

# Janabel Xia

[janabelx.com](http://janabelx.com) | [janabeltxia@gmail.com](mailto:janabeltxia@gmail.com) | [linkedin.com/in/janabel-xia](https://linkedin.com/in/janabel-xia) | [github.com/janabel](https://github.com/janabel)

## EDUCATION AND RELEVANT COURSEWORK (\*GRADUATE-LEVEL)

### Harvard University

*PhD in Mathematics*

Cambridge, MA

Sep. 2025 – Present

### Massachusetts Institute of Technology (MIT)

*Bachelor of Science in Mathematics, GPA 5.0/5.0*

Cambridge, MA

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

- Janabel Xia, *Deterministic Stack-Sorting for Set Partitions*, ECA **4** (2024), no. 3, Article S2R23  
[doi.org/10.54550/ECA2024V4S3R23](https://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](https://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](https://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](https://doi.org/10.1007/978-3-031-14791-3_20)

## ACADEMIC RESEARCH EXPERIENCE

### UMN Duluth Combinatorics REU

*Research Experience for Undergraduates (REU) sponsored by Jane Street Capital*

June 2023 – August 2023

*University of Minnesota Duluth*

- Conducted combinatorics research under Colin Defant and Noah Kravitz. Investigating the novel problem of stack-sorting unordered sequences, improving bounds for minimum stack numbers required to sort specific sequences, resulting in a solo publication listed above.

### UMN Twin Cities Combinatorics and Algebra REU

*National Science Foundation, Research Experience for Undergraduates (REU)*

June 2022 – August 2022

*University of Minnesota Twin Cities*

- Conducted combinatorics research on group actions on linear extensions under Professor Vic Reiner and simultaneous core partitions under Hannah Burson, resulting in two publications listed above. Tested conjectures with Python using SageMath software.

### Oregon State University Math and Theoretical CS REU

*National Science Foundation, Research Experience for Undergraduates (REU)*

June 2021 – August 2021

*Oregon State University*

- Conducted cryptography research under Professor Mike Rosulek. Worked on secure Diffie-Hellman Private Set Intersection protocols for variations on sampling a single item from the intersection, resulting in a publication at the Security and Cryptography for Networks (SCN) 2022 international conference.

## 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 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

---

<b>Community Privacy Residency</b>	November 2024 - Present
<i>Co-founder</i>	<i>Remote &amp; Taipei, Taiwan</i>
• Co-founded and co-organized the <u>Community Privacy Residency</u> , 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, booked physical spaces, designed programming and community events, all from late November to late February. Led finances and operations. Ran first iteration from February - March 2025.	
<b>zkID Research and Standards</b>	May 2025 - September 2025
<i>Researcher</i>	<i>Remote</i>
• Worked on <u>ZK Standards</u> efforts. Conducted research, architecture design, and writing for <u>zkID</u> , 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.	
<b>0xPARC Foundation</b>	July 2024 - February 2025
<i>Research and Development Contractor</i>	<i>San Francisco &amp; Remote</i>
• Wrote blog posts <u>here</u> and <u>here</u> to distill hard mathematical concepts into a form accessible to technical generalists. Developed <u>interactive educational demos</u> for key cryptographic primitives, as well as <u>proof-of-concept zero-knowledge applications</u> . Conducted research review into distributed and collaborative proving systems that allow users to jointly and verifiably compute on private data.	
<b>Mathematical Olympiad Program Teaching Assistant</b>	June 2021, June 2022
<i>Mathematical Association of America</i>	<i>Carnegie Mellon University</i>
• 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

---

<b>Justice 4 Housing</b>	Sept. 2024 – February 2025
<i>Intern</i>	<i>Boston, MA</i>
• Volunteered with <u>Justice 4 Housing</u> 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.	
<b>Active Community Engagement Freshman Pre-Orientation Program</b>	Dec. 2020 – August 2023
<i>Coordinator, Counselor</i>	<i>MIT</i>
• 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.	
<b>MIT Fixation</b>	September 2021 – Present
<i>Artistic Director, Captain</i>	<i>MIT</i>
• 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

---

<b>POD Folding</b>	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. <a href="https://github.com/janabel/frog-POD-counting">https://github.com/janabel/frog-POD-counting</a> .	
<b>zkPoll Private Polling dApp</b>	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. <a href="https://github.com/zk-poll/zk-poll">https://github.com/zk-poll/zk-poll</a> .	