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
  - ◇ **Key-value Data Collection under Local Differential Privacy [USENIX Security' 20]**
    - We developed a novel framework that utilizes correlated perturbations (between key and values) to enhance the privacy-utility tradeoff under local differential privacy (LDP).
    - We proposed an optimized privacy budget allocation approach with closed-form solutions to further improve the utility.
    - Experimental results validates the improvement of the proposed scheme (which outperforms the state-of-the-art).
- **Graduate Research Assistant, University of Arizona** Fall 2018 - Present
  Advisor: Dr. Ming Li Tucson, AZ
  - ◇ **Privacy-preserving and Robust Federated Learning** (paper under review)
    - Background: comparing with centralized machine learning, federated learning with differential privacy (DP) suffers from both poor privacy-utility tradeoff and venerability to model poisoning attacks.
    - We developed a hybrid solution (with both DP and crypto), which achieves better privacy-utility tradeoff and is resistant to client collusion. By leveraging Secure Multiparty Computation (MPC) techniques, the Gaussian noise added for privacy purpose is shown to provide robustness guarantee against model poisoning attacks.
    - Experiments on non-iid MNIST and CIFAR-10 validate that DP enhances robustness in our solution.
  - ◇ **Input-Discriminative Local Differential Privacy [ICDE' 20]**
    - We proposed a new privacy notion called Input-Discriminative LDP (ID-LDP), which is shown to be a fine-grained version of LDP and only needs less perturbation (and thus yields better utility) than LDP.
    - We developed two mechanisms for single-item input and item-set input on the application of frequency estimation, where both two mechanisms are shown to satisfy ID-LDP.
    - Experimental results validate the correctness of the theoretical Mean Squared Error analysis and effectiveness of our new notion and proposed mechanisms (comparing with the state-of-the-art LDP protocols).
  - ◇ **On Hybrid Queries under Local Differential Privacy [CNS' 19]**
    - We proposed a novel and practical protocol for location-based applications to simultaneously enhance the utility for record-level queries and statistical/aggregated analysis.
    - We analyzed the theoretical Mean Squared Error of our protocol and showed the relationship to an existing protocol.
    - Experimental results on both synthetic and real-world location datasets show that the proposed scheme outperforms the state-of-the-art mechanisms on both range queries and frequency estimation.

SKILLS

- Python (numpy, scipy, pandas, pytorch, scikit-learn), Matlab, C/C++, Java, SQL
- Optimization, Statistics, Multivariate Analysis, Algorithms, Machine Learning, Federated Learning
- Privacy-preserving techniques: Differential Privacy (DP) and Secure Multi-Party Computation (MPC)
- Robust machine learning (and federated learning) against adversarial examples and poisoning attacks

PUBLICATIONS

- **Preprints**

  [1] **Xiaolan Gu**, Ming Li, and Li Xiong, "PRECAD: Privacy-Preserving and Robust Federated Learning via Crypto-Aided Differential Privacy", *arXiv preprint*, 2021.

- **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", **USENIX Security**, 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", *IEEE International Conference on Data Engineering* (**ICDE**), 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", *IEEE Conference on Communications and Network Security* (**CNS**), 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:** INFOCOM'22, ICICS'19.

– **Journal Reviewers:** IEEE TKDE 2021, ACM TOPS 2021, IEEE TVT 2020.

– **External Reviewers:** VLDB'22, VLDB'21, INFOCOM'21, ICDE'21, ACSAC'20, ACM WiSec'20, IEEE TIFS 2020, IEEE ICDCS'20, INFOCOM'20, ACM CCS'19.

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

RELEVANT COURSEWORK

– Machine Learning Theory; Online Learning and Multi-armed Bandits; Fundamentals of Data Science for Engineers.

– Nonlinear Optimization; Information Theory; Probability and Random Processes for Engineering; Fundamentals of Information and Network Security; Fundamentals of Computer Network.