Hello! I wanted to share some thoughts and open a discussion within the community about ideas regarding new frontiers for cryptography towards solutions for MEV-related challenges (as well as blockchain-related ones).

As a reminder, there are some protocol-design challenges related to MEV which would be ideally solved using cryptography-based solutions, but we haven't discovered satisfactory solutions yet. Our mid-term approaches to these challenges are centered around the use of TEE (Trusted Execution Environment) technology, which allow us to bypass the mathematical barriers of establishing provably-private protocols that satisfy our use-cases, and instead achieve those guarantees via hardware-based assumptions. As a long-term goal though, we aim to overcome these barriers via provably secure and private (cryptographic) solutions. Towards this, I've been taking a birds' eye view into some ideas from sub-fields of cryptography research, exploring if any of these ideas can lead to relevant community discussions or future FRP project ideas.

Let the community know if there are any similar lines of thought or research you're looking into!