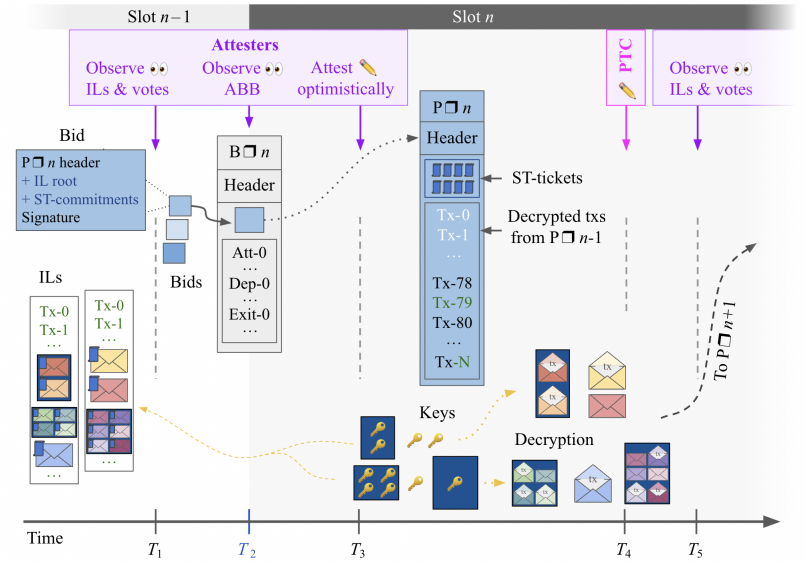
Metadata Leakage in Threshold-Encrypted Mempools



In a decentralized blockchain, the mempool is a public space holding pending transactions awaiting inclusion in a block. Block builders may select, order and discard these transactions to construct blocks that maximize transaction fees, or extract Maximal Extractable Value (MEV) by front-running, back-running or sandwiching user trades, in order to compete for their block being chosen by the proposer. Threshold-encrypted mempools are one approach to protecting users against such exploitation: transactions are submitted encrypted, a committee of key holders releases the decryption key only once the block order is committed, and no single party can decrypt early.

Encryption protects transaction payloads, not their metadata. Sender address, nonce, gas limit, gas price, ciphertext size and arrival time typically remain visible before decryption, and may be sufficient for a builder to infer a transaction's type, target and value, and to attack it regardless.

This project will systematize the metadata exposed by several threshold-encrypted mempool designs, covering both industry implementations and academic proposals, and assess how effective MEV attacks remain under each leakage profile.

Read more: https://eprint.iacr.org/2026/1643.pdf

Practicalities

Promotor:	Yunwen Liu		
Daily supervisor:	Roozbeh Sarenche	firstname.lastname@esat.kuleuven.be	office B01.13
Nature of the work:	30% literature, 10% theoretical work, 60% software		
Number of students:	1		

 © 2026 – 2027 COSIC