FIRESIDE CHAT

ZOOKO WILCOX

Join this welcoming session to discuss about the impact of cryptography in society.

mod
DANIEL BENARROCH

Discover what we can do to align industry around ethical intentions and world-awareness.

ZAC WILLIAMSON

mod

KOBI GURKAN

NEW FRONTIERS, COUNTERNARRATIVES AND STATE-OF-THE-ART IN CRYPTOGRAPHY

PRATYUSH MISHRA

WHAT CAN MPC DO FOR ZKPS?:

How can we design specialized MPC protocols to endow ZKPs with new efficiency, expressivity, and privacy properties, focusing in particular on the use cases of collaborative zkSNARK generation and private delegation of zkSNARK proving.

SOME COUNTERNARRATIVES IN SNARK DESIGN:

We will discuss assorted pieces of "accepted wisdom" that are incorrect, or for which the jury is still out

JUSTIN THALER

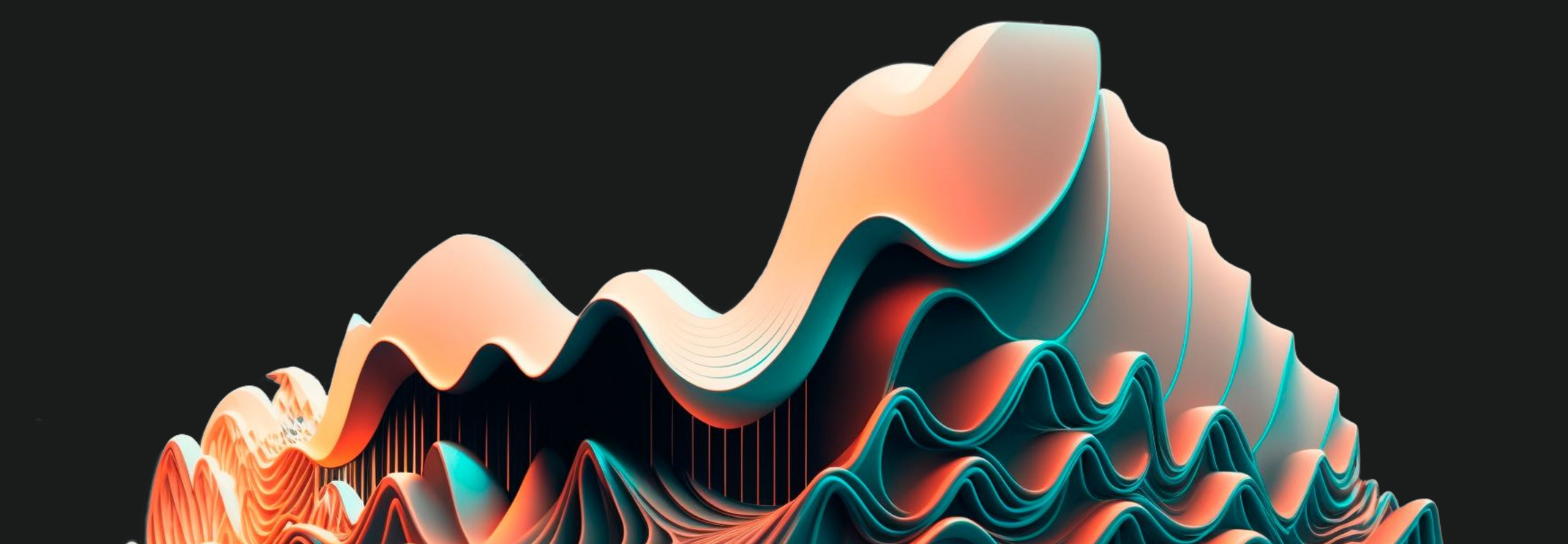
ZOOM PANEL

HEXAGON TABLES

POLYNOMIAL COMMITMENT SCHEMES

ANCA NITULESCU

In the first session, we will give an introduction to polynomial commitment schemes, their security requirements (hiding, binding, knowledge binding), and divisibility property of polynomials (equivalent to proof evaluation). If needed, we will cover useful background including: Schwartz Zippel lemma, assumptions, bilinear groups and pairings… We will finish by explaining how and why KZG works.
In the follow-up session, we will focus on extensions such as: batching KZG, Gemini, DLOG-based polynomial commitments from Bulletproofs (Pedersen vector commitment, IPA), and others (Hyrax, Dark, FRI, Dory).



SECURITY NOTIONS OF NIZKS: FROM SOUNDNESS TO SIMULATION-EXTRACTABILITY

DARIO FIORE

The goal of the basic session is to walk through the security definitions of non-interactive zero-knowledge proofs. We will start from the basic notion of soundness and we will get to understand how to model non-malleability of proofs. In the second, more advanced, session we will do an hands-on experience of simulation extractability with zkSNARK constructions, analyzing malleability attacks and ways to avoid them.

SUM-CHECK PROTOCOL

ARANTXA ZAPICO

Multivariate and univariate sum-check protocols allow a party, the prover, to convince any other, the verifier, that “all the evaluations of a polynomial P(X) over a set S sum to σ.”How does it work? WHY does it work? What’s the hype about it? Univariate, multivariate? Hyperwhat? Have you implemented one of them? Or maybe designed a protocol that relies on one of them? Your experience matters as we want to answer the following question: Which is the best one? Join us for a friendly introduction to the proving system that rules them all (or not).

UNDERSTANDING PRIVACY TECHNOLOGIES THROUGH THE LENS OF MEV

ANDREW MILLER

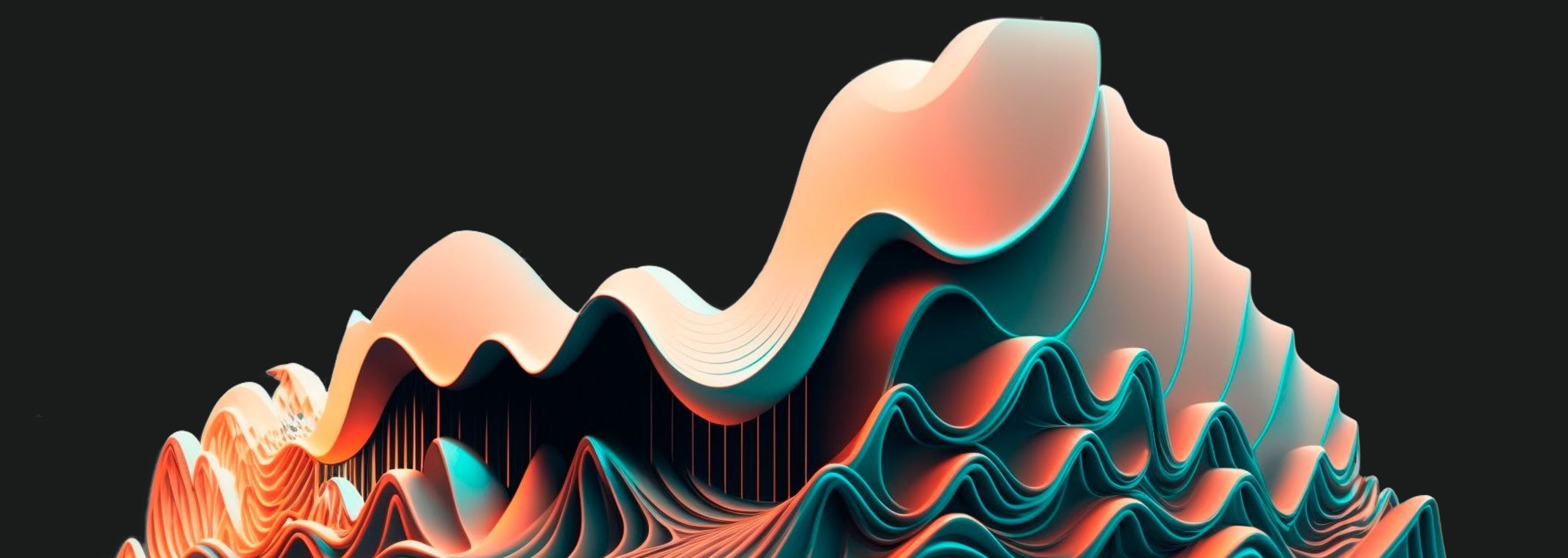
THE MEV PROBLEM:

This session is the first session of a series of sessions on MEV and privacy. This session will introduce the MEV problem, its negative externalities on stateful blockchains, and why privacy technologies are essential to address those. It can be understood by a wide audience, but some entry-level knowledge of DeFi, and basic knowledge of blockchains needed

ALEX OBADIA

USING TEEs & ZKPs FOR MEV APPLICATIONS:

This session is the second session of a series of sessions on MEV and privacy. After introducing the MEV problem and the important role privacy technologies will play in solving it, this session will focus on applicability and how this problem can be tackled with Trusted Execution Enclaves & ZKPs. It can be understood by a wide audience, but some knowledge of MEV, DeFi and blockchains will be welcome.



RECURSIVE PROOF COMPOSITION

YING TONG LAI

A recursive proof is a proof that enforces the accepting computation of the proof system’s own verifier. Recursive proof composition is an efficient way of instantiating proof-carrying data (PCD) and its useful special-case, incrementally-verifiable computation (IVC). It can also be used to conceal the computation being checked; to shrink the size of a proof; or to compose proofs from different proof systems. In this dual-session, we will discuss the foundations of recursive proofs; the wider contexts in which they are used today; and the open questions that remain to be explored.

RECENT FOLDING TECHNIQUES

ARIEL GABIZON

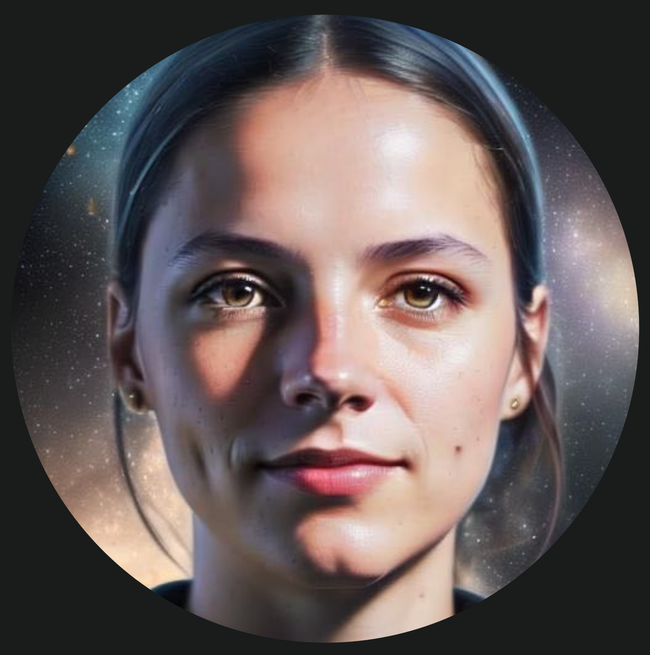
This hexagon table will explain the recent ideas behind folding schemes. The first session will be focusing on Nova, whereas in the second session we will move on to Hypernova and Protostar.

CONCEPTUAL MPC: COMBINING PRIVACY AND UTILITY

LUÍS BRANDÃO

This informal crypto lounge session takes a creative look at the concept of MPC (secure multi-party computation): a notable feat of cryptography. Starting with a riddle (no computer needed) related to secure two-party computation, we'll explore a few basic underpinning concepts, such as ideal functionality, and composability. We'll also consider the relation to zero-knowledge proofs (ZKP). We'll then jointly reflect on the power of conceptual understanding, and how/where it can help devise future applications conciliating privacy and utility.

PHYSICAL ZERO KNOWLEDGE PROOFS ARE CONTRIVED - CHANGE MY MIND!



MARY MALLER

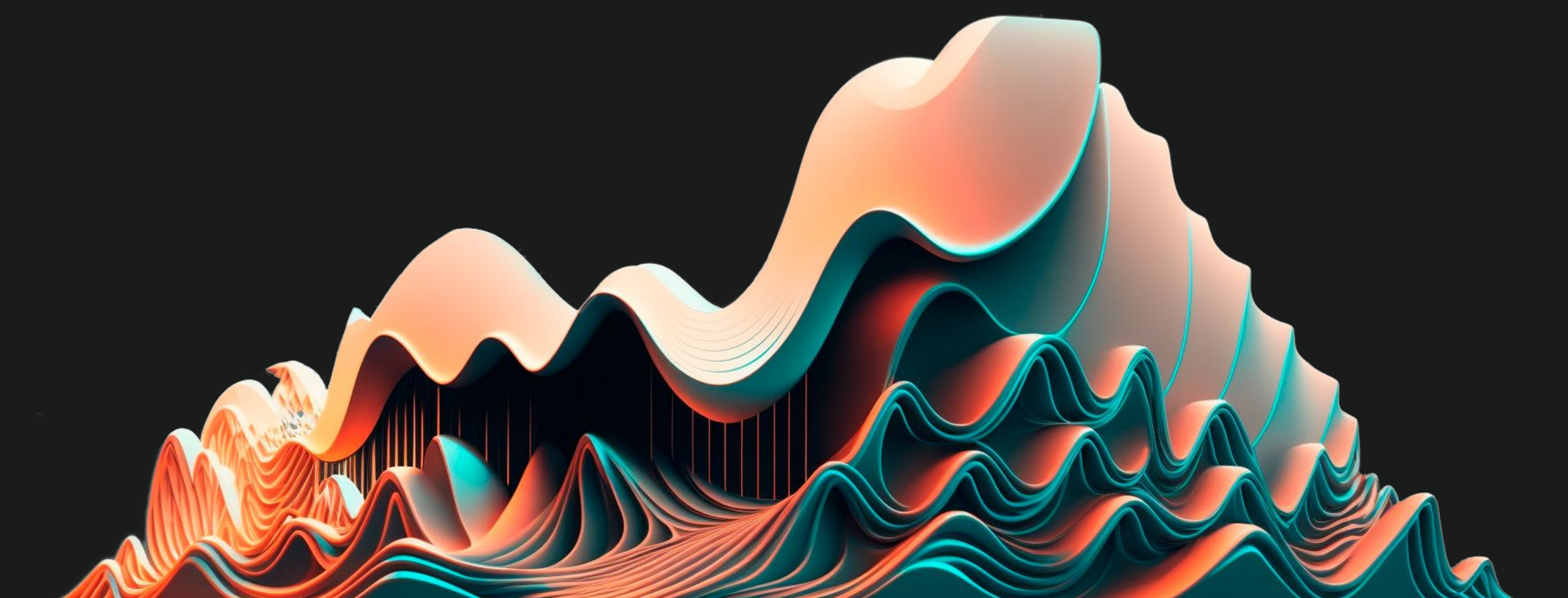
Come to this hexagon table if you want to gain knowledge of zero knowledge from zero. Learn complex notions from scratch thanks to physical examples. Analyse them in the real world and compare them to their theoretical counterparts.

PLAYGROUND

MULTI-PARTY-CARDS: PROTOCOL PUZZLES AND CRYPTO GAMES

ANAÏS QUEROL

During these sessions, we will learn simple interactive protocols with puzzles, cards, and games. You will be split into small groups to put multi-party computation concepts into practice through playing. We will analyse basic boolean components with real world analogies to build more complex structures. Did you know you could build any circuit with a bunch of decks? Find out here!



SECURITY AUDITING

ANNA KAPLAN

During this workshop, participants can learn about the process behind a security audit for cryptography-heavy projects as well as common pitfalls in implementations on zero-knowledge proof technology. We’ll start by giving a bigger picture of how source code audits are planned and conducted, and how project teams can best prepare for a security audits in advance. We will dive into different common error types we as security auditors have seen recently in implementations of zero-knowledge proof technology and, in smaller groups, want to share common struggles and ways out when developing cryptography-heavy systems.

WORKSHOP