# CV: Yibin Yang

yyang811@gatech.edu, +1-6785649024, https://cc.gatech.edu/∼yyang811

## EDUCATION

**Georgia Institute of Technology, Atlanta, USA** **Aug 2019 - present**
*Ph.D. Program* in Computer Science
**Advisor:** Vladimir Kolesnikov

**Tsinghua University, Beijing, China** **Aug 2015 - Jun 2019**
*B.Eng Program* in Computer Science and Technology

**KTH Royal Institute of Technology, Stockholm, Sweden** **Spring 2018**
*Exchange Student*, Department of Computational Science and Technology

## RESEARCH INTERESTS

Zero-Knowledge Proof
Multi-Party Computation
Blockchain

## EXPERIENCE

**Bar-Ilan University, Ramat Gan, Israel** **May 2023 - July 2023**
*Visiting Researcher*, **Advisor:** Carmit Hazay
**Topic:** Arithmetic garbled circuits

**Visa Research, Palo Alto, USA** **May 2022 - Aug 2022**
*Research Intern*, **Mentor:** Srinivasan Raghuraman
**Topic:** Impossibility of fairness MPC, UC formalization for the channel protocols

**Visa Research, Palo Alto, USA** **May 2021 - Aug 2021**
*Research Intern*, **Mentors:** Ranjit Kumaresan, Mohsen Minaei
**Topic:** Programmable payment channel, scalable non-malleable NFT auction

**Carnegie Mellon University, Pittsburgh, USA** **Jul 2018 - Sep 2018**
*Research Intern*, **Advisor:** Guy Blelloch
**Topic:** Faster parallel sorting algorithm based on sample sort

## PUBLICATIONS

∗: Co-first authors
†: Alphabetic order

1. Yang, Y. and Heath, D. Two Shuffles Make a RAM: Improved Constant Overhead Zero Knowledge RAM. (To appear on **USENIX Security** 2024)

2. Hazay, C. and Yang, Y. †Toward Malicious Constant-Rate 2PC via Arithmetic Garbling. (To appear on IACR **EUROCRYPT** 2024)

3. Kumaresan R., Le, D., Minaei, M., Raghuraman, S., Yang, Y. and Zamani, M. †Programmable Payment Channels. (In Proceedings of **ACNS** 2024)

4. Raghuraman, S. and Yang, Y. †Just How Fair is an Unreactive World? (In Proceedings of IACR **ASIACRYPT** 2023)

5. Yang, Y., Heath, D., Hazay, C., Kolesnikov, V. and Venkitasubramaniam, M. Batchman and Robin: Batched and Non-batched Branching for Interactive ZK. (In Proceedings of ACM **CCS** 2023) 🏆 **Distinguished Paper Award**

6. Yang, Y., Peceny, S., Heath, D. and Kolesnikov, V. Towards Generic MPC Compilers via Variable Instruction Set Architectures (VISAs). (In Proceedings of ACM **CCS** 2023)

7. Yang, Y., Heath, D., Kolesnikov, V. and Devecsery, D. EZEE: Epoch Parallel Zero Knowledge for ANSI C. (In Proceedings of IEEE **EuroS&P** 2022)

8. *Heath, D., *Yang, Y., Devecsery, D. and Kolesnikov, V. Zero Knowledge for Everything and Everyone: Fast ZK Processor with Cached ORAM for ANSI C Programs. (In Proceedings of IEEE **S&P** 2021)

9. *Shao, L., *Yang, Y., Yao, H., Ho, T. Y. and Cai, Y. LUTOSAP: Lookup table based online sample preparation in microfluidic biochips. (In Proceedings of ACM **GLSVLSI** 2017)

## MANUSCRIPTS

∗: Co-first authors
†: Alphabetic order

1. Yang, Y., Heath, D., Hazay, C., Kolesnikov, V. and Venkitasubramaniam, M. Tight ZK CPU: Batched ZK Branching with Cost Proportional to Evaluated Instruction. (Under Submission)

2. Wang, H., Park, S., Yang, Y., Feng, B., Lunardi, W., Kim, T., Zonouz, S., and Lee W. Sound-Boost-Soundness: Effective RCA and Attack Detection for UAVs via the Acoustic Side-Channel. (Under Submission)

3. Minaei, M., Le, D., Kumaresan, R., Beams, A., Moreno-Sanchez, P., Yang, Y., Raghuraman, S. and Zamani, M. Scalable Off-Chain Auctions. (Under Submission)

## SERVICES

- **Program Committee:** CCS 2024, CANS 2023
- **External Reviewer:** CRYPTO 2024, EUROCRYPT 2024, CRYPTO 2023, PKC 2023, EuroS&P 2022
- **Volunteer:**
  - K-12 Math Kangaroo Competition 2024: Manager of Georgia Tech's Center
  - CRYPTO 2023: Student Volunteer

## HONORS & AWARDS

| | |
|---|---|
| Distinguished Paper Award, ACM CCS Conference | 2023 |
| RSAC Security Scholar, RSA Conference | 2022 |
| Gold Medal, ACM International Collegiate Programming Contest (Beijing) | 2016 |
| Gold Medal, China Collegiate Programming Contest (Changchun) | 2016 |
| Gold Medal, China Collegiate Programming Contest (Nanyang) | 2015 |
| Top 600 of Google Codejam | 2014 |
| Silver Medal, National Olympiad in Informatics | 2014 |