# Yang Xiao

Updated October 21, 2022

**Email**: xiaoy@uky.edu

**Office**: 233 James F. Hardymon Building, University of Kentucky

**Phone**: +1 (859) 257-3101

**Web**: https://yang-sec.github.io/

| | | |
|---|---|---|
| PROFESSIONAL EXPERIENCE | **Assistant Professor**<br>Department of Computer Science, University of Kentucky | 08/2022 – Present |
| | **Graduate Research Assistant**<br>Department of Electrical and Computer Engineering, Virginia Tech | 08/2017 – 05/2022 |
| | **Research Intern**<br>Mathematics and Modeling Department, Schlumberger-Doll Research | 05/2016 – 08/2016 |

RESEARCH INTERESTS

Distributed System Security
Blockchain and Decentralized Systems
Trusted and Privacy-preserving Computing
Mobile Communications and Network Security
Cyber-Physical Security

| | | |
|---|---|---|
| EDUCATION | **Virginia Polytechnic Institute and State University** | 08/2017 – 05/2022 |

– Ph.D. in Computer Engineering
   Dissertation: *Blockchain and Distributed Consensus: From Security Analysis to Novel Applications*
   Advisor: Dr. Wenjing Lou

**University of Michigan**   09/2015 – 04/2017
– M.S. in Electrical Engineering-Systems

**Shanghai Jiao Tong University**   09/2010 – 06/2014
– B.S.E. in Information Engineering
– (Secondary) B.Econ. in Finance

BOOK CHAPTERS

1. Distributed Consensus Protocols and Algorithms
   **Y. Xiao**, N. Zhang, J. Li, W. Lou, Y. T. Hou
   *Blockchain for Distributed Systems Security, Wiley & Sons, 2019*

JOURNAL PUBLICATIONS

1. SoftMix: A Secure Offchain-Supported Bitcoin-Compatible Mixing Protocol
   H. Xie, S. Fei; Z. Yan; **Y. Xiao**
   *In by IEEE Transactions on Dependable and Secure Computing (**TDSC**), October 2022 (early access).*

2. MANDA: On Adversarial Example Detection for Network Intrusion Detection System
   N. Wang, Y. Chen, **Y. Xiao**, Y. Hu, W. Lou, Y. T. Hou
   *In IEEE Transactions on Dependable and Secure Computing (**TDSC**), February 2022 (early access).*

3. Decentralized Spectrum Access System: Vision, Challenges, and a Blockchain Solution
   **Y. Xiao**, S. Shi, W. Lou, C. Wang, X. Li, N. Zhang, Y. T. Hou, J. H. Reed
   *In IEEE Wireless Communications, February 2022.*

4. Challenges and New Directions in Securing Spectrum Access Systems
   S. Shi, **Y. Xiao**, W. Lou, C. Wang, X. Li, Y. T. Hou, J. H. Reed
   *In IEEE Internet of Things Journal (**IOT-J**), April 2021.*

5. A Survey of Distributed Consensus Protocols for Blockchain Networks

**Y. Xiao**, N. Zhang, W. Lou, Y. T. Hou
*In IEEE Communications Surveys & Tutorials (**COMST**), 2020.*

6. Offloading Decision in Edge Computing for Continuous Applications Under Uncertainty
W. Chang, **Y. Xiao**, W. Lou, G. Shou
*In IEEE Transactions on Wireless Communications (**TWC**), 2020.*

7. Performance Analysis of Random Access Network with Post-backoff
C. Bu, **Y. Xiao**, T. Ye, P. Wu, X. Zhang, J. Wu
*In Telecommunications Science, 2016.*

CONFERENCE
PUBLICATIONS

1. Squeezing More Utility via Adaptive Clipping on Deferentially Private Gradients in Federated Meta-Learning
N. Wang, **Y. Xiao**, Y. Chen, N. Zhang, W. Lou, Y. T. Hou
*Annual Computer Security Applications Conference (**ACSAC**), December 2022. (AR=24.1%)*

2. Mobile Tracking in 5G and Beyond Networks: Problems, Challenges, and New Directions
C. Du, H. Yu, **Y. Xiao**, W. Lou, C. Wang, R. Gazda, Y. T. Hou
*IEEE International Conference on Mobile Ad-Hoc and Smart Systems (**MASS**), October 2022.*

3. CANShield: Signal-based Intrusion Detection for Controller Area Networks
M. H. Shahriar, **Y. Xiao**, P. Moriano, W. Lou, Y. T. Hou
*Embedded Security in Cars (**escar**) USA conference, June 2022.*

4. FLARE: Defending Federated Learning against Model Poisoning Attacks via Latent Space Representations
N. Wang, **Y. Xiao**, Y. Chen, Y. Hu, W. Lou, Y. T. Hou
*ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**), May 2022. (AR=18.4%)*

5. Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication
**Y. Xiao**, S. Shi, N. Zhang, W. Lou, Y. T. Hou
*Annual Computer Security Applications Conference (**ACSAC**), December 2020. (AR=23.2%)*

6. PrivacyGuard: Enforcing Private Data Usage Control with Blockchain and Off-chain Contract Execution
**Y. Xiao**, N. Zhang, J. Li, W. Lou, Y. T. Hou
*European Symposium on Research in Computer Security (**ESORICS**), September 2020. (AR=19.7%)*

7. Modeling the Impact of Network Connectivity on Consensus Security of Proof-of-Work Blockchain
**Y. Xiao**, N. Zhang, W. Lou, Y. T. Hou
*IEEE International Conference on Computer Communications (**INFOCOM**), July 2020. (AR=19.8%)*

TEACHING
EXPERIENCE

**Instructor**, University of Kentucky
– CS585/685: Intermediate/Special Topics in Computer Science: Blockchain Technologies    Fall 2022

**Guest Lecturer**, Virginia Tech
– CS5560: Fundamentals of Information Security - Cryptocurrency & Blockchain    Spring 2019

**Graduate Teaching Assistant**, Virginia Tech
– ECE2534: Microcontroller Programming and Interfacing    Fall 2017

**Undergraduate Tutor**, SJTU
– CS358: Data Structure    Fall 2014

ACADEMIC
SERVICES

**Journal and Conference Review**
– IEEE International Conference on Computer Communications (INFOCOM)    2021
– IEEE International Conference on Sensing, Communication, and Networking (SECON)    2022
– IEEE/ACM Transactions on Networking (TON)    2020, 2021, 2022

|  |  |  |
|---|---|---|
|  | – IEEE Internet of Things Journal (IOT-J) | 2020, 2021, 2022 |
|  | – International Journal of Intelligent Systems (INT2) | 2021 |
|  | – IEEE Transactions on Dependable and Secure Computing (TDSC) | 2019, 2020, 2022 |
|  | – Digital Communications and Networks (DCAN) | 2019, 2020 |
|  | – EAI International Conference on Security and Privacy in Comm. Netw. (SecureComm) | 2019 |
|  | – Future Generation Computer Systems (FGCS) | 2018, 2019 |

**Program Committee**

– International Conference on Computer Communictions and Networks (ICCCN) — 2023

**Panelist**

2019 Secure and Trustworthy CyberSpace (SaTC) PI Meeting Undergraduate Track, NSF — 10/2019
– Panel: What to Expect from Grad School

**Conference Organization**

IEEE International Conference on Computer Communications (INFOCOM)
– Web Co-chair, INFOCOM 2023, New York area — 06/2022 − 05/2023

IEEE Conference on Communications and Network Security (CNS)
– Web Chair, CNS 2020, virtual — 09/2019 − 07/2020
– Student Volunteer, CNS 2019, Washington DC — 06/2019

TALKS,
POSTERS

Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication
– Invited talk, *Learning from Authoritative Security Experiment Results (LASER) Workshop* — 12/2020

A Layered View towards Blockchain: From Consensus Security to Smart Contract Application
– Invited talk, *CS Graduate Seminars*, Virginia Tech — 11/2020

Enforcing Private Data Usage Control with Blockchain and Attested Off-chain Contract Execution
– Poster, 2019 SaTC PI Meeting, NSF, Alexandria, VA — 04/2019

A Graph Random-Walk Based Sampling Algorithm for Load Balancing in Cloud Systems
– Poster, *6th Midwest Workshop on Control and Game Theory*, Ann Arbor, MI — 04/2017

AWARDS

**INFOCOM 2020 Student Travel Grant** — 2020
– Awarded by the INFOCOM 2020 organizing committee

**BitShares Graduate Fellowship** — 2019
– Awarded by Virginia Tech CS Department, funded by BitShares Inc.

**Completion of the Elite Engineer Cultivation Program in Information Engineering** — 2014
– Certified by Shanghai Jiao Tong University

**First Prize in the 28th National Physics Contest of College Students (Shanghai Division)** — 2011
– Awarded by Shanghai Physics Society

PROFESSIONAL
MEMBERSHIPS

– IEEE Member, Communications Society, Computer Society — 11/2017 − Present
– ACM Professional Member — 10/2020 − Present

CODING SKILLS   C/C++, Python, MATLAB, HTML, C#