Zhikun Zhang

Ph.D.

CISPA Helmholtz Center for Information Security
Stuhlsatzenhaus 5, 66123 Saarbrücken
☎
✉ *zhikun.zhang@cispa.saarland*

Education & Experience

2019.12- **Postdoc at CISPA Helmholtz Center for Information Security**.
Supervised by Prof. Michael Backes

2014.09-2019.09 **Ph.D. of Control Science and Engineering**, *College of Control Science and Engineering, Zhejiang University*.
Co-supervised by Prof. Jiming Chen (Changjiang Scholar) and Prof. Shibo He (Thousand Youth Talents Plan)

2017.10-2019.05 **Visiting Scholar of Computer Science**, *Computer Science Department, Purdue University*.
Supervised by Prof. Ninghui Li (Chair of ACM SIGSAC)

2010.09-2014.06 **Bachelor, Major in Control Science and Engineering**, *College of Control Science and Engineering, Shandong University*.
Supervised by Prof. Huanshui Zhang (Changjiang Scholar)

Research Interest

My recent research concentrates on differential privacy, machine learning privacy and their interactions. Specifically, I am interested in appling differential privacy (as well as local differential privacy) to enhence privacy for different data analysis tasks. Besides, I am also interested in evaluating the privacy leakage risks of different machine learning models (e.g., membership inference, property inference, etc), and denfending these potential threats using differential privacy.

Publications

Conference: [C3] **Zhikun Zhang**, Tianhao Wang, Ninghui Li, Shibo He, Jiming Chen. CALM: Consistent Adaptive Local Marginal for Marginal Release under Local Differential Privacy, Proceedings of **ACM CCS**, Toronto, Canada, 2018.

[C2] Jiajun Zhang, Xiaohui Liang, Shibo He, **Zhikun Zhang**, Zhiguo Shi. Re-DPoctor: Real-time Health Data Releasing with w-day Differential Privacy, *Proceedings of IEEE GLOBECOM*, Singapore, 2017.

[C1] **Zhikun Zhang**, Heng Zhang, Shibo He, Peng Cheng. Achieving Bilateral Utility Maximization and Location Privacy Preservation in Database-driven Cognitive Radio Networks, *Proceedings of IEEE MASS*, Dallas, USA, 2015.

Journal: [J3] **Zhikun Zhang**, Shibo He, Junshan Zhang, Jiming Chen. REAP: An Efficient Incentive Mechanism for Reconciling Aggregation Accuracy and Individual Privacy in Crowdsensing, *IEEE Transactions on Information Forensics & Security* (**TIFS**), Vol. 13(12): 2995-3007, Dec, 2018.

[J2] Yuyi Sun, Fei Tong, **Zhikun Zhang**, Shibo He. Throughput Modeling and Analysis of Random Access in Narrow-band Internet of Things, Vol. 5(3): 1485-1493, Jun, 2018.

[J1] **Zhikun Zhang**, Heng Zhang, Shibo He, Peng Cheng. Bilateral Privacy-preserving Utility Maximization Protocol in Database-driven Cognitive Radio Networks, *IEEE Transactions on Dependable and Secure Computing* (**TDSC**), DOI:10.1109/TDSC.2017.2781248, to appear.

Preprint: [P1] **Zhikun Zhang**, Shibo He, Mengyuan Zhang, Jiming Chen. LEPA: Incentivizing Long-term Privacy-perserving Data Aggregation in Crowdsensing, submitted to IEEE ToN.

Ongoing: [G1] **Zhikun Zhang**, Tianhao Wang, Ninghui Li. DPSyn: Differentially Private Synthetic Data Publication.

Projects

2018.11–2019.05 **Differentially Private Synthetic Dataset Challenge**, *National Institute of Standards and Technology*, Runner Up Prize.

2018.08–2018.09 **The Unlinkable Data Challenge: Advancing Methods in Differential Privacy**, *National Institute of Standards and Technology*, Runner Up Prize.

Honors & Awards

2018.10 **National Scholarship for Excellent Ph.D. Student**, The Chinese Government.

2018.10 **Tang Lixin Scholarship**, Zhejiang University.

2015.10 **Student Travel Grant**, IEEE MASS.

2014.09 **Quantification to defense the Ph.D degree directly without examination**.

2013.10 **National Scholarship for Excellent Undergraduate Student**, The Chinese Government.

2012.10 **Scholarship for Excellent Student**, Shandong University.

Academic Services

Reviewer for: IEEE Transactions on Vehicular Technology

IEEE Communication Letter

Peer-to-Peer Networking and Applications

IEEE International Conference on Computer Communications (INFOCOM'17 18)

ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'17)

IEEE International Conference on Sensing, Communication and Networking (SECON'17)

IEEE International Conference on Communications (ICC'15 16 17)

IEEE Global Communications Conferences (GLOBECOM'15 16)

IEEE Annual Conference on Decision and Control (CDC'15 16)

Attendence: ACM Conference on Computer and Communications Security (CCS'18), Toronto, Canada, Oct. 15-19, 2018

IEEE International Conference on Communications in China (ICCC'16), Chengdu, China, Jul. 27-29, 2016

Chinese Automation Congress (CAC'15), Wuhan, China, Nov. 27-29, 2015

IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS'15), Dallas, USA, Oct. 19-22, 2015

ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'15), Hangzhou, China, Jun. 22-25, 2015

China Internet Security Conference (ISC'14), Beijing, China, Sep. 29-30, 2014

Skilled Computer Languages

Programming Python, C, Visual C++, MATLAB, SQL

OS MacOS, Linux, Windows