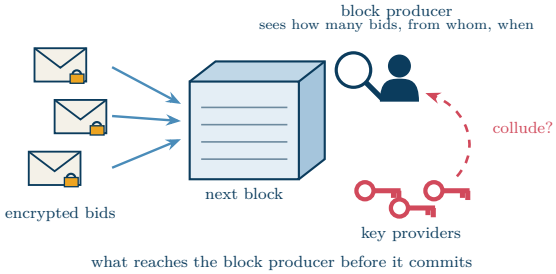
Evaluation of Leakage and Collusion in Encrypted Mempools



Blockchains sell scarce block space through a transaction fee mechanism: users attach bids (fees) to their transactions and the block producer decides which ones to include. Unlike a classical auctioneer, the block producer is a strategic player: it can censor bids, insert fake ones, or adapt its choices to what it sees. Encrypted mempools, now also proposed for Ethereum (EIP-8105), counter this by keeping transactions encrypted until the block content is fixed, typically via threshold encryption with a committee of key providers [1]. Theory confirms the benefit: hiding bids from the block producer enables guarantees that are provably impossible otherwise [2].

Real deployments, however, never hide everything. They leak metadata — how many bids there are, who sent them, and when — and a colluding committee can decrypt early and hand the bids to the block producer, a threat that can be deterred but provably not ruled out [3]. Which leaks are harmless, which are costly, and how much stake must the key providers put at risk to make collusion unprofitable?

In this thesis you will (i) study the basics of fee mechanisms and two or three encrypted-mempool designs, listing what each reveals to the block producer before it commits; (ii) build a simulator that computes the block producer's best response and extra revenue under a given leakage, for standard fee auctions and bid distributions (including ones fitted to real Ethereum fee data); and (iii) use it to rank leakage types and estimate the deposit needed to deter a colluding committee. Ambitious students can study noisy leakage (e.g., timing side channels) or coalitions of users. The topic suits a student interested in blockchain security who is comfortable with basic probability and Python; no background in auction theory is required. More information can be found by contacting Feiyang Qiu (email below).

[1] J. Passerat-Palmbach, "SoK: Encrypted mempools through the MEV lens," in *Advances in Financial Technologies – AFT 2026*, to appear; Cryptology ePrint Archive, Paper 2026/1643.

[2] E. Shi, H. Chung, and K. Wu, "What can cryptography do for decentralized mechanism design?" in *Innovations in Theoretical Computer Science – ITCS 2023*, LIPIcs vol. 251, 2023, art. 97.

[3] M. Kelkar, A. Ganesh, A. Partap, J. Bonneau, and S. M. Weinberg, "Breaking Omertà: On threshold cryptography, smart collusion, and whistleblowing," in *Proc. ACM CCS 2025*, 2025.

Practicalities

Promotor:	Bart Preneel
Daily supervisor:	Feiyang Qiu feiyang.qiu@esat.kuleuven.be office B01.34
Nature of the work:	30% literature, 30% theoretical work (modelling), 40% software
Number of students:	1