I'm curating a list of open research questions related to Anoma's cryptographic subcomponents. Feel free to respond with anything relevant; I'll edit the top post to keep it up-to-date.

Solver privacy (general topic)

In the Anoma architecture, solvers must know some information about user preferences (the "what") in order to match intents. After intents have been matched, zero-knowledge proofs can be created for full privacy to subsequent verifiers. In general, we are interested in different ways of making solvers privacy (which can compose freely with each other as long as they produce Taiga-compliant outputs). A few particular directions of investigation

Can we improve solver privacy by using TEEs?

Can we improve solver privacy by using TEEs? In particular, can we use clever techniques such as re-randomisation to run the solver algorithm in the TEE, then produce output information which can be used to make the requisite zero-knowledge proof, without losing privacy (subject to the typical TEE assumptions)?

Can we improve solver privacy by using MPC?

Can we run some kind of MPC solver algorithm followed by a collaborative ZKP (link) to match intents in private, then generate the requisite zero-knowledge proof, without losing privacy (subject to some quorum honesty assumption)?

What is the frontier of witness encryption research?

What is the frontier of witness encryption research? Relatively little effort and capital seems to have been devoted to the topic, relative to the potential for applications (e.g. trust-minimized bridging, improved encrypted mempools, intent encryption to a possible counterparty). Are there potentially any low-hanging fruit?

What is the frontier of FHE research?

What is the frontier of fully homomorphic encryption research? Are there known bounds on how (asymptotically) efficient FHE constructions can be, and why or why not? What are the areas theorists should focus on?