Zeyu (Thomas) Liu

email: zl2967@columbia.edu | **website: zeyuthomasliu.github.io**

EDUCATION

Columbia University New York, NY
M.S. in Computer Science, Thesis track, Advanced Research Program Aug 2020 – May 2022
GPA: 4.17/4.33
Relevant Courses: Analysis of Algorithms, Intrusion Detection
Thesis: Oblivious Message Retrieval
Award: Andrew P. Kosoresow Memorial Award for Excellence in Teaching and Service

University of California, Los Angeles Los Angeles, CA
B.S. in Computer Science & B.S. in Applied Mathematics Sep 2016 – Jun 2020
GPA: 3.66/4.00
Dean's Honors List: Fall 2018, Winter 2018, Spring 2018, Winter 2019, and Spring 2020
Relevant Courses: Foundations of Cryptography, Cryptographic Protocols, Mathematical Cryptology

PUBLICATIONS

- **Zeyu Liu**; Eran Tromer, "*Oblivious message retrieval*," Cryptology ePrintArchive, Report 2021/1256, 2021, https://ia.cr/2021/1256. (Accepted by CRYPTO 2022; Contributed talk at RWC 2022)
- **Zeyu Liu**; Daniele Micciancio; Yuriy Polyakov, "*Large-precision homomorphic sign evaluation using FHEW/TFHE bootstrapping*," Cryptology ePrintArchive, Report 2021/1337, 2021, https://ia.cr/2021/1337. (In submission to Asiacrypt 2022.)
- Chengyu Lin**; Zeyu Liu**; Tal Malkin, "*XSPIR: Efficient Symmetric PIR from Ring-LWE*," (Accepted to ESORICS 2022.)
- Tengyu Liu; **Zeyu Liu**; Ziyuan Jiao; Yixin Zhu; Songchun Zhu, "*Synthesizing Diverse and Physically Stable Grasps with Arbitrary Hand Structures using Differentiable Force Closure Estimator*," in IEEE Robotics and Automation Letters, vol. 7, no. 1, pp. 470-477, Jan. 2022.

RESEARCH EXPERIENCE

Graduate Research Assistant under supervision of Dr. Tal Malkin Jun 2020 – Present
The Cryptography Lab, Columbia University

- Designed and implemented novel algorithms for symmetric Private Information Retrieval (PIR) and asymmetric Private Set Intersection (PSI)
- Constructed secure multi-party neural network training based on threshold CKKS homomorphic encryption scheme, with MPI and specially designed FHE-friendly circuits
- Working on the communication lower bounds for PSI and PIR, and on the relationship between the two protocols and between their lower bounds

Graduate Research Assistant under supervision of Dr. Eran Tromer Feb 2021 – Present
The Cryptography Lab, Columbia University

- Defined the notions of compact Oblivious Message Retrieval (OMR) and Oblivious Message Detection (OMD), allowing the recipients to retrieve or detect their messages privately against malicious senders/recipients (that can cause Denial-of-Service attacks) and key-linkability attacks and proved the correctness and security of our schemes using Ring-LWE assumption.
- Constructed practical (and compact) OMR/OMD algorithms using various techniques including a bespoke composition of different lattice-based schemes, designing special circuits for our purpose and optimizing the multiplicative depth to avoid bootstrapping operations, sparse linear random coding, etc; implementation publicly available at: https://github.com/ZeyuThomasLiu/ObliviousMessageRetrieval; paper will be presented at RWC 2022

- Working on integrating our OMR schemes with Zcash light-wallets and on group OMR/OMD for group anonymous message delivery systems

Research Scientist Trainee under supervision of Dr. Yuriy Polyakov Jun 2021 – Present
Crypto Team, Duality Technologies Inc.

- Contributed to designing large-precision homomorphic sign evaluation using FHEW/TFHE bootstrapping and constructed FHEW/TFHE functional bootstrapping procedure supporting arbitrary function evaluation; implementation publicly available at https://gitlab.com/palisade/palisade-development/-/tree/SignEval
- Developed and coded the scheme switching algorithm between CKKS and FHEW/TFHE, involving several implementation-specific optimizations, and introduced arcsine function during FHEW/TFHE functional bootstrapping to improve the output precision
- Integrated large-precision homomorphic sign evaluation and scheme switching to construct ArgMin/ArgMax functionalities for non-interactive secure decision tree training, which has not been fully achieved by any prior works yet.

Research under supervision of Dr. Songchun Zhu Mar 2018 – May 2021
Center for Vision, Cognition, Learning, and Autonomy, UCLA

- Developed novel differentiable estimator of force closure to synthesize diverse grasps with arbitrary hand structures; our paper was accepted by IEEE Robotics and Automation Letters

TEACHING EXPERIENCE

Graduate Course Assistant, Introduction to Cryptography, Prof. Tal Malkin
Columbia University Jan 2022 –May 2022
Graduate Course Assistant, Introduction to Cryptography, Prof. Periklis Papakonstantinou
Columbia University Jun 2021 – Aug 2021
Graduate Course Assistant, Analysis of Algorithms, Prof. Eleni Drinea
Columbia University Jan 2021 – May 2021

TECHNICAL SKILLS AND SPOKEN LANGUAGES

Technical Skills: C++, Python, MATLAB, C, Lisp, Assembly, R, ML, Java, OCaml, Prolog, Scheme, Verilog, Golang
Spoken Languages: Chinese (Native), English (Fluent)