

WELCOME

NOVEL LATTICE ASSUMPTIONS WORKSHOP

Martin R. Albrecht

13 July 2026

We have gathered here to murder funny lattice assumptions!

PURPOSE II

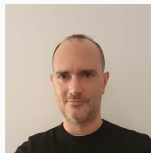
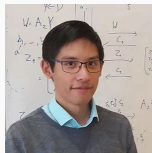
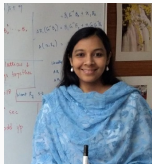
- The aim of this workshop is that there are *fewer* lattice assumptions at the end of this workshop¹ than there were before.
- You are "not allowed" to come up with novel assumptions unless they *replace* existing ones.
 - Replacing one assumption by another is neutral: it doesn't remove assumptions but keeps their number constant.

¹... and the papers are written up

HOW TO KILL AN ASSUMPTION?

- Break it!
- Show that it is implied by another assumption.
- Construct its flagship applications from another, preferably more conservative, assumption.
- ...

ORGANISERS



- Shweta Agrawal, IIT Madras
- Martin Albrecht, King's College London
- Ngoc Khanh Nguyen, King's College London
- Russell W F Lai , Aalto University
- Damien Stehlé, PQShield
- Hoeteck Wee, NTT Research
- Alex Liu, ICMS

- We have talks in the mornings
- We have open discussion sessions in the afternoons
 - We rely on you to make this work.
 - Find each other and **kill some assumptions!**

Schedule

<https://icms.ac.uk/activities/workshop/novel-lattice-assumptions/>

Niklas started a fairly comprehensive zoo of novel lattice assumptions

<https://latticeassumptionzoo.org/>

- If you see an issue, help fix it
- If you murder an assumption, record it on the wiki

FIN

QUESTIONS?