

TIANREN LIU 刘天任

trl@pku.edu.cn - (+86) 152 0152 3571 - liutianren.com

Last updated on Oct 24, 2024

EMPLOYMENT

- FEB. 2022 ~ **Peking University**, Beijing
Assistant Professor in CENTER ON FRONTIERS OF COMPUTING STUDIES
- SEP. 2019 ~ **University of Washington**, Seattle
OCT. 2021 Postdoctoral Researcher in COMPUTER SCIENCE & ENGINEERING

EDUCATION

- JUL. 2016 ~ **Massachusetts Institute of Technology**, Cambridge
AUG. 2019 Ph.D. in COMPUTER SCIENCE
- SEP. 2014 ~ **Massachusetts Institute of Technology**, Cambridge
JUN. 2016 M.Sc. in ELECTRICAL ENGINEERING & COMPUTER SCIENCE
- SEP. 2010 ~ **Tsinghua University**, Beijing
JUN. 2014 B.Eng. in COMPUTER SCIENCE & TECHNOLOGY

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

- **How to Garble Mixed Circuits that Combine Boolean and Arithmetic Computations.**
Hanjun Li, Tianren Liu. EUROCRYPT 2024.
- **On Deterministically Approximating Total Variation Distance.**
Weiming Feng, Liqiang Liu, Tianren Liu. SODA 2024.
- **Layout Graphs, Random Walks and the t -wise Independence of SPN Block Ciphers.**
Tianren Liu, Angelos Pelecanos, Stefano Tessaro, Vinod Vaikuntanathan. CRYPTO 2023.
- **Succinct Computational Secret Sharing.**
Benny Applebaum, Amos Beimel, Yuval Ishai, Eyal Kushilevitz, Tianren Liu, Vinod Vaikuntanathan. STOC 2023.
- **New Ways to Garble Arithmetic Circuits.**
Marshall Ball, Hanjun Li, Huijia Lin, Tianren Liu. EUROCRYPT 2023.
- **Two-Round MPC Without Round Collapsing Revisited - Towards Efficient Malicious Protocols.**
Huijia Lin, Tianren Liu. CRYPTO 2022.
- **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.

SERVICE

Conference Program Committees: CRYPTO 2021, 2023, 2024. ASIACRYPT 2022. ICICS 2023. ITC 2024. IJTCS 2024.

Editorial Board: CiC 2024.