# YUE QIN

(+86)18609637782 | (+1)8126069439 | qinyue@iu.edu | Academic Homepage

## Research Interests

Trustworthy AI; Privacy compliance check; Cybercrime; Data-driven privacy and security

## Education

**Indiana University Bloomington** — Aug. 2018 – Jun. 2024 (expected)
*Ph.D. Program in Computer Science* — *GPA: 4.0/4.0*

**Xiamen University** — Aug. 2014 – Jun. 2018
*Bachelor of Engineering in Software Engineering* — *GPA: 3.56/4.0*

## Publications

**Conference Papers** | *Cybersecurity, Machine Learning, Natural Language Processing*

- **Yue Qin**, Yue Xiao, Xiaojing Liao. "Vulnerability Intelligence Alignment via Masked Graph Attention Networks". *to appear in Proceedings of ACM Conference on Computer and Communications Security (CCS), 2023.*
- **Yue Qin**, Zhuoqun Fu, Chuyun Deng, Xiaojing Liao, Jia Zhang, Haixin Duan. "Stolen Risks of Models with Security Properties". *to appear in Proceedings of ACM Conference on Computer and Communications Security (CCS), 2023.*
- Yue Xiao, Zhengyi Li, **Yue Qin**, Xiaolong Bai, Jiale Guan, Xiaojing Liao, Luyi Xing."Lalaine: Measuring and Characterizing Non-Compliance of Apple Privacy Labels at Scale". *In Proceedings of USENIX Security Symposium (Security), 2023.*
- Zhuoqun Fu, Mingxuan Liu, **Yue Qin**, Jia Zhang, Yuan Zou, Qilei Yin, Qi Li, Haixin Duan. "Encrypted Malware Traffic Detection via Graph-based Network Analysis". *In Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2022.*
- Chuyun Deng, Mingxuan Liu, **Yue Qin**, Jia Zhang, Hai-Xin Duan, Donghong Sun. "ValCAT: Variable-Length Contextualized Adversarial Transformations Using Encoder-Decoder Language Model". *In Proceedings of the 2022 Conference of the North American Chapter of the Association for Computational Linguistics (NAACL)*, 2022.
- Yizheng Chen, Shiqi Wang, **Yue Qin**, Xiaojing Liao, Suman Jana, David Wagner. "Learning Security Classifiers with Verified Global Robustness Properties". *In Proceeding of ACM Conference on Computer and Communications Security (CCS)*, 2021.
- Jian Peng, **Yue Qin**, Yadi Wei, Yuan Zhou. "A PTAS for the Bayesian Thresholding Bandit Problem". *International Conference on Artificial Intelligence and Statistics.*, 2020.
- Peng Wang, Xiaojing Liao, **Yue Qin**, XiaoFeng Wang. "Into the Deep Web: Understanding E-commerce Fraud from Autonomous Chat with Cybercriminals". *In Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS)*, 2020.
- Yi Chen, Luyi Xing, **Yue Qin**, Xiaojing Liao, XiaoFeng Wang, Kai Chen, Wei Zou. "Devils in the Guidance: Predicting Logic Vulnerabilities in Payment Syndication Services through Automated Documentation Analysis". *In Proceeding of USENIX Security Symposium (Security)*, 2019.
- Xiangwen Zhang, Jinsong Su, **Yue Qin**, Yang Liu, Rongrong Ji, and Hongji Wang. "Asynchronous Bidirectional Decoding for Neural Machine Translation". *In Proceedings of Association for the Advancement of Artificial Intelligence (AAAI)*, 2018.
- Jing Yang, Biao Zhang, **Yue Qin**, Xiangwen Zhang, Qian Lin and Jinsong Su. "Otem&Utem: Over- and Under Translation Evaluation Metric for NMT". *In Proceddings of 7th CCF International Conference, (NLPCC)*, 2018.

**Journal Papers & Thesis** | *Natural Language Processing, Graph Analysis*

- Jinsong Su, Xiangwen Zhang, Qian Lin, Yue Qin, Junfeng Liu, Yang Liu. "Exploiting Reverse Target-Side Contexts for Neural Machine Translation via Asynchronous Bidirectional Decoding". *Artificial Intelligence* (CCF-A, JCR-2) 2019. 10.1016/j.artint. 2019.103168
- Biao Zhang, Deyi Xiong, Jinsong Su, Yue Qin. "Alignment-Supervised Bidimensional Attention-Based Recursive Auto encoders for Bilingual Phrase Representation". *IEEE Transactions on Cybernetics.* (CCF-B, JCR-1) PP(99):1-11.2018. DOI: 10.1109/TCYB. 2018.2868982
- Jinsong Su, Shan wu, Biao Zhang, Changxing Wu, Yue Qin, Deyi Xiong. "A Neural Generative Autoencoder for Bilingual Word Embeddings". *Information Sciences.*(CCF-B, JCR-2) 2017.
- Yue Qin. (2014). Time Series Analysis of Multiple Financial Evolving Network Based on Motif Entropy. (Bachelor Thesis, Xiamen University).

## Professional Activities

**Review Service** | *Served as a reviewer*

- IEEE Transactions on Information Forensics and Security (TIFS), 2023
- EAI SecureComm 2023
- Annual Computer Security Applications Conference (ACSAC) 2022,2023 Artifact Evaluation (AE)
- Information Processing and Management, 2023

**Review Service** | *Served as a sub-reviewer*

- IEEE Symposium on Security and Privacy (Oakland), 2020, 2021, 2022, 2024
- ACM Conference on Computer and Communications Security (CCS), 2019
- Network and Distributed System Security Symposium (NDSS), 2019, 2020, 2021, 2022
- Annual Computer Security Applications Conference (ACSAC), 2019, 2020, 2021
- IEEE Transactions on Dependable and Secure Computing (TDSC), 2020, 2021, 2022

## Experience

**Research Assistant** Sept. 2018 – Now

*Indiana University Bloomington* *Computer Science Department*

- Exploring robust learning frameworks to enforce machine learning models with security and privacy guarantees.
- Investigating the interconnections between robustness, privacy, and generalization of machine learning systems.
- Developing trustworthy intelligent systems for cybersecurity thrusts and practices such as privacy compliance, threat detection, and vulnerability assessment.

**Advisor**: Xiaojing Liao

**Front-end Engineer Intern** Oct. 2017 – Jan. 2018

*Tech Valley, Xiamen Big Data Education & Research Center, China* *Technology Department*

- Responsible for the front-end design based on Bootstrap/Ajax frame and realizing Javascript
- Running parts of mapping between database model and java model
- Developing through SpringMVC + Spring + MyBatis frame; using SVN and Scrum for management
- Gaining experience in project development and in team cooperation

## Student Research Mentoring

| | | |
|---|---|---|
| Zhuoqun Fu | M.S. Institute for Network Sciences and Cyberspace, Tsinghua University | 2022 |
| *Project:* | *Spatio-Temporal Graph for Encrypted Malware Traffic Detection* | |
| | *Learning ML models with security properties* | |
| Chuyun Deng | M.S. Institute for Network Sciences and Cyberspace, Tsinghua University | 2022 |
| *Project:* | *Variable-Length Contextualized Adversarial Text Transformations* | |
| | *Learning security properties for NLP models* | |
| Ruize Gao | B.S. Industrial and Enterprise Systems Engineering, UIUC (expected 2024) | 2023 |
| *Project:* | *Membership inference attacks against models with security properties* | |

## Honors and Awards

| | |
|---|---|
| ACM CCS Student Travel Grant | 2023 |
| IEEE EthiCS Student Travel Grant | 2023 |
| ACM CCS Best Paper Award Runner-up | 2021 |