

TIANREN LIU 刘天任

trl@pku.edu.cn - (+1) 857 701 8730 - liutianren.com

EMPLOYMENT

- FEB. 2022 ~ **Peking University**, Beijing
Assistant Professor in CENTER ON FRONTIERS OF COMPUTING STUDIES
- SEP. 2019 ~ **University of Washington**, Seattle
OCT. 2021 Postdoct in COMPUTER SCIENCE & ENGINEERING
Host: *Rachel Huijia Lin*

EDUCATION

- JUL. 2016 ~ **Massachusetts Institute of Technology**, Cambridge
AUG. 2019 Ph.D. in COMPUTER SCIENCE
Thesis: Breaking Barriers in Secret Sharing
Advisor: *Vinod Vaikuntanathan*
- SEP. 2014 ~ **Massachusetts Institute of Technology**, Cambridge
JUN. 2016 M.Sc. in ELECTRICAL ENGINEERING & COMPUTER SCIENCE
Thesis: On Basing Private Information Retrieval on NP-Hardness
Advisor: *Vinod Vaikuntanathan*
- SEP. 2010 ~ **Tsinghua University**, Beijing
JUN. 2014 B.Eng. in COMPUTER SCIENCE & TECHNOLOGY
Thesis: Indifferentiability of Confusion-Diffusion Networks
Advisor: *John P. Steinberger*

OTHER ACADEMIC EXPERIENCE

- JAN. 2019 ~ **Technion**, Haifa
FEB. 2019 Research visit, hosted by *Yuval Ishai*
- DEC. 2017 ~ **Technion**, Haifa
JAN. 2018 Research visit, hosted by *Yuval Ishai*
- JUN. 2017 ~ **École Normale Supérieure**, Paris
JUL. 2017 Research visit, hosted by *Hoeteck Wee*
- MAY. 2015 ~ **University of California, Berkeley**, Berkeley
AUG. 2015 Summer program "Cryptography" in Simons Institute
- JAN. 2013 ~ **Massachusetts Institute of Technology**, Cambridge
MAY. 2013 Exchange semester in EECS department
- MAR. 2012 ~ **Microsoft Research Asia**, Beijing
SEP. 2012 Natural linguistic programming, Mentor: *Eric Chang*

CRYPTO PUBLICATIONS (In theoretical computer science, authors are listed in alphabetical order)

- **The t -wise Independence of Substitution-Permutation Networks..**
Tianren Liu, Stefano Tessaro, Vinod Vaikuntanathan. CRYPTO 2021.
- **Multi-party PSM, Revisited: Improved Communication and Unbalanced Communication..**
Leonard Assouline, Tianren Liu. TCC 2021.
- **Information-Theoretic 2-Round MPC without Round Collapsing: Adaptive Security, and More.**
Huijia Lin, Tianren Liu, Hoeteck Wee. TCC 2020.
- **On the Complexity of Decomposable Randomized Encodings, or: How Friendly Can a Garbling-Friendly PRF be?.**
Marshall Ball, Justin Holmgren, Yuval Ishai, Tianren Liu, Tal Malkin. ITCS 2020.
- **Reusable Non-interactive Secure Computation.**
Melissa Chase, Yevgeniy Dodis, Yuval Ishai, Daniel Kraschewski, Tianren Liu, Rafail Ostrovsky, Vinod Vaikuntanathan. CRYPTO 2019.
- **On Basing Search SIVP on NP-Hardness.**
Tianren Liu. TCC 2018. **Best Student Paper.**
- **Breaking the Circuit-Size Barrier in Secret Sharing.**
Tianren Liu, Vinod Vaikuntanathan. STOC 2018.
- **Towards Breaking the Exponential Barrier for General Secret Sharing.**
Tianren Liu, Vinod Vaikuntanathan, Hoeteck Wee. EUROCRYPT 2018.
- **Conditional Disclosure of Secrets via Non-Linear Reconstruction.**
Tianren Liu, Vinod Vaikuntanathan, Hoeteck Wee. CRYPTO 2017.
- **Indifferentiability of Confusion-Diffusion Networks.**
Yevgeniy Dodis, Martijn Stam, John P. Steinberger, Tianren Liu. EUROCRYPT 2016.
- **On Basing Private Information Retrieval on NP-Hardness.**
Tianren Liu, Vinod Vaikuntanathan. TCC 2016-A.

TALKS

- The t -wise Independence of Substitution-Permutation Networks. CRYPTO 2021.
- Multi-party PSM, Revisited: Improved Communication and Unbalanced Communication. TCC 2021.
- Information Theoretic Cryptography with Minimal Interaction.
 - ITCS, Shanghai University of Finance and Economics, 2021 and
 - Peking University, 2021 and
 - Rochester University, 2021 and
 - NYU Shanghai, 2021 and
 - Columbia University, 2021.
- 2-round MPC without Round Collapsing
 - CIS seminar, MIT, 2020 and
 - TCC 2020.
- Reusable Non-interactive Secure Computation. CRYPTO 2019.

- On Basing Search SIVP on NP-Hardness. TCC 2018.
- Secret Sharing and Conditional Disclosure of Secrets.
 - China Theory Week, Tsinghua University, 2018 and
 - ITCS, Shanghai University of Finance and Economics, 2018 and
 - Tokyo Crypto Day, NTT, 2018.
- Breaking the Circuit-Size Barrier in Secret Sharing.
 - Charles River Crypto Day, Cambridge, 2018 and
 - STOC 2018.
- Towards Breaking the Exponential Barrier for General Secret Sharing.
 - NY Crypto Day, Columbia University, 2017 and
 - CIS seminar, MIT, 2017 and
 - EUROCRYPT 2018.
- Conditional Disclosure of Secrets via Non-Linear Reconstruction. CRYPTO 2017.
- Indifferentiability of Confusion-Diffusion Networks. EUROCRYPT 2016.
- On Basing Private Information Retrieval on NP-Hardness. TCC 2016-A.

SERVICE

Conference Program Committees: CYRPTO 2021, ASIACRYPT 2022

AWARDS AND HONORS

NOV. 2018	Best Student Paper Award, TCC
JUL. 2013	Yao Award (Bronze Medal, Tsinghua University)
JAN. 2010	Chinese Mathematical Olympiad (Gold Medal)