Xiaolan Gu

University of Arizona, Tucson, AZ
✉ xiaolang@email.arizona.edu
🏠 https://xiaolangu.github.io/

EDUCATION

- **University of Arizona, Tucson, AZ** 2018 - Present
  Ph.D., Electrical and Computer Engineering (GPA: 4.00/4.00)
- **Beihang University, Beijing, China** 2015 - 2018
  M.S., Automation Science and Electrical Engineering (GPA: 3.94/4.00)
- **Beihang University, Beijing, China** 2011 - 2015
  B.S., Mathematics and Systems Science (GPA: 3.58/4.00)

EXPERIENCE

- **Research Intern, Security Lab, Baidu Inc. USA** Summer 2019
  Mentor: Dr. Yueqiang Cheng Sunnyvale, CA
  - ◇ Job Description:
    - – Contribute to breakthrough innovations in technologies of security-oriented big data analysis.
    - – For private key-value data collection, we developed a novel framework with an advanced data sampling method and optimized perturbation of key-value pairs, which outperforms state-of-the-art protocol.
    - – Publication highlight: top-tier conference (refer to paper [USENIX Security' 20])
- **Graduate Research Assistant, University of Arizona** Fall 2018 - Present
  Advisor: Dr. Ming Li Tucson, AZ
  - ◇ Local Differential Privacy and Its Applications (publication highlight: top-tier conferences)
    - – To simultaneously enhance the utility for record-level queries and statistical/aggregated analysis, we proposed a novel and practical protocol for location-based applications (refer to paper [CNS' 19])
    - – For private frequency estimation of categorical data, we proposed a relaxed privacy notion that provides differentiated privacy guarantees for data inputs that have distinct privacy requirements, and developed a practical protocol with optimized parameters to get the benefit from the non-uniform indistinguishability (refer to paper [ICDE' 20])
  - ◇ Differentially Private and Robust Machine Learning/Federated Learning
    - – Compared with centralized setting, federated learning with differential privacy (DP) suffers from bad privacy-utility tradeoff and is venerable to model poisoning attacks. To mitigate these challenges, we leverage secure multiparty computation techniques and develop a hybrid solution (with both DP and crypto), which achieves better privacy-utility tradeoff and provides robustness guarantee against model poisoning attacks.

SKILLS

- – Python (numpy, scipy, pandas, pytorch, sklearn), Matlab, C
- – Privacy-preserving techniques: differential privacy (DP) and secure multiparty computation (SMC)
- – Robust machine learning/federated learning against adversarial examples and poisoning attacks

RELEVANT COURSEWORK

- – Machine Learning Theory
- – Online Learning and Multi-armed Bandits
- – Fundamentals of Data Science for Engineers
- – Data Structure
- – Database Admin
- – Nonlinear Optimization
- – Probability and Random Processes for Engineering
- – Fundamentals of Information and Network Security
- – Fundamentals of Computer Network
- – Information Theory

PUBLICATIONS

- **Conference Papers**

[1] **Xiaolan Gu**, Ming Li, Yueqiang Cheng, Li Xiong and Yang Cao, "PCKV: Locally Differentially Private Correlated Key-Value Data Collection with Optimized Utility", 29th USENIX Security Symposium (**USENIX Security 2020**), pp. 967-984, Boston, MA, August 2020. (acceptance rate: 158/972=16.3%)

[2] **Xiaolan Gu**, Ming Li, Li Xiong and Yang Cao, "Providing Input-Discriminative Protection for Local Differential Privacy", 36th IEEE International Conference on Data Engineering (**ICDE 2020**), pp. 505-516, Dallas, TX, April 2020. (acceptance rate: 129/568=23%)

[3] **Xiaolan Gu**, Ming Li, Yang Cao and Li Xiong. "Supporting both Range Queries and Frequency Estimation with Local Differential Privacy", 7th IEEE Conference on Communications and Network Security (**IEEE CNS 2019**), pp. 124-132, Washington, D.C., June 2019. (acceptance rate: 32/115=28%)

- **Journal Papers**

[1] **Xiaolan Gu** and Qiusheng Wang, "Sparse canonical correlation analysis algorithm with alternating direction method of multipliers", *Communications in Statistics - Simulation and Computation*, pp. 1-17, 2019.

[2] **Xiaolan Gu**, Yong Cui, Qiusheng Wang, Haiwen Yuan, Luxing Zhao and Guifang Wu, "Received signal strength indication-based localisation method with unknown path-loss exponent for HVDC electric field measurement", *IET - High Voltage*, 2(4), pp. 261-266, 2017.

[3] Qiusheng Wang, **Xiaolan Gu** and Jinyong Lin, "Adaptive notch filter design under multiple identical bandwidths", *AEU - International Journal of Electronics and Communications*, 2017(82), pp. 202-210, 2017.

[4] Qiusheng Wang, **Xiaolan Gu**, Yingyi Liu, and Haiwen Yuan, "Digital multiple notch filter design with Nelder-Mead simplex method", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, 100(1), pp. 259-265, 2017.

PROFESSIONAL SERVICES

- **Conference Reviewers:** ICICS 2019.
- **Journal Reviewers:** IEEE TVT 2020, ACM TOPS 2021.
- **External Reviewers:** VLDB 2022, VLDB 2021, IEEE INFOCOM 2021, IEEE ICDE 2021, ACSAC 2020, ACM WiSec 2020, IEEE TIFS 2020, IEEE ICDCS 2020, IEEE INFOCOM 2020, ACM CCS 2019.

AWARDS AND HONORS

– Student Grant	*USENIX Security Symposium*	Aug. 2020
– Student Travel Grant	*IEEE Conference on Communications and Network Security*	Jun. 2019
– Outstanding Graduate Award	*Beihang University*	Mar. 2018
– *Guanghua* Scholarship	*Beihang University*	Nov. 2016
– Outstanding Graduate Award	*Beihang University*	Jun. 2015

TEACHING

- Teaching Assistant, Computer Programming for Engineering Applications (C language) 2018 - 2019