern — May 2019 – Aug 2019

- Updated and deployed a React web service used by 100+ medical professionals to access DICOM medical imaging data, updating the UI/UX design and deployment mechanisms and ensuring secure authenticated access.

Selected Projects

Groth-Sahai Proof Library | *Rust, Coq, Arkworks, SymPy* — June 2021 – Present

- **Developing an open-source library** which allows users to automatically create efficient proofs of satisfiable cryptographic signature and proof verification equations, while also keeping prover-defined variables secret.
- **Designing an equation rewriting engine to automatically synthesize zero-knowledge proofs** of equation satisfiability by re-arranging pairing product and other algebraic equations into an equivalent normal form.

zk-creds | *Rust, Solidity, Arkworks, Circom* — June 2021 – Jan 2023

- **Designed a modular paradigm for anonymous credentials** schemes, using zkSNARKs for privacy-preserving identity attestation over distributed systems such as blockchains. Associated paper 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.

Presentations

[1] Jacob White. *Linear PCPs and Groth16 SNARKs*. Oct. 2024. [Lecture].

[2] Jacob White and Michael Rosenberg. `zk-creds`: *Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure*. UIUC. Sept. 2023. **[Invited Talk]**.

[3] 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] Jacob White, Jimmy Hwang, Jack Roscoe, Jaxson Pahukula, and Vinh Pham. *"Medical Infrastructure Supply Chain (MISC) Protocol"*. In: *MITRE Embedded Capture The Flag (eCTF) Poster Session*. MITRE, Apr. 2024.

[2] Jacob White. *"`zk-creds`: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure"*. In: *2024 CERIAS Symposium Poster Session*. Purdue University, Apr. 2024.

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

Leadership and Service Experience

`b01lers` Capture the Flag (CTF) Team

General Officer — Aug 2022 – Present

- **Teaching introductory workshops** and presenting technical write-ups about cryptography to 50+ students.
- **Organizing competitions** and creating hands-on security challenges for 1000+ CTF competitors each year.
- **Leading teams to design cryptographic protocols for** and **execute side-channel attacks against embedded systems** in MITRE eCTF since 2023, presenting award-winning posters and placing 2$^{\text{nd}}$/120 in 2025.

Purdue Computer Science Graduate Student Association

Vice President — May 2024– Present

- **Leading a team of 20 people** to advocate and address the concerns of 600+ students each year by strengthening financial and social support and by co-organizing various social, grant, and professional programs.
- **Drafting departmental policies and procedures** in collaboration with CS administration to support travel grants for graduate students and to improve quality of instruction.
- **Led an organizing committee** to plan for and host the inaugural Purdue CS Graduate Symposium, procuring **$6000** in grant funding to allow 200+ students to showcase their research and explore collaboration opportunities.
- **Led meetings with Purdue department heads, upper administration**, and students to strategize plans for and communicate the needs of CS graduate TAs and instructors planning to teach at Purdue in Indianapolis.

Purdue Graduate Student Government Senator — Aug 2022 – May 2024

- **Reviewed and enacted legislation** to advocate for graduate student needs to Purdue and Indiana leaders.
- **Led community outreach efforts** to support safety and engagement of all graduate students on campus.

Purdue University — West Lafayette, IN

Graduate Teaching Assistant — Aug 2023 – May 2024

- **Guided and taught students** through weekly office hours, feedback and grading for projects and exams, and answered dozens of technical questions for 80-100 students per semester.
- **Courses**: CS 526 / CS 426 **Information Security** (Fall 2023, Spring 2024)

Awards and Honors

May 2024	**Ross-Lynn Research Scholar Grant**, *Purdue Office of Research* — $34,000
Apr 2024	**Best Poster Award**, *MITRE eCTF Competition*
Apr 2024	**Above & Beyond Award**, *Purdue Graduate Student Government*
Feb 2024	**Student Travel Grant**, *Real World Crypto Symposium*
Apr 2023	**Best Poster Award**, *MITRE eCTF Competition*

Technical Skills

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