Yang Zhang | CV

zhang@cispa.saarland • yangzhangalmo.github.com

last update: June 9, 2020

Employment

CISPA Helmholtz Center for Information Security — **Saarbrücken, Germany**
Faculty Member — *February 2020 –*

CISPA Helmholtz Center for Information Security — **Saarbrücken, Germany**
Research Group Leader — *January 2019 – January 2020*

CISPA, Saarland University — **Saarbrücken, Germany**
Postdoctoral Researcher — *January 2017 – December 2018*
Host: Michael Backes

Education

University of Luxembourg — **Luxembourg, Luxembourg**
Ph.D. in Computer Science, highest honor — *December 2012 – November 2016*
Supervisor: Sjouke Mauw and Jun Pang

Shandong University — **Jinan, China**
Master in Computer Science — *September 2009 – June 2012*

University of Luxembourg — **Luxembourg, Luxembourg**
Master in Informatics, exchange student — *September 2010 – October 2011*

Shandong University — **Jinan, China**
Bachelor in Software Engineering — *September 2005 – June 2009*

Research Projects

Leading Scientist — **Helmholtz Medical Security, Privacy, and AI Research Center**
November 2018 -

co-PI — **Helmholtz Pilot Funding "TFDA" (~120,000 Euro)**
December 2019 - November 2022

Research Interests

Privacy, Machine Learning, Social Network Analysis, Algorithmic Fairness, Urban Informatics

Service

- PC member
  - CCS 2020 2019, WWW 2020, ICWSM 2020 2018, RAID 2020, PETS 2021 2020, ESORICS 2020, Socinfo 2020 2019, ISMB/ECCB 2019, SACMAT 2020 2019, TrustCom 2019
- External reviewer
  - CSCW 2018, ICWSM 2019, CCS 2018, S&P 2019 2018, NDSS 2020, USENIX Security 2017,

Euro S&P 2018, ESORICS 2017, PETS 2019 2017
- IEEE TKDE, PLOS ONE, PeerJ

Awards

- Best paper award, ARES 2014
- Distinguished paper award, NDSS 2019 (4/521)

Publication

Conference

[1] Rui Wen and Yu Yu and Xiang Xie and **Yang Zhang**. LEAF: A Faster Secure Search Algorithm via Localization, Extraction, and Reconstruction. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2020.

[2] Dingfan Chen and Ning Yu and **Yang Zhang** and Mario Fritz. GAN-Leaks: A Taxonomy of Membership Inference Attacks against Generative Models. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2020.

[3] Ahmed Salem and Apratim Bhattacharya and Michael Backes and Mario Fritz and **Yang Zhang**. Updates-Leak: Data Set Inference and Reconstruction Attacks in Online Learning. In *USENIX Security Symposium (USENIX Security)*. USENIX, 2020.

[4] Inken Hagestedt and Mathias Humbert and Pascal Berrang and Irina Lehmann and Roland Eils and Michael Backes and **Yang Zhang**. Membership Inference Against DNA Methylation Databases. In *IEEE European Symposium on Security and Privacy (Euro S&P)*. IEEE, 2020.

[5] **Yang Zhang** and Mathias Humbert and Bartlomiej Surma and Praveen Manoharan and Jilles Vreeken and Michael Backes. Towards Plausible Graph Anonymization. In *Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2020.

[6] Jinyuan Jia and Ahmed Salem and Michael Backes and **Yang Zhang** and Neil Zhenqiang Gong. MemGuard: Defending against Black-Box Membership Inference Attacks via Adversarial Examples. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 259–274. ACM, 2019.

[7] Zheng Li and Chengyu Hu and **Yang Zhang** and Shanqing Guo. How to Prove Your Model Belongs to You: A Blind-Watermark based Framework to Protect Intellectual Property of DNN. In *Annual Computer Security Applications Conference (ACSAC)*, pages 126–137. ACSAC, 2019.

[8] Zhiqiang Zhong and **Yang Zhang** and Jun Pang. A Graph-Based Approach to Explore Relationship Between Hashtags and Images. In *International Conference Web Information Systems Engineering (WISE)*, pages 473–488. Springer, 2019.

[9] Tahleen Rahman and Bartlomiej Surma and Michael Backes and **Yang Zhang**. Fairwalk: Towards Fair Graph Embedding. In *International Joint Conferences on Artifical Intelligence (IJCAI)*, pages 3289–3295. IJCAI, 2019.

[10] **Yang Zhang**. Language in Our Time: An Empirical Analysis of Hashtags. In *The Web Conference (WWW)*, pages 2378–2389. ACM, 2019.

[11] Ahmed Salem and **Yang Zhang** and Mathias Humbert and Pascal Berrang and Mario Fritz and Michael Backes. ML-Leaks: Model and Data Independent Membership Inference Attacks and Defenses on Machine Learning Models. In *Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2019.

[12] Inken Hagestedt and **Yang Zhang** and Mathias Humbert and Pascal Berrang and Haixu Tang and XiaoFeng Wang and Michael Backes. MBeacon: Privacy-Preserving Beacons for DNA Methylation Data. In *Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2019.

[13] Fanghua Zhao and Linan Gao and **Yang Zhang** and Zeyu Wang and Bo Wang and Shanqing Guo. You Are Where You App: An Assessment on Location Privacy of Social Applications. In *International Symposium on Software Reliability Engineering (ISSRE)*, pages 236–247. IEEE, 2018.

[14] **Yang Zhang** and Mathias Humbert and Tahleen Rahman and Cheng-Te Li and Jun Pang and Michael Backes. Tagvisor: A Privacy Advisor for Sharing Hashtags. In *The Web Conference (WWW)*, pages 287–296. ACM, 2018.

[15] Pascal Berrang and Mathias Humbert and **Yang Zhang** and Irina Lehmann and Roland Eils and Michael Backes. Dissecting Privacy Risks in Biomedical Data. In *IEEE European Symposium on Security and Privacy (Euro S&P)*. IEEE, 2018.

[16] Michael Backes and Mathias Humbert and Jun Pang and **Yang Zhang**. walk2friends: Inferring Social Links from Mobility Profiles. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1943–1957. ACM, 2017.

[17] Jun Pang and **Yang Zhang**. Quantifying Location Sociality. In *ACM Conference on Hypertext and Social Media (HT)*, pages 145–154. ACM, 2017.

[18] Jun Pang and **Yang Zhang**. DeepCity: A Feature Learning Framework for Mining Location Check-Ins. In *International Conference on Weblogs and Social Media (ICWSM)*, pages 652–655. AAAI, 2017.

[19] Yan Wang and Zongxu Qin and Jun Pang and **Yang Zhang** and Xin Jin. Semantic Annotation for Places in LBSN Using Graph Embedding. In *ACM International Conference on Information and Knowledge Management (CIKM)*, page 2343–2346. ACM, 2017.

[20] **Yang Zhang** and Minyue Ni and Weili Han and Jun Pang. Does #like4like Indeed Provoke More Likes? In *International Conference on Web Intelligence (WI)*, pages 179–186. ACM, 2017.

[21] Minyue Ni and **Yang Zhang** and Weili Han and Jun Pang. An Empirical Study on User Access Control in Online Social Networks. In *ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 12–23. ACM, 2016.

[22] Jun Pang and Polina Zablotskaia and **Yang Zhang**. On Impact of Weather on Human Mobility in Cities. In *International Conference Web Information Systems Engineering (WISE)*, pages 247–256. Springer, 2016.

[23] Jun Pang and **Yang Zhang**. Location Prediction: Communities Speak Louder than Friends. In *ACM Conference on Online Social Networks (COSN)*, pages 161–171. ACM, 2015.

[24] **Yang Zhang** and Jun Pang. Distance and Friendship: A Distance-based Model for Link Prediction in Social Networks. In *Asia-Pacific Web Conference (APWeb)*, pages 55–66. Springer, 2015.

[25] Jun Pang and **Yang Zhang**. Event Prediction with Community Leaders. In *Conference on Availability, Reliability and Security (ARES)*, pages 238–243. IEEE, 2015.

[26] Marcos Cramer and Jun Pang and **Yang Zhang**. A Logical Approach to Restricting Access in Online Social Networks. In *ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 75–86. ACM, 2015.

[27] Jun Pang and **Yang Zhang**. Cryptographic Protocols for Enforcing Relationship-based Access Control Policies. In *Annual IEEE Computers, Software and Applications Conference (COMPSAC)*, pages 484–493. IEEE, 2015.

[28] Ran Cheng and Jun Pang and **Yang Zhang**. Inferring Friendship from Check-in Data of Location-based Social Networks. In *Workshop on Social Network Analysis in Applications (SNAA)*. IEEE, 2015.

[29] Jun Pang and **Yang Zhang**. Exploring Communities for Effective Location Prediction. In *International Conference on World Wide Web (WWW)*, pages 87–88. ACM, 2015.

[30] **Yang Zhang** and Jun Pang. Community-driven Social Influence Analysis and Applications. In *International Conference on Web Engineering (ICWE)*. Springer, 2015.

[31] Jun Pang and **Yang Zhang**. A New Access Control Scheme for Facebook-style Social Networks. In *Conference on Availability, Reliability and Security (ARES)*, pages 1–10. IEEE, 2014.

[32] Dalin Chu and Johann Großschädl and Zhe Liu and Volker Müller and **Yang Zhang**. Twisted Edwards-Form Elliptic Curve Cryptography for 8-bit AVR-based Sensor Nodes. In *ACM Workshop on Asia Public-key Cryptography (ASIAPKC)*, pages 39–44. ACM, 2013.

[33] Johann Großschädl and **Yang Zhang**. Efficient Prime-Field Arithmetic for Elliptic Curve Cryptography on Wireless Sensor Nodes. In *International Conference on Computer Science and Network Technology (ICCSNT)*. IEEE, 2011.

Journal

[34] Bo-Heng Chen and Cheng-Te Li and Kun-Ta Chuang and Jun Pang and **Yang Zhang**. An Active Learning-based Approach for Location-aware Acquaintance Inference. *Knowledge and Information Systems*, 2018.

[35] Jun Pang and **Yang Zhang**. A New Access Control Scheme for Facebook-style Social Networks. *Computers & Security*, 2015.

Teaching

Instructor — **Advanced Lecture: Privacy Enhancing Technologies**
May 2020 - September 2020, Saarland University

Instructor — **Seminar: Data-driven Approaches on Understanding Disinformation**
May 2020 - September 2020, Saarland University

Instructor — **Seminar: Data Privacy**
October 2019 - February 2020, Saarland University

Instructor — **Advanced Lecture: Privacy Enhancing Technologies**
April 2019 - September 2019, Saarland University

Instructor — **Seminar: Biomedical Privacy**
April 2019 - September 2019, Saarland University

Instructor — **Seminar: Data Privacy**
October 2018 - February 2019, Saarland University

Instructor — **Advanced Lecture: Privacy Enhancing Technologies**
April 2018 - September 2018, Saarland University

Instructor — **Seminar: Adversarial Machine Learning**
April 2018 - September 2018, Saarland University

Students

Ph.D. Students

Allen Xinlei He — **CISPA Helmholtz Center for Information Security**
February 2020 -

Zheng Li — **CISPA Helmholtz Center for Information Security**
August 2020 -

Co-supervised Ph.D. Students

Min Chen — **CISPA Helmholtz Center for Information Security**
with Michael Backes — *August 2019 -*

Yugeng Liu — **CISPA Helmholtz Center for Information Security**
with Michael Backes — *October 2019 -*

Ahmed Salem — **CISPA Helmholtz Center for Information Security**
with Michael Backes — *February 2017 -*

Bartlomiej Surma — **CISPA Helmholtz Center for Information Security**
with Michael Backes — *June 2016 -*

Rui Wen — **CISPA Helmholtz Center for Information Security**
with Michael Backes — *October 2019 -*

Yang Zou — **CISPA Helmholtz Center for Information Security**
with Michael Backes — *August 2019 -*

Visiting Ph.D. Students

Suliya — **Chinese Academy of Science**
January 2020 -

Interns

Yuhao Mao — **Zhejiang University**
June 2020 - September 2020

Yihan Ma — **Fudan University**
June 2020 - September 2020

Ziqi Zhang — **Peking University**, *June 2020 - December 2020*

Alumni

Xiaoyi Chen — **Peking University**
visiting Ph.D. student — *October 2019 - March 2020*

Ge Han — **Shandong University**
visiting Ph.D. student — *October 2019 - March 2020*

Tianhao Wang — **Purdue University**
intern — *February 2020 - March 2020*

Zeyu Yang — **Zhejiang University**
visiting Ph.D. student — *October 2019 - March 2020*

Bachelor/Master Thesis Students

Ran Cheng — **University of Luxembourg**, *March 2015 - September 2015*

Haftom Meles — **Saarland University**, *January 2019 - June 2019*

Arthur Sanin — **Saarland University**, *August 2019 - December 2019*

Franz Schramm — **Saarland University**, *August 2019 - December 2019*