Janabel Xia

janabelx.com | janabeltxia@gmail.com | linkedin.com/in/janabel-xia | github.com/janabel

Education and Relevant Coursework (*graduate-level)

Harvard University — Cambridge, MA
PhD in Mathematics — *Sep. 2025 – Present*

Massachusetts Institute of Technology (MIT) — Cambridge, MA
Bachelor of Science in Mathematics, GPA 5.0/5.0 — *Sep. 2020 – May 2024*

- **Math**: Algebra I (18.701), Real Analysis (18.100B), Nonlinear Dynamics (18.353), Continuum Modelling (18.300), Discrete Math Seminar (18.204), Info Theory Seminar (18.424), Complexity Theory* (18.405), Algebraic Extremal Combinatorics* (18.218), Theoretical Cryptography* (18.425), Graph Theory & Additive Combinatorics* (18.225)

Publications and Preprints

- Liam Eagen, Hy Ngo, Vikas Rushi, Ying Tong, Moven Tsai, and Janabel Xia, *OpenAC: Open Design for Transparent and Lightweight Anonymous Credentials*, Cryptology ePrint Archive, Paper 2026/251 (2026), eprint.iacr.org/2026/251
- Janabel Xia, *Deterministic Stack-Sorting for Set Partitions*, ECA **4** (2024), no. 3, Article S2R23 doi.org/10.54550/ECA2024V4S3R23
- Ethan Pesikoff, Benjamin Przybocki, and Janabel Xia, *The Maximum Hook Length of d-Distinct Simultaneous Core Partitions*, Electron. J. Combin. **30** (2023), no. 3, Paper No. 3.30, doi.org/10.37236/11553
- Judy Hsin-Hui Chiang, Anh Trong Nam Hoang, Matthew Kendall, Ryan Lynch, Son Nguyen, Benjamin Przybocki, and Janabel Xia, *Bender-Knuth involutions on linear extensions of posets*, Discrete Mathematics **347** (2024), no. 9, 114068,doi.org/10.1016/j.disc.2024.114068
- Tyler Beauregard, Janabel Xia, and Mike Rosulek, *Finding One Common Item, Privately*, Security and cryptography for networks, Lecture Notes in Comput. Sci., vol. 13409, Springer, Cham, [2022] © 2022, pp. 462–480, doi.org/10.1007/978-3-031-14791-3_20

Academic Research Experience

UMN Duluth Combinatorics REU — June 2023 – August 2023
Research Experience for Undergraduates (REU) sponsored by Jane Street Capital — *University of Minnesota Duluth*

- Conducted research under Colin Defant and Noah Kravitz on stack-sorting unordered sequences. Improved bounds for minimum stack numbers required to sort specific sequences, resulting in a solo publication listed above.

UMN Twin Cities Combinatorics and Algebra REU — June 2022 – August 2022
National Science Foundation, Research Experience for Undergraduates (REU) — *University of Minnesota Twin Cities*

- Conducted research under Professor Vic Reiner on group actions on linear extensions and under Hannah Burson on simultaneous core partitions. Tested conjectures in Python using SageMath software.

Oregon State University Math and Theoretical CS REU — June 2021 – August 2021
National Science Foundation, Research Experience for Undergraduates (REU) — *Oregon State University*

- Conducted research under Professor Mike Rosulek on secure Diffie-Hellman Private Set Intersection protocols for variations on sampling a single item from the intersection, resulting in a publication at the international SCN 2022.

Awards and Achievements

James Mills Peirce Fellowship 2025-2026 — Jan. 2025
On recommendation of the math department, received as a PhD student in the natural sciences an engineering.

National Science Foundation Graduate Research Fellowship Program Recipient — Apr. 2024
Received the NSF GRFP as one of 83 mathematical sciences students.

Invitation to the XI Chapter of Phi Beta Kappa Honor Society — Apr. 2024
Invited to be a member of Phi Beta Kappa, the oldest academic honor society, as an MIT undergraduate.

European Girls' Math Olympiad (EGMO) Individual Silver Medalist — Apr. 2019
Competed internationally as 1 of 4 members on the 1st place US Team.

Two-time Math Olympiad Program (MOP) Attendee — June 2018, June 2019
Attended the US math Olympiad training camp for top high school students.

Work Experience

Community Privacy Residency November 2024 - Present
Co-founder *Remote & Taipei, Taiwan*

- Co-founded and co-organized the Community Privacy Residency, a 4-week residency bringing together 43 cryptographers, developers, designers, community organizers and activists from 15 countries to research, co-design, and build privacy infrastructure. Applied for grants, ran applications, and designed programming from late November to late February. Led finances and operations. Ran first residency from February - March 2025.

zkID Research and Standards May 2025 - September 2025
Researcher *Remote*

- Worked on ZK Standards efforts. Conducted research, architecture design, and writing for zkID, an initiative() by the Ethereum Foundation to promote the adoption of privacy layers around government-issued digital ID systems, such as the EUDI, and more.

0xPARC Foundation July 2024 - February 2025
Research and Development Contractor *San Francisco & Remote*

- Wrote blog posts here and here to distill hard mathematical concepts into a form accessible to technical generalists. Developed interactive educational demos for key cryptographic primitives, as well as proof-of-concept zero-knowledge applications. Conducted research review into distributed and collaborative proving systems that allow users to jointly and verifiably compute on private data.

Mathematical Olympiad Program Teaching Assistant June 2021, June 2022
Mathematical Association of America *Carnegie Mellon University*

- Graded student work on Mock Olympiad tests held every other day of the program. Developed detailed rubrics for grading, and presented problem solutions during test review.

Volunteering and Leadership

Justice 4 Housing Sept. 2024 – February 2025
Intern *Boston, MA*

- Volunteered with Justice 4 Housing in their Hands On Defense (HOD) program under Naia Wilson. Strengthened data infrastructure by cleaning, organizing, and migrating case data; enhanced the nonprofit's capacity to manage housing support for formerly incarcerated individuals.

Active Community Engagement Freshman Pre-Orientation Program Dec. 2020 – August 2023
Coordinator, Counselor *MIT*

- As a coordinator, directed all programming and managed counselors beyond counselor duties. As a counselor, led social justice workshops, supervised community service placements, organized community-building events like Boston walking tours, and facilitated sensitive discussions based on year-round training.

MIT Fixation September 2021 – Present
Artistic Director, Captain *MIT*

- As an artistic director for MIT's competitive contemporary dance team, choreographed and directed the team set piece. As captain, led warmups and organized team bonding.

Skills

Languages: Python, Typescript/JavaScript, HTML/CSS, Circom, Rust
Tools: Jupyter Notebook, SageMath, NumPy, Matplotlib, Git, GitHub, VS Code, Android Studio

Development Projects

POD Folding August 2024 - November 2024

- Built a proof-of-concept website combining applied cryptography "folding schemes" and "PODs", which are highly general cryptographic data types. Website demonstrates the ability to prove ownership of many PODs by "folding" many instances into a singular proof. https://github.com/janabel/frog-POD-counting.

zkPoll Private Polling dApp January 2023

- Created zkpoll.xyz, an end-to-end private polling site deployed on the Ethereum blockchain. Wrote zkSNARK circuits in the Circom programming language to enable anonymous proofs of membership in voter sets with the Groth16 proving system. https://github.com/zk-poll/zk-poll.