io

# This talk starts with an inciting incident..

- 2023 trip to Marseille

# Life changing moment

- Trip to Marseille

# Life changing moment

- Trip to Marseille

# Changed my life

- Started living alone
- Moved to a city to be close to my friends
- Stopped digital nomad , have a home
- Started focusing on health an exercise
- Found a peace that I didn’t know was possible
- Left PSE / EF

# All of this

- Food poisoning
  - AND
- Cos I want more !
- Never enough !
- Its not enough what we have
- I’m not the only one who’s life was changed / will be changed by food poisoning

# What is not enough

- Proof of validity
  - Kind of useful
  - Not transform the world
- ZKid
  - Why is currency more empowering than zkID?
  - Inherently about excluding people

# What could we have ?

- 2pc is for lovers
  - FHE / MPC multiplayer
  - But needs interaction
  - 1 million users ! No ! Liveness!
- IO is what we need !

If you want something new you have to do things differently

# Why don’t we have this already

- Its hard
- Theoretically possible but impracticable **from standard assumptions**
- BTW we are already using many non standard assumptions
  - Snark friendly hash function
  - Grinding in Fri

# Why do we assume

- P =? NP
  - Can’t prove this is true
  - Can’t prove some things are hard
  - Have to Assume some things are hard
- What assumptions do we currently use ?
  - Prime number stuff
  - Lattices are an attempt to base assumptions on something simpler

# Newer assumptions

- Lattices are much simpler than prime number based assumptions
- It seems more clearly hard to me.
- Prime number are security by obscurity it seems.
- RLWE (Lattices) became standard assumption after ~10 years
  - Tho many people still skeptical about them

# Which is gonna break more AI or Quantum computer

- AI seems likely to break more things than Quantum will
- Because AI is making it easier to learn
- Quantum is a weird tool
- If I had to bet on people with more knowledge or people with better tools. I would always bet on more knowledge
- Prediction
  - AI will break more than Quantum in next 20 years

# So lets actually just do IO

# Candidate schemes

- IO from standard assumptions: https://eprint.iacr.org/2020/1003.pdf
- IO from LPN : https://eprint.iacr.org/2021/1334.pdf
- IO from Evasive LWE: https://eprint.iacr.org/2024/1719
- IO from ADP: https://eprint.iacr.org/2020/889.pdf
- Psudo random obfuscation: https://eprint.iacr.org/2024/1742.pdf
- Local Mixing: https://eprint.iacr.org/2024/006

# Implementations

- LPN: https://github.com/SoraSuegami/iOMaker
- Local Mixing: https://github.com/gausslabs/obfustopia
- Evasive LWE WE: https://tinyurl.com/y62cn45m

# Goals

- Break schemes
- Implement tooling to build IO appbuildlications from standard or non standard assumptions

# Bounty

- https://obfustopia.io/
- Local mixing
  - ~1014 gates circuits
  - Obfuscated circuits ~230k gates
  - Find circuit that has ~1014 gates
- 10k USD
- phantom.zone , 0xparc , EF

# Will IO finish cryptography ?

- Very close !
- What am I suppose to do then ?
  - Finish cryptogrpahy !
  - Never enough !
  - Inconsistent

# Join us!

# More talks

- 2pm Stage 6: Phantom.zone and IO Jay
- IO Friday Breakout 2: 2:15 – 3:45

When you assume you make an ass of u and me