Yongming Fan

fan322@purdue.edu http://www.yongming.fan +1 (812) 327-8479

Research Interest

My research interests lie at the intersection of applied cryptography, zero knowledge proof, protocol security evaluation, privacy, and software security. Specifically, I am intrigued by the potential of zk-SNARKs to enhance privacy and efficiency in various applications. I also have a keen interest in evaluating the security of cryptographic protocols software implementation, ensuring they are robust against emerging threats and vulnerabilities. Overall, my research aims to bridge the gap between theoretical cryptography and practical security solutions, addressing critical challenges in the rapidly evolving digital landscape.

Education

2020 – Present **Ph.D. Computer Science**, Purdue University, *West Lafayette, IN*
Advisor: *Dr. Christina L. Garman*

2018 – 2020 **M.S. Computer Science**, Indiana University Bloomington, *Bloomington, IN*
Advisor: *Dr. David J. Crandall*

2014 – 2018 **B.A. Mathematics**, Indiana University Bloomington, *Bloomington, IN*
B.S. Computer Science, Indiana University Bloomington, *Bloomington, IN*

Research Experience

Aug 2020 – Present **Research Assistant**, *Purdue University, West Lafayette, IN*
Research Assistant with Christina L. Garman

May 2018 – Aug 2018 **Visiting Scholar**, *York University, Toronto, ON*
Visiting Scholar with James H. Elder

Aug 2018 – Jul 2020 **Research Assistant**, *Indiana University, Bloomington, IN*
Research Assistant with Xiaojing Liao, David J. Crandall, and Selma Sabanovic

Jan 2017 – May 2017 **Undergraduate Researcher**, *Indiana University, Bloomington, IN*

Employment History

May 2025 – Aug 2025 **Software Developer Intern**, *Amazon.com Inc, Seattle, WA*

Aug 2024 – Dec 2024 **Instructor**, *Ball State University, Muncie, IN*

Aug 2020 – Dec 2023 **Teaching Assistant**, *Purdue University, West Lafayette, IN*

Aug 2019 – Aug 2020 **Software Developer**, *Indiana University, Bloomington, IN*

Apr 2018 – June 2020 **Education Specialist**, *Pervasive Technology Institute, Bloomington, IN*

May 2017 – Aug 2017 **Assistant Registrar**, *Indiana University, Bloomington, IN*

Aug 2016 – Dec 2017 **Teaching Assistant**, *Indiana University, Bloomington, IN*

Professional Service

Conference Leadership/Organization

2024 **Organizer**, iDash Privacy & Security Workshop

Organizer, NDSS Workshop on AI System with Confidential Computing

Professional Service (continued)

Program Committees

2025 **Reviewer**, International Journal of Applied Cryptography
Artifact PC Member, Privacy Enhancing Technologies Symposium
2024 **Artifact PC Member**, Journal of Systems Research
Reviewer, International Journal of Applied Cryptography
2023 **Reviewer**, IEEE/ACM Transactions on Computational Biology and Bioinformatics
PC Member, ICLR Workshop on Backdoor Attacks and Defenses in Machine Learning
Sub-Reviewer, IEEE International Conference on Medical Artificial Intelligence
2022 **Sub-Reviewer**, Financial Cryptography and Data Security

Research Publications

Publications

1. **Yongming Fan**, Priyam Biswas, and Christina Garman, "R+R: A systematic study of cryptographic function identification approaches in binaries," in *Proceedings of the 40th Annual Computer Security Applications Conference*, 2024.
2. **Yongming Fan**, Yuquan Xu, and Christina Garman, "SNARKProbe: An automated security analysis framework for zksnark implementations," in *International Conference on Applied Cryptography and Network Security*, Springer Nature Switzerland, 2024, pp. 340–372.
3. Zhixin Li, Rui Zhu, Zihao Wang, Jiale Li, Kaiyuan Liu, Yue Qin, **Yongming Fan**, Mingyu Gu, Zhihui Lu, Jie Wu, *et al.*, "FairFix: Enhancing fairness of pre-trained deep neural networks with scarce data resources," in *2024 10th IEEE International Conference on Intelligent Data and Security (IDS)*, IEEE, 2024, pp. 14–20.
4. Xurui Li, Yue Qin, Rui Zhu, Tianqianjin Lin, **Yongming Fan**, Yangyang Kang, Kaisong Song, Fubang Zhao, Changlong Sun, Haixu Tang, *et al.*, "STINMatch: Semi-supervised semantic-topological iteration network for financial risk detection via news label diffusion," in *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing*, 2023, pp. 9304–9315.

Thesis

1. **Yongming Fan**, "Segmentation of retinal optic from a new approach hough transform," M.S. thesis, Indiana University Bloomington, May 2020.

Preprint

1. **Yongming Fan**, Priyam Biswas, and Christina Garman, "Evaluating approaches for identifying cryptographic functions in binaries," Currently under review, 2025.
2. **Yongming Fan** and Christina Garman, "SigmaGraph: Using graph algorithms to verify sigma protocols," Currently under review, 2024.
3. **Yongming Fan**, Rui Zhu, Zihao Wang, Chenghong Wang, Haixu Tang, Ye Dong, Hyunghoon Cho, and Lucila Ohno-Machado, "ByzSFL: Achieving byzantine-robust secure federated learning with zero-knowledge proofs," Currently under review, 2024.

Teaching

Primary Instructor

Fall 2024 — **CS 647 Cybersecurity and Secure Software** *at Ball State University*

Teaching Assistant

Fall 2022 — **CS 52600 Information Security** *at Purdue University*
Spring 2021 — **CS 50023 Data Engineering I** *at Purdue University*
Fall 2020 — **CS 50023 Data Engineering I** *at Purdue University*
Fall 2019 — **CSCI-A 202 Introduction to Programming II** *at Indiana University Bloomington*
Fall 2017 — **CSCI-A 290 Topics in Programming: Arduino** *at Indiana University Bloomington*
CSCI-A 290 Topics in Programming: Python *at Indiana University Bloomington*
CSCI-A 201 Introduction to Programming I *at Indiana University Bloomington*
Summer 2017 — **CSCI-A 201 Introduction to Programming I** *at Indiana University Bloomington*
Spring 2017 — **CSCI-A 201 Introduction to Programming I** *at Indiana University Bloomington*
Fall 2016 — **CSCI-A 201 Introduction to Programming I** *at Indiana University Bloomington*

Miscellaneous Experience

Talks and Presentations

Dec 2024 — **A Systematic Study of Cryptographic Function Identification Approaches in Binaries**, 40th Annual Computer Security Applications Conference, *Honolulu, HI*

Dec 2024 — **Evaluating Approaches for Identifying Cryptographic Functions in Binaries**, Learning from Authoritative Security Experiment Results Workshop, *Honolulu, HI*

Awards and Achievements

2024 — **ACSAC 2024 Student Conferenceships**
Total: $800 *from Applied Computer Security Associates (ACSA)*

2019 — **Intelligent Systems for Sustainable Urban Mobility Travel Expenses**
Total: Can$1,500 *from Intelligent Systems for Sustainable Urban Mobility (ISSUM)*

Vision: Science to Applications Awards
Total: Can$7,500 *from Vision: Science to Applications (VISTA), York University*

2018 — **Graduate Student Fellowship**
Total: $39,041 *from University Information Technology Services (UITS), Indiana University*

2017 — **Anurag & Aruna Mendhekar Scholarship**
Total: $2,000 *from Luddy School of Informatics, Computing, and Engineering, Indiana University Bloomington*

Software Development

2022-2024 — **CryptoBinary:** Cryptographic Function Identification Reproduction and Replication Framework (`https://github.com/BARC-Purdue/CryptoBinary`); *developed at BARC, Purdue University.*

2021-2023 — **SNARKProbe:** An Automated Security Analysis Framework for zkSNARK Implementation (`https://github.com/fanym919/snarkprobe`); *developed at BARC, Purdue University.*

2019-2020 — **DLO Post Processing:** Glaucomatous Blind Spots Analysis and Blood Vessel Calibration System; *developed at Swanson Lab, Indiana University.*

Miscellaneous Experience (continued)

2019 **Trans-Plan:** An Intelligent Systems for Sustainable Urban Mobility (`https://www.elderlab.yorku.ca/research/systems/`); *developed at Elder Laboratory, York University.*