Yongming Fan

✉ fan322@purdue.edu 🌐 http://www.yongming.fan

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: *Christina Garman*
2018 – 2020	**M.S. Computer Science**, Indiana University Bloomington, Bloomington, IN Advisor: *David Crandall* Thesis title: *Segmentation of Retinal Optic from a New Approach Hough Transform*
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*
May 2018 – Aug 2018	**Visiting Scholar** *York University, Toronto, ON*
Aug 2018 – Jul 2020	**Research Assistant** *Indiana University Bloomington, Bloomington, IN*
Jan 2017 – May 2017	**Undergraduate Researcher** *Indiana University Bloomington, Bloomington, IN*

Professional Service

Conference Leadership/Organization

2024	**Organizer**, NDSS Workshop on AI System with Confidential Computing

Program Committees

2023	**Reviewer**, IEEE/ACM Transactions on Computational Biology and Bioinformatics
	Reviewer, 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**, Yuquan Xu, and Christina Garman, "Snarkprobe: An automated security analysis framework for zksnark implementations," in *International Conference on Applied Cryptography and Network Security*, Springer, 2024.

2. Xurui Li, Yue Qin, Rui Zhu, Tianqianjin Lin, **Yongming Fan**, Yangyang Kang, Kaisong Song, Fubang Zhao, Changlong Sun, Haixu Tang, and Xiaozhong Liu, “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.
3. **Yongming Fan**, “Segmentation of retinal optic from a new approach hough transform,” M.S. thesis, Indiana University Bloomington, May 2020.

Submitted

1. **Yongming Fan**, Priyam Biswas, and Christina Garman, “Sok: A systematic study of cryptographic function identification approaches in binaries,” Currently under review, 2023.
2. **Yongming Fan** and Christina Garman, “Sigmagraph: Using graph algorithms to verify sigma protocols,” Currently under review, 2023.
3. Zhixin Li, Rui Zhu, Zihao Wang, Jiale Li, Kaiyuan Liu, Yue Qin, **Yongming Fan**, Mingyu Gu, Zhihui Lu, Jie Wu, Hongfeng Chai, Xiaofeng Wang, and Haixu Tang, “Fairfix: Enhancing fairness of pre-trained deep neural networks with scarce data resources,” Currently under review, 2023.

Employment History

Aug 2020 – Dec 2023	**Teaching Assistant** *Purdue University, West Lafayette, IN*
Aug 2019 – Aug 2020	**Software Developer** *Indiana University School of Optometry, Bloomington, IN*
Apr 2018 – June 2020	**Application Developer** *Pervasive Technology Institute, Bloomington, IN*
May 2017 – Aug 2017	**Assistant Registrar** *Indiana University Bloomington, Bloomington, IN*
Aug 2016 – Dec 2017	**Teaching Assistant** *Indiana University Bloomington, Bloomington, IN*

Miscellaneous Experience

Awards and Achievements

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

2021-2023
- **Purdue University**, West Lafayette, IN
  SNARKProbe: An Automated Security Analysis Framework for zkSNARK Implementation (`https://github.com/fanym919/snarkprobe`)

2019-2020
- **Indiana University**, Bloomignton, IN
  DLO Post Processing: Glaucomatous Blind Spots Analysis and Blood Vessel Calibration System

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