Yang Zhang | Curriculum Vitae

Saarland Informatics Campus E9 1, 66123 – Saarbrücken – Germany

✉ yang.zhang@cispa.saarland • 🌐 yangzhangalmo.github.com

last update: July 30, 2019

Employment

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

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

Education

University of Luxembourg **Luxembourg, Luxembourg**
Ph.D. in Informatics, 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 and Privacy Research Center (HMSP)**
November 2018 -

Research Interests

Privacy (machine learning, biomedical data, social networks, location, IoT), Machine Learning, Social Network Analysis, Urban Informatics, Information Security

Service

- PC member
  - PETS 2020, PPML 2019, Socinfo 2019, ISMB/ECCB 2019, CCS 2019, ICWSM 2018, LEMINCS19, SACMAT 2019, TrustCom 2019, ICWS 2019, AI4Mobile 2019
- External reviewer
  - CSCW 2018, ICWSM 2019, CCS 2018, S&P 2018 2019, USENIX Security 2017, Euro S&P 2018, Esorics 2017, PETS 2017 2019
  - IEEE TKDE, PLOS ONE, PeerJ

Awards

- Best paper award, ARES 2014
- Distinguished paper award, NDSS 2014 (4/89)

Publication

[†]lead author [§]corresponding author

Conference

[1] Tahleen Rahman and Bartlomiej Surma and Michael Backes and **Yang Zhang**[§], "Fairwalk: Towards Fair Graph Embedding," in *Proceedings of the 2019 International Joint Conferences on Artifical Intelligence (IJCAI)*. IJCAI, 2019.

[2] **Yang Zhang**[†], "Language in Our Time: An Empirical Analysis of Hashtags," in *Proceedings of the 2019 Web Conference (WWW)*. ACM, 2019.

[3] 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 *Proceedings of the 2019 Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2019.

[4] 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 *Proceedings of the 2019 Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2019.

[5] 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 *Proceedings of the 2018 International Symposium on Software Reliability Engineering (ISSRE)*. IEEE, 2018, pp. 236–247.

[6] **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 *Proceedings of the 2018 Web Conference (WWW)*. ACM, 2018, pp. 287–296.

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

[8] Michael Backes and Mathias Humbert and Jun Pang and **Yang Zhang**†, "walk2friends: Inferring Social Links from Mobility Profiles," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2017, pp. 1943–1957.

[9] Jun Pang and **Yang Zhang**†, "Quantifying Location Sociality," in *Proceedings of the 2017 ACM Conference on Hypertext and Social Media (HT)*. ACM, 2017, pp. 145–154.

[10] Jun Pang and **Yang Zhang**†, "DeepCity: A Feature Learning Framework for Mining Location Check-Ins," in *Proceedings of the 2017 International Conference on Weblogs and Social Media (ICWSM)*. AAAI, 2017, pp. 652–655.

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

[12] **Yang Zhang**† and Minyue Ni and Weili Han and Jun Pang, "Does #like4like Indeed Provoke More Likes?" in *Proceedings of the 2017 International Conference on Web Intelligence (WI)*. ACM, 2017, pp. 179–186.

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

[14] Jun Pang and Polina Zablotskaia and **Yang Zhang**†, "On Impact of Weather on Human Mobility in Cities," in *Proceedings of the 2016 International Conference Web Information Systems Engineering (WISE)*. Springer, 2016, pp. 247–256.

[15] Jun Pang and **Yang Zhang**†, "Location Prediction: Communities Speak Louder than Friends," in *Proceedings of the 2015 ACM Conference on Online Social Networks (COSN)*. ACM, 2015, pp. 161–171.

[16] **Yang Zhang**† and Jun Pang, "Distance and Friendship: A Distance-based Model for Link Prediction in Social Networks," in *Proceedings of the 2015 Asia-Pacific Web Conference (APWeb)*. Springer, 2015, pp. 55–66.

[17] Jun Pang and **Yang Zhang**†, "Event Prediction with Community Leaders," in *Proceedings of the 2015 Conference on Availability, Reliability and Security (ARES)*. IEEE, 2015, pp. 238–243.

[18] Marcos Cramer and Jun Pang and **Yang Zhang**†, "A Logical Approach to Restricting Access in Online Social Networks," in *Proceedings of the 2015 ACM Symposium on Access Control Models and Technologies (SACMAT)*. ACM, 2015, pp. 75–86.

[19] Jun Pang and **Yang Zhang**†, "Cryptographic Protocols for Enforcing Relationship-based Access Control Policies," in *Proceedings of the 2015 Annual IEEE Computers, Software and Applications Conference (COMPSAC)*. IEEE, 2015, pp. 484–493.

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

[21] Jun Pang and **Yang Zhang**†, "Exploring Communities for Effective Location Prediction," in *Proceedings of the 2015 International Conference on World Wide Web (WWW)*. ACM, 2015, pp. 87–88.

[22] **Yang Zhang**† and Jun Pang, "Community-driven Social Influence Analysis and Applications," in *Proceedings of the 2015 International Conference on Web Engineering (ICWE)*. Springer, 2015.

[23] Jun Pang and **Yang Zhang**†, "A New Access Control Scheme for Facebook-style Social Networks," in *Proceedings of the 2014 Conference on Availability, Reliability and Security (ARES)*. IEEE, 2014, pp. 1–10.

[24] 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 *Proceedings of the 2013 ACM Workshop on Asia Public-key Cryptography (ASIAPKC)*. ACM, 2013, pp. 39–44.

[25] Johann Großschädl and **Yang Zhang**†, "Efficient Prime-Field Arithmetic for Elliptic Curve Cryptography on Wireless Sensor Nodes," in *Proceedings of the 2011 International Conference on Computer Science and Network Technology (ICCSNT)*. IEEE, 2011.

Journal

[26] 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.

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

Teaching

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 — **Saarland University**
January 2020 -

Co-supervised Ph.D. Students

Min Chen **Saarland University**
with Michael Backes *February 2017 -*

Xiaoyi Chen **Peking University**
Visiting Ph.D. student *September 2019 -*

Ge Han **Shandong University**
Visiting Ph.D. student *September 2019 -*

Yugeng Liu **Saarland University**
with Michael Backes *October 2019 -*

Tahleen Rahman **Saarland University**
with Michael Backes *September 2016 -*

Ahmed Salem **Saarland University**
with Michael Backes *February 2017 -*

Bartlomiej Surma **Saarland University**
with Michael Backes *June 2016 -*

Rui Wen **Saarland University**
with Michael Backes *October 2019 -*

Zeyu Yang **Zhejiang University**
Visiting Ph.D. student *September 2019 -*

Rui Ye **Saarland University**
with Michael Backes *December 2018 -*

Master Thesis Students

Haftom Meles **Spam Detection in Social Networks**
January 2019 - June 2019, Saarland University

Ran Cheng **Link Prediction in Location-based Social Networks**
March 2015 - September 2015, University of Luxembourg

Student Helper (HIWI)

Leonard Schild **Applied Machine Learning**
May 2017 - , Saarland University

Franz Schramm **Location-based Social Network Mining**
May 2017 - , Saarland University

Joshua Sonnet **Web API Development**
May 2018 - , Saarland University

Selected Talks

- Privacy in the Modern Era: The Cases of Online Social Network and Machine Learning Model
  December 2018, Tsinghua University, Zhejiang University, Shandong University

- Dissecting Privacy Risks in Biomedical Data
  November 2018, Future Medicine 2018
- ML-Leaks: Model and Data Independent Membership Inference Attacks and Defenses on Machine Learning Models
  October 2018, University of Luxembourg and INRIA (Nancy)