Zhikun Zhang

Dr.

CISPA Helmholtz Center for Information Security
Stuhlsatzenhaus 5, 66123 Saarbrücken
☎ *+86 137 5716 2052*
✉ *zhikun.zhang@cispa.de*

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 and Prof. Shibo He

2017.10-2019.05 **Visiting Scholar of Computer Science**, *Computer Science Department, Purdue University*.
Supervised by Prof. Ninghui Li

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

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:

[C10] Min Chen, **Zhikun Zhang**, Tianhao Wang, Michael Backes, Mathias Humbert, Yang Zhang. Graph Unlearning. **ACM CCS** 2021 (under major revision).

[C9] Yugeng Liu, Rui Wen, Xinlei He, Ahmed Salem, **Zhikun Zhang**, Michael Backes, Emiliano De Cristofaro, Mario Fritz, Yang Zhang. ML-Doctor: Holistic Risk Assessment of Inference Attacks Against Machine Learning Models. **USENIX Security** 2022 (under major revision).

[C8] **Zhikun Zhang**, Min Chen, Michael Backes, Yun Shen, Yang Zhang. Inference Attacks Against Graph Embedding. To appear in **USENIX Security** 2022.

[C7] Min Chen, **Zhikun Zhang**, Tianhao Wang, Michael Backes, Mathias Humbert, Yang Zhang. When Machine Unlearning Jeopardize Privacy. To appear in **ACM CCS** 2021.

[C6] Tianhao Wang, Joann Qiongna Chen, **Zhikun Zhang**, Dong Su, Yueqiang Cheng, Zhou Li, Ninghui Li, Somesh Jha. Continuous Release of Data Streams under both Centralized and Local Differential Privacy. To appear in **ACM CCS** 2021.

[C5] Linkang Du, **Zhikun Zhang**, Shaojie Bai, Changchang Liu, Shouling Ji, Peng Cheng, Jiming Chen. AHEAD: Adaptive Hierarchical Decomposition for Range Query under Local Differential Privacy. To appear in **ACM CCS** 2021.

[C4] **Zhikun Zhang**, Tianhao Wang, Ninghui Li, Jean Honorio, Michael Backes, Shibo He, Jiming Chen, Yang Zhang. PrivSyn: Differentially Private Data Synthesis. To appear in **USENIX Security** 2021.

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

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

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

Journal:

[J4] Ninghui Li, **Zhikun Zhang**, Tianhao Wang. DPSyn: Experiences in the NIST Differential Privacy Data Synthesis Challenges. In *Journal of Privacy and Confidentiality (JPC)*.

[J3] **Zhikun Zhang**, Shibo He, Junshan Zhang, Jiming Chen. REAP: An Efficient Incentive Mechanism for Reconciling Aggregation Accuracy and Individual Privacy in Crowdsensing. In *IEEE Transactions on Information Forensics & Security* (**TIFS**).

[J2] Yuyi Sun, Fei Tong, **Zhikun Zhang**, Shibo He. Throughput Modeling and Analysis of Random Access in Narrow-band Internet of Things. In IEEE Internet of Things Journal.

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

Competitions

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

2021.07 **Nomination Award for Outstanding Doctoral Thesis**, Zhejiang University.

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

Conference PC Member: PoPETS 2022

ICLR 2021

ESORICS 2021

TrustCom 2020, 2021

GLOBECOM 2020

ICA3PP 2020

Journal Guest Editor: Frontiers in Communications and Networks

External Reviewer: USENIX Security 2021

CCS 2020, 2021

EuroSP 2021

AsiaCCS 2021

PoPETS 2021

CCSW 2020

ESORICS 2020

AAAI 2020

INFOCOM 2017, 2018, 2020

MobiHoc 2017

SECON 2017

ICC 2015, 2016, 2017

GLOBECOM 2015, 2016

CDC 2015, 2016

IEEE TII 2021

ACM TOPS 2020

IEEE TDSC 2019

IEEE TVT 2017

PPNA 2016