

Security Guidelines for zkEVMs – Feedback Session

R&D Session at Forschungsingenieurtagung - June 2025.

Duration: 2 hr

Moderator: George Kadianakis (@asn_d6) // Alex Hicks (@alexanderlhicks)

Note taker: TBA

Agenda

- [5 mins] Motivation for a zkEVM security guidelines document
- [20 mins] Overview of zkEVM security guidelines
- [35 mins] Feedback on security guidelines (Breakouts?)
- [5 mins] Break
- [35 mins] Breakout summaries and group discussion
- [20 mins] Discuss next steps

Summary

This session introduces our draft document (https://docs.google.com/document/d/1W6Y_JPxkt9D2P2sJe29FPOe8luNiaPUvySpuzWcvnwK/edit?usp=sharing) on zkEVM Security Guidelines and gathers feedback from researchers, client teams, and zkEVM projects. After an initial overview we split into focused breakout rooms: proof system, implementation, testing, and formal verification.

At the end of the session, we will have an open discussion on the outcomes of the breakouts and how the EF should reason about zkEVM security going forward.

Goals

It would be great for us to receive community feedback on how we should think about the security of zkEVMs, and how to evaluate the various projects in terms of security and diversity. We plan to update the document according to the feedback of this session.

Pre-reads

Draft of security guidelines doc (https://docs.google.com/document/d/1W6Y_JPpkt9D2P2sJe29FPOe8luNiaPUvySpuzWcvnwK/edit?usp=sharing)