

Tianren LIU

EMAIL: liutr@mit.edu
PHONE: (+1) 857 701 8730
OFFICE: G604 Stata Center, MIT
HOMEPAGE: liutianren.com

EDUCATION

- JUL. 2016 ~ **Massachusetts Institute of Technology**, Cambridge
Current Ph.D. in ELECTRICAL ENGINEERING & COMPUTER SCIENCE
Advised by Prof. *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
Advised by Prof. *Vinod Vaikuntanathan*
- SEP. 2010 ~ **Tsinghua University**, Beijing
JUN. 2014 B.Eng. in COMPUTER SCIENCE AND TECHNOLOGY, GPA: 92.1/100
Thesis: Indifferentiability of Confusion-Diffusion Networks
Advised by Prof. *John P. Steinberger*

ACADEMIC EXPERIENCE

- 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, GPA: 5.0/5.0
- MAR. 2012 ~ **Microsoft Research Asia**, Beijing
SEP. 2012 Natural linguistic programming, Mentor: *Eric Chang*

PUBLICATIONS

Author names in theoretical computer science are listed in alphabetical order.

- **On Basing Search SIVP on NP-Hardness.**
Tianren Liu. The 16th Theory of Cryptography Conference (TCC 2018).
- **Breaking the Circuit-Size Barrier in Secret Sharing.**
Tianren Liu, Vinod Vaikuntanathan. 50th Annual ACM Symposium on the Theory of Computing (STOC 2018).
- **Towards Breaking the Exponential Barrier for General Secret Sharing.**
Tianren Liu, Vinod Vaikuntanathan, Hoeteck Wee. 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2018).

- **Conditional Disclosure of Secrets via Non-Linear Reconstruction.**
Tianren Liu, Vinod Vaikuntanathan, Hoeteck Wee. 37th International Cryptology Conference (CRYPTO 2017).
- **Indifferentiability of Confusion-Diffusion Networks.**
Yevgeniy Dodis, Tianren Liu, Martijn Stam, John P. Steinberger. 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2016).
- **On Basing Private Information Retrieval on NP-Hardness.**
Tianren Liu, Vinod Vaikuntanathan. The 13th Theory of Cryptography Conference (TCC 2016-A).
- **An End-to-end System to Identify Temporal Relation in Discharge Summaries: 2012 i2b2 Challenge.**
Yan Xu, Yining Wang, Tianren Liu, Junichi Tsujii, Eric I-Chao Chang. Journal of the American Medical Informatics Association (JAMIA), 2013.
- **Joint Segmentation and Named Entity Recognition using Dual Decomposition in Chinese Discharge Summaries.**
Yan Xu, Yining Wang, Tianren Liu, Jiahua Liu, Yubo Fan, Yi Qian, Junichi Tsujii, Eric I Chang. Journal of the American Medical Informatics Association (JAMIA), 2013.

MANUSCRIPTS

- **Reusable Non-interactive Secure Computation.**
Melissa Chase, Yevgeniy Dodis, Yuval Ishai, Daniel Kraschewski, Tianren Liu, Rafail Ostrovsky, Vinod Vaikuntanathan.

TALKS

- Secret Sharing and CDS.
 - China Theory Week, Tsinghua University, 2018 and
 - ITCS, Shanghai University of Finance and Economics, 2018 and
 - (scheduled) Tokyo Crypto Day, Tokyo, 2018.
- Breaking the Circuit-Size Barrier in Secret Sharing. 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.

AWARDS AND HONORS

JUL. 2013 Yao Award (Bronze Medal, Tsinghua University)
 SEP. 2012 National Scholarship
 JAN. 2010 Chinese Mathematical Olympiad (Gold Medal)