Tianren Liu

tianrenl@uw.com - (+1) 857 701 8730 - liutianren.com

Current

Sep. 2019 ~ **University of Washington**, Seattle
Postdoct in Computer Science & Engineering
Host: *Rachel Lin*

Education

Jul. 2016 ~ Aug. 2019 **Massachusetts Institute of Technology**, Cambridge
Ph.D. in Computer Science
Thesis: Breaking Barriers in Secret Sharing
Advisor: *Vinod Vaikuntanathan*

Sep. 2014 ~ Jun. 2016 **Massachusetts Institute of Technology**, Cambridge
M.Sc. in Electrical Engineering & Computer Science
Thesis: On Basing Private Information Retrieval on NP-Hardness
Advisor: *Vinod Vaikuntanathan*

Sep. 2010 ~ Jun. 2014 **Tsinghua University**, Beijing
B.Eng. in Computer Science & Technology
Thesis: Indifferentiability of Confusion-Diffusion Networks
Advisor: *John P. Steinberger*

Academic Experience

Jan. 2019 ~ Feb. 2019 **Technion**, Haifa
Research visit, hosted by *Yuval Ishai*

Dec. 2017 ~ Jan. 2018 **Technion**, Haifa
Research visit, hosted by *Yuval Ishai*

Jun. 2017 ~ Jul. 2017 **École Normale Supérieure**, Paris
Research visit, hosted by *Hoeteck Wee*

May. 2015 ~ Aug. 2015 **University of California, Berkeley**, Berkeley
Summer program "Cryptography" in Simons Institute

Jan. 2013 ~ May. 2013 **Massachusetts Institute of Technology**, Cambridge
Exchange semester in EECS department

Mar. 2012 ~ Sep. 2012 **Microsoft Research Asia**, Beijing
Natural linguistic programming, Mentor: *Eric Chang*

Selected Publications (In theoretical computer science, authors are listed in alphabetical order)

- **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, Tianren Liu, Martijn Stam, John P. Steinberger. EUROCRYPT 2016.
- **On Basing Private Information Retrieval on NP-Hardness**.
  Tianren Liu, Vinod Vaikuntanathan. TCC 2016-A.

Manuscripts

- **Multi-Party PSM, Revisited**.
  Leonard Assouline and Tianren Liu.

Talks

- Reusable Non-interactive Secure Computation. CRYPTO 2019.
- On Basing Search SIVP on NP-Hardness. TCC 2018.
- Secret Sharing and Conditional Disclosure of Secrets (CDS).
  - China Theory Week, Tsinghua University, 2018 and
  - ITCS, Shanghai University of Finance and Economics, 2018 and
  - Tokyo Crypto Day, Tokyo, 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.

Selected Awards and Honors

Nov. 2018	Best Student Paper Award, Theory of Cryptography Conference
Jul. 2013	Yao Award (Bronze Medal, Tsinghua University)
Sep. 2012	National Scholarship (Tsinghua University)
Jan. 2010	Chinese Mathematical Olympiad (Gold Medal)