Trusted Execution Environments (TEE) — Intel SGX

Secret Network uses Intel's Software Guard Extensions (SGX) implementation of TEE technology. TEE refers to a secure area of a processor where data is inaccessible to any other component in the system. A TEE acts as a blackbox for computation, input and output can be known, but the state inside the TEE is never revealed.

Intel’s Software Guard Extensions (SGX) is a set of security-related instructions built into certain Intel CPUs enabling TEEs. By using SGX chips, the chip owners, system operators, and observers have strong cryptographic guarantees that no party can view what's happening inside of the Secret memory space.

This part of the documentation will discuss all aspects of TEE technology and the way that Secret Network implements it for a secure private computation environment.

Overview

- How Secret Network Uses SGX
- SGX-SPS Security & Reliability
- Trusted & Untrusted Core
- Remote Attestation
- Sealing
-

Last updated11 days ago On this page Was this helpful?Edit on GitHub Export as PDF