

# Yang Zhang | CV

✉ zhang@cispa.de • 🌐 yangzhangalmo.github.com

last update: July 1, 2021

## Employment

---

<b>CISPA Helmholtz Center for Information Security</b> <i>Faculty</i>	<b>Saarbrücken, Germany</b> <i>February 2020 –</i>
<b>CISPA Helmholtz Center for Information Security</b> <i>Research Group Leader</i>	<b>Saarbrücken, Germany</b> <i>January 2019 – January 2020</i>
<b>CISPA, Saarland University</b> <i>Postdoctoral Researcher</i> Host: Michael Backes	<b>Saarbrücken, Germany</b> <i>January 2017 – December 2018</i>

## Education

---

<b>University of Luxembourg</b> <i>Ph.D. in Computer Science, highest honor</i> Supervisor: Sjouke Mauw and Jun Pang	<b>Luxembourg, Luxembourg</b> <i>December 2012 – November 2016</i>
<b>Shandong University</b> <i>Master in Computer Science</i>	<b>Jinan, China</b> <i>September 2009 – June 2012</i>
<b>University of Luxembourg</b> <i>Master in Informatics, exchange student</i>	<b>Luxembourg, Luxembourg</b> <i>September 2010 – October 2011</i>
<b>Shandong University</b> <i>Bachelor in Software Engineering</i>	<b>Jinan, China</b> <i>September 2005 – June 2009</i>

## Research Projects

---

<b>Leading Scientist</b>	<b>Helmholtz Medical Security, Privacy, and AI Research Center</b> <i>November 2018 -</i>
<b>co-PI</b>	<b>Helmholtz Pilot Funding “TFDA” (~120,000 Euro)</b> <i>December 2019 - November 2022</i>

## Research Interests

---

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

## Service

---

- PC member
  - 2022: USENIX Security, ICLR, PETS, ASIACCS
  - 2021: USENIX Security, CCS, WWW, AAI, Euro S&P, PETS, ASIACCS, ESORICS, SACMAT
  - 2020: CCS, WWW, ICWSM, RAID, PETS, ESORICS, Socinfo, SACMAT
  - 2019: CCS, Socinfo, ISMB/ECCB, SACMAT

## Awards

---

- Distinguished paper award, NDSS 2019
- Distinguished reviewer award, TrustML Workshop 2020 (co-located with ICLR 2020)
- Best paper award, ARES 2014

## Publication

---

### Conference.....

- [1] Zheng Li and **Yang Zhang**. Membership Leakage in Label-Only Exposures. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2021.
- [2] Xinlei He and Jinyuan Jia and Michael Backes and Neil Zhenqiang Gong and **Yang Zhang**. Stealing Links from Graph Neural Networks. In *USENIX Security Symposium (USENIX Security)*. USENIX, 2021.
- [3] Zhikun Zhang and Tianhao Wang and Jean Honorio and Ninghui Li and Michael Backes and Shibo He and Jiming Chen and **Yang Zhang**. PrivSyn: Differentially Private Data Synthesis. In *USENIX Security Symposium (USENIX Security)*. USENIX, 2021.
- [4] Fatemeh Tahmasbi and Leonard Schild and Chen Ling and Jeremy Blackburn and Gianluca Stringhini and **Yang Zhang** and Savvas Zannettou. “Go eat a bat, Chang!”: On the Emergence of Sinophobic Behavior on Web Communities in the Face of COVID-19. In *The Web Conference (WWW)*. ACM, 2021.
- [5] 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)*, pages 1219–1232. ACM, 2020.
- [6] 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)*, pages 343–362. ACM, 2020.
- [7] 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)*, pages 1291–1308. USENIX, 2020.
- [8] 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)*, pages 509–520. IEEE, 2020.
- [9] **Yang Zhang** and Mathias Humbert and Bartłomiej 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.
- [10] 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.

- [11] 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.
- [12] 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.
- [13] Tahleen Rahman and Bartlomiej Surma and Michael Backes and **Yang Zhang**. Fairwalk: Towards Fair Graph Embedding. In *International Joint Conferences on Artificial Intelligence (IJCAI)*, pages 3289–3295. IJCAI, 2019.
- [14] **Yang Zhang**. Language in Our Time: An Empirical Analysis of Hashtags. In *The Web Conference (WWW)*, pages 2378–2389. ACM, 2019.
- [15] 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.
- [16] 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.
- [17] 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.
- [18] **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.
- [19] 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)*, pages 62–76. IEEE, 2018.
- [20] 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.
- [21] Jun Pang and **Yang Zhang**. Quantifying Location Sociality. In *ACM Conference on Hypertext and Social Media (HT)*, pages 145–154. ACM, 2017.
- [22] 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.
- [23] 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.

- [24] **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.
- [25] 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.
- [26] 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.
- [27] 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.
- [28] **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.
- [29] Jun Pang and **Yang Zhang**. Event Prediction with Community Leaders. In *Conference on Availability, Reliability and Security (ARES)*, pages 238–243. IEEE, 2015.
- [30] 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.
- [31] 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.
- [32] Jun Pang and **Yang Zhang**. Exploring Communities for Effective Location Prediction. In *International Conference on World Wide Web (WWW)*, pages 87–88. ACM, 2015.
- [33] **Yang Zhang** and Jun Pang. Community-driven Social Influence Analysis and Applications. In *International Conference on Web Engineering (ICWE)*. Springer, 2015.
- [34] 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.
- Journal**.....
- [35] Xinlei He and Qingyuan Gong and Yang Chen and **Yang Zhang** and Xin Wang and Xiaoming Fu. DatingSec: Detecting Malicious Accounts in Dating Apps Using a Content-Based Attention Network. *IEEE Transactions on Dependable and Secure Computing*, 2021.
- [36] 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.
- [37] Jun Pang and **Yang Zhang**. A New Access Control Scheme for Facebook-style Social Networks. *Computers & Security*, 2015.

## Teaching

---

### Lectures

---

Instructor	<b>Advanced Lecture: Privacy Enhancing Technologies</b> <i>May 2021 - September 2021, Saarland University</i>
Instructor	<b>Seminar: Data-driven Understanding of the Disinformation Epidemic</b> <i>May 2021 - September 2021, Saarland University</i>
Instructor	<b>Seminar: Data Privacy</b> <i>October 2020 - February 2021, Saarland University</i>
Instructor	<b>Advanced Lecture: Privacy Enhancing Technologies</b> <i>May 2020 - September 2020, Saarland University</i>
Instructor	<b>Seminar: Data-driven Approaches on Understanding Disinformation</b> <i>May 2020 - September 2020, Saarland University</i>
Instructor	<b>Seminar: Data Privacy</b> <i>October 2019 - February 2020, Saarland University</i>
Instructor	<b>Advanced Lecture: Privacy Enhancing Technologies</b> <i>April 2019 - September 2019, Saarland University</i>
Instructor	<b>Seminar: Biomedical Privacy</b> <i>April 2019 - September 2019, Saarland University</i>
Instructor	<b>Seminar: Data Privacy</b> <i>October 2018 - February 2019, Saarland University</i>
Instructor	<b>Advanced Lecture: Privacy Enhancing Technologies</b> <i>April 2018 - September 2018, Saarland University</i>
Instructor	<b>Seminar: Adversarial Machine Learning</b> <i>April 2018 - September 2018, Saarland University</i>

### Summer School

---

Instructor	<b>AI Security Summer School</b> <i>August 2020, Zhejiang University</i>
Instructor	<b>InForSec Summer School</b> <i>July 2020, Tsinghua University</i>
Instructor	<b>G.O.S.S.I.P. Summer School</b> <i>August 2019, Shanghai Jiao Tong University</i>
Instructor	<b>InForSec Summer School</b> <i>July 2019, Tsinghua University</i>

## Students

---

### Ph.D. Students

---

Xinlei He	<b>CISPA Helmholtz Center for Information Security</b> <i>February 2020 -</i>
Zheng Li	<b>CISPA Helmholtz Center for Information Security</b> <i>February 2021 -</i>

## Co-supervised Ph.D. Students

<b>Min Chen</b> <i>with Michael Backes</i>	<b>CISPA Helmholtz Center for Information Security</b> <i>August 2019 -</i>
<b>Yihan Ma</b> <i>with Michael Backes</i>	<b>CISPA Helmholtz Center for Information Security</b> <i>July 2021 -</i>
<b>Ahmed Salem</b> <i>with Michael Backes</i>	<b>CISPA Helmholtz Center for Information Security</b> <i>February 2017 -</i>
<b>Bartlomiej Surma</b> <i>with Michael Backes</i>	<b>CISPA Helmholtz Center for Information Security</b> <i>June 2016 -</i>
<b>Yang Zou</b> <i>with Michael Backes</i>	<b>CISPA Helmholtz Center for Information Security</b> <i>August 2019 -</i>

## Ph.D. Preparatory Phase

<b>Yiyong Liu</b>	<b>CISPA Helmholtz Center for Information Security</b> <i>October 2021 -</i>
<b>Yugeng Liu</b>	<b>CISPA Helmholtz Center for Information Security</b> <i>October 2019 -</i>
<b>Xinyue Shen</b>	<b>CISPA Helmholtz Center for Information Security</b> <i>May 2021 -</i>
<b>Rui Wen</b>	<b>CISPA Helmholtz Center for Information Security</b> <i>October 2019 -</i>
<b>Minxing Zhang</b>	<b>CISPA Helmholtz Center for Information Security</b> <i>May 2021 -</i>

## Visiting Ph.D. Students

<b>Joann Chen</b>	<b>UC Irvine</b> <i>July 2021 -</i>
<b>Ge Han</b>	<b>Shandong University</b> <i>October 2019 -</i>
<b>Haiming Wang</b>	<b>Zhejiang University</b> <i>July 2021 -</i>

## Alumni

<b>Suliya</b> <i>visiting Ph.D. student</i>	<b>Chinese Academy of Science</b> <i>January 2020 - January 2021</i>
<b>Xiaoyi Chen</b> <i>visiting Ph.D. student</i>	<b>Peking University</b> <i>October 2019 - October 2020</i>
<b>Yuhao Mao</b> <i>intern</i>	<b>Zhejiang University</b> <i>June 2020 - September 2020</i>
<b>Leonard Schild</b> <i>research assistant</i>	<b>Saarland University</b> <i>March 2017 - July 2020</i>
<b>Tianhao Wang</b> <i>intern</i>	<b>Purdue University</b> <i>February 2020 - March 2020</i>

**Zeyu Yang**  
*visiting Ph.D. student*

**Zhejiang University**  
*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*

**Yannick Sautter**

**Saarland University**  
*December 2019 - May 2020*

**Franz Schramm**

**Saarland University**  
*August 2019 - December 2019*