Yibin Yang

📍 3604 Stonewall Ct SE, Atlanta, GA-30339, USA
☎ (678) 564-9024 ✉ yyang811@gatech.edu
🌐 https://yibinyang.info/

Research Interests

● Applied Cryptography ● Zero-Knowledge Proofs (ZKP) ● Secure Multi-Party Computation (MPC)

I am interested in applied cryptography and privacy, focusing on designing novel provably secure ZKP and MPC protocols. I build efficient ZKP and MPC systems that can execute *off-the-shelf* programs written in high-level programming languages, such as C and Assembly.

Education

2019 – Present **Ph.D. in Computer Science,** Georgia Institute of Technology, Atlanta, USA
Advisor: Vladimir Kolesnikov
GPA: 4.0/4.0

2015 – 2019 **B.Eng. in Computer Science and Technology,** Tsinghua University, Beijing, China
Exchange in Spring 2018, KTH Royal Institute of Technology, Stockholm, Sweden
GPA: 3.8/4.0

Awards and Grants

2023 – 2025 **Visa Research Award,** Visa Inc.
Principal Investigator: Vladimir Kolesnikov
$125,000 gift to support research in our lab. I initiated the discussion of this grant when I spent two summers at Visa Research as a research intern. I drafted and collaborated on this successful grant proposal with my advisor, Vladimir Kolesnikov. To date, I have led three published research papers associated with this grant — "LogRobin++: Optimizing Proofs of Disjunctive Statements in VOLE-Based ZK" (ASIACRYPT 2024), "Tight ZK CPU: Batched ZK Branching with Cost Proportional to Evaluated Instruction" (CCS 2024), and "Toward Malicious Constant-Rate 2PC via Arithmetic Garbling" (EUROCRYPT 2024).

2023 **Distinguished Paper Award,** ACM CCS 2023
My first-author research paper, "Batchman and Robin: Batched and Non-batched Branching for Interactive ZK," was selected as one of the distinguished papers on ACM CCS 2023. CCS is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM).

2022 **RSAC Security Scholar,** RSA Conference
Each year, RSA conference selects "brightest up-and-coming cybersecurity students" as the RSAC Security Scholar. I was selected in 2022 after being nominated by Georgia Tech.

2016 **Gold Medal,** ACM International Collegiate Programming Contest (Beijing, China)

Gold Medal, China Collegiate Programming Contest (Changchun, China)

2015 **Gold Medal,** China Collegiate Programming Contest (Nanyang, China)

2014 **Silver Medal,** National Olympiad in Informatics (NOI), China

Research Publications

(∗: Co-First Authorship †: Alphabetic Order)

Conference Proceedings

[1] †C. Hazay, D. Heath, V. Kolesnikov, M. Venkitasubramaniam, and **Y. Yang**, "LogRobin++: Optimizing Proofs of Disjunctive Statements in VOLE-Based ZK," in *Annual International Conference on the Theory and Application of Cryptology and Information Security* (ASIACRYPT), 2024.

[2] **Y. Yang**, D. Heath, C. Hazay, V. Kolesnikov, and M. Venkitasubramaniam, "Tight ZK CPU: Batched ZK Branching with Cost Proportional to Evaluated Instruction," in *ACM SIGSAC Conference on Computer and Communications Security* (CCS), 2024.

[3] **Y. Yang** and D. Heath, "Two Shuffles Make a RAM: Improved Constant Overhead Zero Knowledge RAM," in *USENIX Security Symposium* (USENIX Security), 2024.

[4] †C. Hazay and **Y. Yang**, "Toward Malicious Constant-Rate 2PC via Arithmetic Garbling," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (EUROCRYPT), 2024.

[5] †R. Kumaresan, D. V. Le, M. Minaei, S. Raghuraman, **Y. Yang**, and M. Zamani, "Programmable Payment Channels," in *International Conference on Applied Cryptography and Network Security* (ACNS), 2024.

[6] †S. Raghuraman and **Y. Yang**, "Just How Fair is an Unreactive World?" In *Annual International Conference on the Theory and Application of Cryptology and Information Security* (ASIACRYPT), 2023.

[7] **Y. Yang**, D. Heath, C. Hazay, V. Kolesnikov, and M. Venkitasubramaniam, "Batchman and Robin: Batched and Non-batched Branching for Interactive ZK," in *ACM SIGSAC Conference on Computer and Communications Security* (CCS), 2023, 🏆 **CCS Distinguished Paper Award**.

[8] **Y. Yang**, S. Peceny, D. Heath, and V. Kolesnikov, "Towards Generic MPC Compilers via Variable Instruction Set Architectures (VISAs)," in *ACM SIGSAC Conference on Computer and Communications Security* (CCS), 2023.

[9] **Y. Yang**, D. Heath, V. Kolesnikov, and D. Devecsery, "EZEE: Epoch Parallel Zero Knowledge for ANSI C," in *IEEE European Symposium on Security and Privacy* (EuroS&P), 2022.

[10] D. Heath*, **Y. Yang***, D. Devecsery, and V. Kolesnikov, "Zero Knowledge for Everything and Everyone: Fast ZK Processor with Cached ORAM for ANSI C Programs," in *IEEE Symposium on Security and Privacy* (S&P), 2021.

[11] L. Shao*, **Y. Yang***, H. Yao, T.-Y. Ho, and Y. Cai, "LUTOSAP: Lookup Table Based Online Sample Preparation in Microfluidic Biochips," in *ACM Great Lakes Symposium on VLSI* (GLSVLSI), 2017.

Unpublished Manuscripts

[12] **Y. Yang**, F. Benhamouda, S. Halevi, H. Krawczyk, and T. Rabin, "Gold OPRFs: Post-Quantum Oblivious Power Residue PRF," 2024, Under submission.

[13] M. Minaei, D. V. Le, R. Kumaresan, A. Beams, P. Moreno-Sanchez, **Y. Yang**, S. Raghuraman, P. Chatzigiannis, and M. Zamani, "Scalable Off-Chain Auctions," *Cryptology ePrint Archive, Paper 2023/1454*, 2023, Under submission. 🔗URL: `https://eprint.iacr.org/2023/1454`.

Professional Experience

2024/05 – 2024/11
Applied Scientist Intern, Amazon Web Services, New York, USA
Mentors: Fabrice Benhamouda, Shai Halevi, Hugo Krawczyk and Tal Rabin
Topic: Post-quantum oblivious pseudorandom functions
Outcome: [12]

2023/05 – 2023/07
Visiting Researcher, Bar-Ilan University, Ramat Gan, Israel
Mentor: Carmit Hazay
Topic: Arithmetic garbled circuits
Outcome: [4]

2022/05 – 2022/08
Research Intern, Visa Research, Palo Alto, USA
Mentor: Srinivasan Raghuraman
Topics: Impossibility of fair MPC, UC formalization for the channel protocols
Outcomes: [5], [6]

2021.05 – 2021/08
Research Intern, Visa Research, Palo Alto, USA
Mentors: Ranjit Kumaresan and Mohsen Minaei
Topics: Programmable payment channels, scalable non-malleable NFT auctions
Outcomes: [5], [13]

2018/07 – 2018/09
Research Intern, Carnegie Mellon University, Pittsburgh, USA
Mentor: Guy Blelloch
Topics: Improved parallel sorting algorithm based on random samplings

Professional Contributions

Program Committee Member

2025	CCS 2025, EuroS&P 2025, WWW 2025
2024	CCS 2024
2023	CANS 2023

External Reviewer

2025	EUROCRYPT 2025
2024	ASIACRYPT 2024, CRYPTO 2024, EUROCRYPT 2024, TCC 2024
2023	CRYPTO 2023, PKC 2023
2022	EuroS&P 2022

Teaching Experience

Spring 2021, 22, 23
Graduate Teaching Assistant, Special Topics: Blockchain
Co-invented an Ethereum coding course project "Buzzcoin." Held office hours and graded homework, reports, and exams. Helped design and update teaching materials according to the latest progress in the field.

Spring 2020
Graduate Teaching Assistant, Intro to Graduate Algorithms
Graded homework and exams for Georgia Tech's CS-6515-O01. This is an online course with over 450 students.

Outreach

2024, 25 **Manager of Georgia Tech's Center,** K-12 Math Kangaroo Competition
Math Kangaroo is an annual international math competition for K–12 students. In 2024, my center had 45 participants, encompassing a diverse range of ages, races, and genders.

Volunteering Experience

2024 **Session Chair** of CCS 2024
Chaired session "Applied Crypto: Customized cryptographic solutions."

2023, 24 **Student Volunteer** of CRYPTO 2023, 24
Helped CRYPTO conferences arrange sessions.

Invited Talks

- "Efficient Batched and Non-Batched Disjunctions in Linear-Homomorphic Commit-and-Prove ZK," in Security Seminar, Stanford University, September 2024
- "Efficient Batched and Non-Batched Disjunctions in Linear-Homomorphic Commit-and-Prove ZK," at NTT Research, September 2024
- "Efficient Batched and Non-Batched Disjunctions in Linear-Homomorphic Commit-and-Prove ZK," in Visa Research Security Seminar, Visa Research, September 2024
- "Efficient Batched and Non-Batched Disjunctions in Linear-Homomorphic Commit-and-Prove ZK," in Private Computing Tech Talk, Google, August 2024
- "Batchman and Robin: Batched and Non-batched Branching for Interactive ZK," in Intern Tech Talk, Amazon, August 2024
- "Zero-Knowledge Proofs Beyond Circuits and Constraints — How to Efficiently Build a ZK CPU?" in CrySP Speaker Series on Privacy, University of Waterloo, March 2024
- "Zero-Knowledge Proofs Beyond Circuits and Constraints — How to Efficiently Build a ZK CPU?" in Theory Seminar, University of Toronto, March 2024
- "Zero-Knowledge Proofs Beyond Circuits and Constraints — How to Build a ZK CPU?" in IIIS Seminar, Tsinghua University, December 2023
- "Zero-Knowledge Proofs Beyond Circuits and Constraints," at Northwestern University, September 2023
- "Two Shuffles Make a RAM: Improved Constant Overhead Zero Knowledge RAM," in Security and Privacy Research at Illinois Seminar, UIUC, September 2023
- "Just How Fair is an Unreactive World?" at Ariel University, July 2023
- "Just How Fair is an Unreactive World?" in BIU-IISC Reading Group, Online, July 2023

Open Source Repositories

- LogRobin++ [1], 🔗URL: `https://github.com/gconeice/logrobinplus/`
- Tight ZK CPU [2], 🔗URL: `https://github.com/gconeice/tight-vole-zk-cpu/`
- Improved ZK RAM [3], 🔗URL: `https://github.com/gconeice/improved-zk-ram/`
- Batchman and Robin for ZK Disjunctions [7], 🔗URL: `https://github.com/gconeice/stacking-vole-zk/`
- VISA 2PC via Garbled Circuits [8], 🔗URL: `https://github.com/gconeice/GAR/`