Here I am starting to collect a list of (mostly) papers that are relevant toProject Open TEE, which is an effort to arrive at a TEEs with acceptable security models for “web3”.

Good for understanding TEEs in general:

- SoK: Hardware-supported Trusted Execution Environments
- the main thing I got out of this paper is a nice taxonomy of adversarial models and subproblems in TEE design
- they also provide a framework to think about different kinds of techniques employed to solve key subproblems.
- the main thing I got out of this paper is a nice taxonomy of adversarial models and subproblems in TEE design
- they also provide a framework to think about different kinds of techniques employed to solve key subproblems.
- Keystone
- really clean explanation of how a TEE works at a high level.
- really clean explanation of how a TEE works at a high level.
- SGX explained
- really long and detailed. Better to go looking for something specific than read front to end
- really long and detailed. Better to go looking for something specific than read front to end

TDX stuff:

- TDX Demystified
- Mostly useful to coming to understand how TEEs actually work.
- found the attestation section useful
- still had some questions on the hardware
- Mostly useful to coming to understand how TEEs actually work.
- found the attestation section useful
- still had some questions on the hardware
- Google’s TDX security review
- lists a bunch of vulnerabilities found in an audit.
- provides more colour on where keys are stored in hardware
- lists a bunch of vulnerabilities found in an audit.
- provides more colour on where keys are stored in hardware

Understanding specifics:

- An Off-Chip Attack on Hardware Enclaves via the Memory Bus
- good for understanding bus attacks
- good for understanding bus attacks
- Software-Based Off-Chip Memory Protection for RISC-V Trusted Execution Environments
- useful for understanding how memory protection works
- useful for understanding how memory protection works

(Physical) Side Channel Analysis (SCA):

- Differential Power Analysis
- Automatic Extraction of Secrets from the Transistor Jungle using Laser-Assisted Side-Channel Attacks

PUFs

- A PUF Taxonomy
- useful given that PUFs are likely the route to know that the manufacturer doesn't have a store of the hardware secrets somewhere
- useful given that PUFs are likely the route to know that the manufacturer doesn't have a store of the hardware secrets somewhere

Tamper Resistance

- Hardware-Based Methods for Electronic Device Protection against Invasive and Non-Invasive Attacks
- Smart Anti-Tamper Conformal Coating System for Electronic Circuits